



5 Наталья КАСПЕРСКАЯ
АРПП «Отечественный софт»
**«Импортозаместиться
быстро не получится»**

40 Анатолий АКСАКОВ
Государственная Дума РФ
Своевременные меры

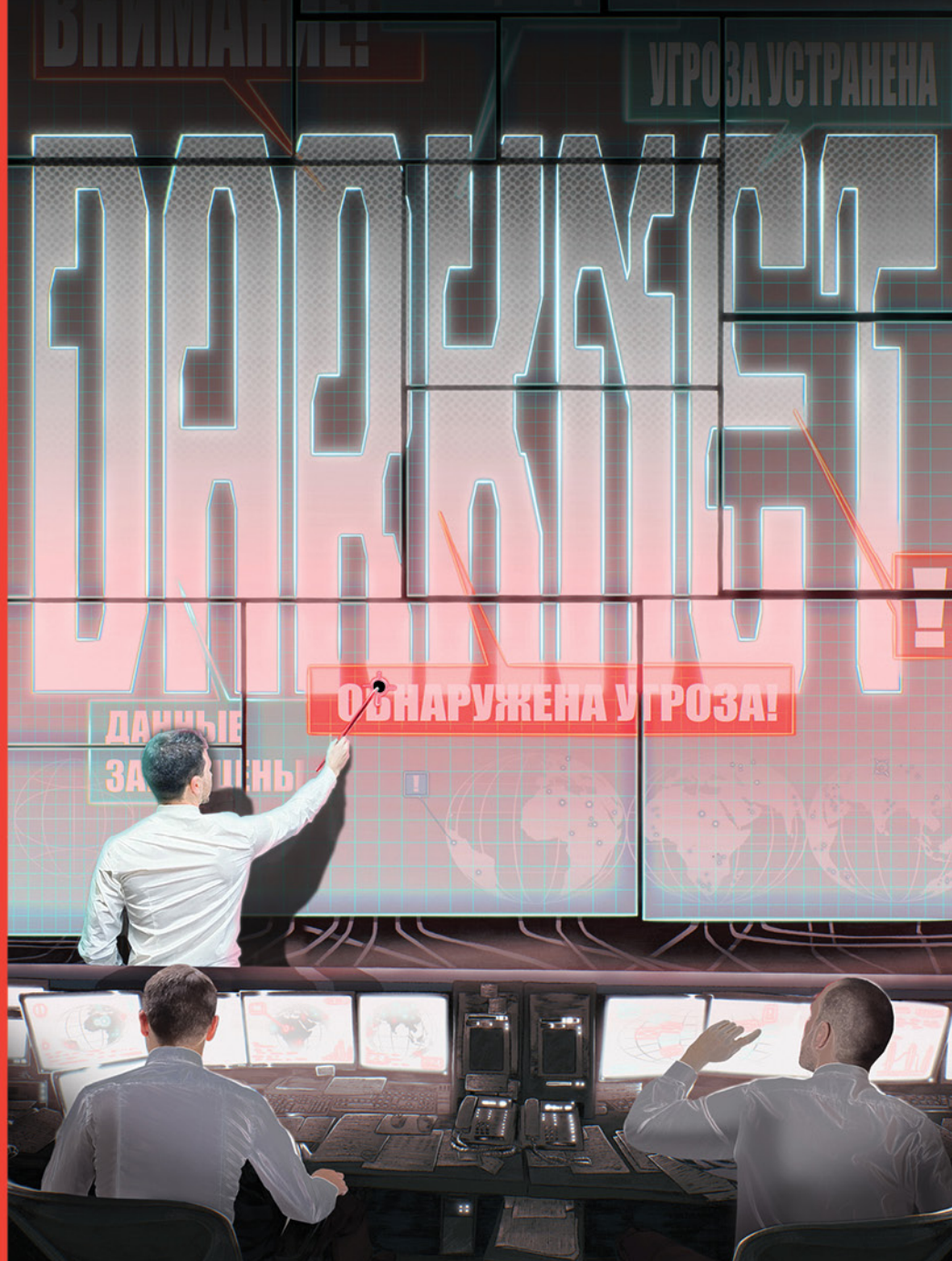
43 Сергей КОРЕЛОВ
Алексей НОВИКОВ
НКЦКИ
**Особенности угроз
в 2022 году**

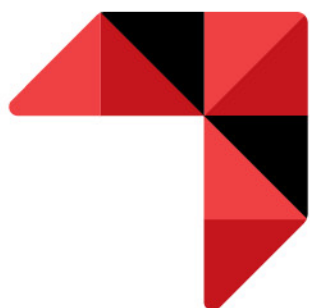


60 Денис БАТРАНКОВ
BIS Journal
Что такое NGFW

146 Борис СТОЛПАКОВ
BIS Journal
**Сталинград. Битва
за информацию**

КИБЕРРАЗВЕДКА. ОБНАРУЖИТЬ, ЧТОБЫ ОБЕЗВРЕДИТЬ





АВАНГАРД



BIS JOURNAL



IB-BANK.RU



BIS TV

Медиа Группа «Авангард»

обеспечивает эффективную многоуровневую
бизнес-коммуникацию на рынке ИБ



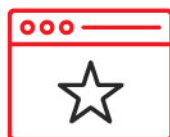
проводит знаковые
деловые мероприятия
отрасли



предлагает самые
широкие возможности
медийного освещения



производит
видеоконтент



предоставляет
медиаресурсы
для решения ваших
маркетинговых задач



Воспользуйтесь уникальным
опытом и медийными площадками
«Авангарда» — с нами вы донесёте
информацию до аудитории
самым эффективным способом!



Игорь НЕКРАСОВ
главный редактор BIS Journal

Говорят, отрасль ИБ очень консервативна и неповоротлива, хотя, как по мне, она больше похожа на трансформер из детского мультфильма. Принимая вызов за вызовом, она на глазах превращается из мирного броневилика в стремительного боевого робота. Но не будем о политике.

Просто поговорим. Тем более, что разговор в сфере ИБ — это и есть та самая консервативная её сердцевина. Ведь не зря уже много лет твердят, что специалисты информационной безопасности не умеют понятно объяснить что-то важное заказчику-руководителю-коллеге из другого отдела — бизнесу, как в последнее время стали это дело называть. Сыплют терминами, несут китайскую тарбарщину и надуваются, как мышь на крупу, — не понимает их бизнес...

А давайте посмотрим, как с этим делом обстоит вообще. В девяностые годы все образованные, и не только, люди поняли, что без английского языка в этом мире — никуда! Стали учить, ездить, практиковать... В результате языковой барьер между нами и другими странами рухнул. Потом стало понятно, что в этом мире нечего делать без языка программирования, — и сегодня программируют все — школьники, лингвисты, разносчики пиццы... Дальше продвинутые родители стали учить детей китайскому или арабскому... и не пожалели.

Но за всем этим забыли про родной язык. Главный вопрос любого подростка: зачем учить русский столько лет?

Как объяснить? И вот недавно появился довод: чтобы тебя понял ИИ!

Генеративные технологии не так давно вышли на уровень, где нейросеть создает картины, музыку, стихи, а скоро станет делать и фильмы. Так вот эти технологии выводят сегодня на первый план именно владение языком. Чтобы ИИ нарисовал или сочинил что-то приличное, ему надо доходчиво и понятно об этом рассказать. А это, как мы уже знаем, не так просто. Появилась даже профессия — промптдизайнер, человек, объясняющий нейросетям, чего от них хотят.

И это только начало: скоро людям предстоит общаться с беспилотными автомобилями, комбайнами, самолетами, кораблями и множеством других умнейших ИИ.

И людям придется учить родной язык, литературу, осваивать риторику.

Тогда, наверное, и в сфере ИБ это дело немного сдвинется))

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

Войлуков А.А. — вице-президент Ассоциации банков России
Сычев А.М. — доцент МГТУ им. Баумана, доктор технических наук
Шипилов В.В. — исполнительный директор Ассоциации российских банков, кандидат технических наук

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Былевский П.Г. — шеф-редактор, доцент департамента ИБ Финансового университета при Правительстве РФ, доцент кафедры международной ИБ МГЛУ, кандидат философских наук
Велигура А.Н. — председатель комитета по банковской безопасности Ассоциации российских банков, руководитель комитета по безопасности НП «НПС», CISA, кандидат физико-математических наук
Виноградов А.Ю. — старший научный сотрудник ФГУП «ЦНИИИХМ»
Вихорев С.В. — советник генерального директора по информационной безопасности IT Expertise
Дзержинский Ф.Я. — независимый эксперт
Зубков А.Н. — генеральный директор ООО «Медиа Группа „Авангард“», директор Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)
Калашников А.И. — директор проекта, Газпромбанк (АО)
Курило А.П. — советник по вопросам ИБ ФБК и FBK CyberSecurity, кандидат технических наук
Левиев Д.О. — председатель Совета НП «Партнерство специалистов по информационной безопасности»
Мельников С.Ю. — заместитель генерального директора ООО «Лингвистические и информационные технологии», доктор физико-математических наук
Некрасов И.В. — главный редактор журнала
Одувалов М.В. — руководитель службы Управления по обеспечению ИБ Банка ВТБ (ПАО)
Окулесский В.А. — заместитель начальника службы ИБ банка «Возрождение», кандидат технических наук
Пазизин С.В. — заместитель начальника Управления по обеспечению ИБ Банка ВТБ (ПАО), кандидат физико-математических наук
Рачкова Е.В. — управляющий директор Управления по обеспечению ИБ Банка ВТБ (ПАО)
Филипчук А.А. — технический директор ГК ЦРТ
Шумский Л.С. — руководитель службы информационной безопасности Яндекс Банка
Янсон И.А. — бизнес-партнер по информационной безопасности, Департамент безопасности ПАО «Сбербанк России», кандидат физико-математических наук

ЭКСПЕРТНАЯ ГРУППА

Баранов А.П. — доктор физико-математических наук, академик Академии криптографии РФ
Батранков Д.В. — руководитель направления сетевой безопасности Positive Technologies
Гадарь Д.А. — вице-президент — директор департамента информационной безопасности, Tinkoff.ru
Калемберг Д.А. — генеральный директор ООО «Сэйфтек»
Лукацкий А.В. — бизнес-консультант по безопасности Positive Technologies
Сабанов А.Г. — заместитель генерального директора АО «Аладдин РД»
Сумманен К.Т. — директор по управлению проектами — вице-президент, Банк ВТБ (ПАО), кандидат физико-математических наук
Хайретдинов Р.Н. — директор по росту компании BIZONE

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И.В.**
Директор по развитию: **Минаков А.В.**
Арт-директор: **Мельников Н.С.**
Руководитель интернет-проектов: **Воробьева А.А.**
Ответственный редактор: **Седов О.В.**
Обозреватели: **Куликов В.А., Бродская М.А., Покатаева Е.Н.**
Иллюстрация на 1-й обложке: **Зинаида Серебрякова**
Фото в номере: **Envato.com, Depositphotos**
Цветокорректор: **Науменко М.Б.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Группа „Авангард“»
Адрес: 127473, Россия, Москва, 3-й Самотечный переулок, д. 21
Тел.: +7 495 921 42 44
Интернет-версия: ib-bankru/bisjournal
E-mail: bis@ib-bank.ru
Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Свидетельство ПИ № ФС-77-61378 от 10 апреля 2015 г.

Все права на материалы, опубликованные в номере, принадлежат журналу «BIS Journal — Информационная безопасность банков». Перепечатка и воспроизведение иными способами без разрешения редакции запрещаются. При использовании материалов ссылка на журнал обязательна. Мнение редакции может не совпадать с мнением авторов. Присланные материалы не рецензируются и не возвращаются.

Подписан в печать 03.02.2023. Тираж 5000 экз. Заказ № 1092023. Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

© BIS Journal, 2023



АКТУАЛЬНОЕ МНЕНИЕ

- 5 Наталья Касперская (InfoWatch)
«Давайте не будем надеяться, что у нас сразу всё импортозаместится»
- 8 Ярослав Бабин (Standoff 365)
Взлёт белой шляпы
- 11 Данила Чежин (Servicepipe)
Особенности DDoS-атак в 2022 году
- 13 Константин Родин (АйТи Бастион)
Востребованные интеграции

НОВОСТИ

- 14 Технологии, законодательство, криминал



52



88

ТЕМА НОМЕРА — КИБЕРРАЗВЕДКА

- 18 Елена Покатаева (BIS Journal)
Узнавать, чтобы защищать
- 25 Дмитрий Шестаков (Group-IB)
Превентивный удар
- 28 Владимир Ульянов (аналитик по кибербезопасности)
«На уровне организации киберразведка нецелесообразна»
- 30 Вячеслав Панкратьев (Университет государственного и муниципального управления)
«В завтрашнем мире будет только одна большая Информационная Безопасность, управляемая ИИ»
- 32 Ашот Оганесян (DLBI)
Бизнес попал... в «ножницы» угроз
- 34 Алексей Павлов (РТК-Солар)
«Киберразведка помогает закрыть множество ИБ-задач»
- 35 Григорий Ревенко (R-Vision)
«Эволюцию не остановишь, а пока... „ТІ ради ТІ“, что не рационально»
- 36 Василий Гурьев (ГК Softline)
«Нельзя разделять ИБ и IT-operations»
- 36 Андрей Арефьев (ГК InfoWatch)
«Вся безопасность под одним «зонтиком» — мечта любого вендора. Но есть нюансы»
- 39 Михаил Смирнов (ГК InfoWatch)
«Без надёжной системы безопасности данные даркнета будут бесполезны»

РЕГУЛЯТОРЫ

- 40 **Государственная Дума РФ**
Анатолий Аксаков (Государственная Дума РФ)
Своевременные меры
- 43 **НКЦКИ**
Сергей Корелов, Алексей Новиков (НКЦКИ)
Тренды и ключевые особенности

БАНКИ

- 48 **Собеседник**
Дмитрий Стуров (Банк Ренессанс)
«Большинство рисков можно снять базовыми средствами защиты»
- 52 **Продолжение разговора**
Артём Калашников (Газпромбанк)
ЦПК. Пора изменить структуру отрасли ИБ
- 55 **GRC**
Николай Казанцев (SECURITM),
Рустам Гусейнов (radcop.online)
Про «народное» GRC

УГРОЗЫ И РЕШЕНИЯ

- 60 **Межсетевые экраны**
Денис Батранков (BIS Journal)
Что такое NGFW
- 65 **Межсетевые экраны**
Владимир Ульянов (аналитик по кибербезопасности)
NGFW как ключевой элемент системы кибербезопасности предприятия
- 69 **DLP**
Дмитрий Слободенюк (ARinteg)
ARZip от ARinteg
- 70 **Обзор**
Яков Гродзенский (CTI)
Защита от скрытых атак
- 72 **Аналитика**
Екатерина Степанова (АМТ-ГРУП)
Оценка рисков
- 74 **Взаимодействие**
Евгений Полян, Анастасия Зуева (Positive Technologies)
Чек-лист
- 78 **Обзор**
Евгения Колодина (ГК «ЦИБИТ»)
Новая эра кибербезопасности
- 80 **Технологии**
Инна Нагимова (Xello)
Как устранить слепые зоны в ИБ

- 82 **Нормативная база**
Александр Моисеев (AKTIV CONSULTING)
Операционная надёжность
- 84 **XDR**
Евгения Лагутина (Лаборатория Касперского)
Мощный ответ на кибервызовы
- 86 **Экосистемы**
Иван Роголев (BI.ZONE),
Антон Свинцицкий (ДиалогНаука)
Безопасность сверху вниз

ИНФРАСТРУКТУРА

- 88 **Деловые мероприятия**
SOC-Форум 2022
- 92 **Деловые мероприятия**
Оксана Дяченко (BIS Journal)
Finopolis-2022
- 94 **Деловые мероприятия**
Марина Бродская (BIS Journal)
AntiFraud Russia 2022
- 98 **Деловые мероприятия**
Марк Новодачный (BIS Journal)
«ИТ-сервис сегодня: от вызовов до решений»
- 99 **Деловые мероприятия**
Марина Бродская (BIS Journal)
Тренд 2023 года — атаки на ИИ
- 100 **Международный конкурс**
Алексей Романенко, Олеся Куликова,
Ольга Рудницкая (Группа компаний ЦРТ)
Золотые ребята
- 104 **Управление рисками**
Сергей Романовский (VK)
Шаг за шагом постепенно
- 106 **API**
Юрий Кардюков (eKassir)
Защищая API
- 111 **Самообразование**
Денис Батранков (BIS Journal)
Что меняется во фреймах Ethernet

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

116 **ИИ+ИБ**

Андрей Жаркевич (Антифишинг)
Анатомия невозможного

ОБРАЗОВАНИЕ И КАРЬЕРА

120 **Продолжение разговора**

Андрей Зарубин (ГК InfoWatch)
Дело за малым: найти систему виртуализации

122 **Обзор hh.ru**

Ксения Трохимец (hh.ru)
Острый дефицит ИБ-специалистов сохраняется

124 **Обзор ИноСМИ**

Анна Катанкина (BIS Journal)
Выживание — это объединение



ПРОГНОЗЫ

136 **Ассоциация ФинТех**

3×10 трендов финансового рынка на 2023 год

138 **Опыт Сбера**

Михаил Анистратенко, Илья Болотов,
Дмитрий Кудияров, Александр Кузьмин
(ПАО СберБанк)
Горизонт — 0–10+ лет



СУБЪЕКТЫ

146 **История**

Борис Столпаков (историк криптографии)
Сталинград 1942–1943

152 **История**

Борис Столпаков (историк криптографии)
Три фрагмента Сталинградской эпопеи

156 **Заметки безопасника**

Александр Игонин (BIS Journal)
Что в имени тебе моем?

ЗА РУБЕЖОМ

128 **Обзор ИноСМИ**

Марина Бродская (BIS Journal)
Киберставки растут

132 **Китай**

Амина Замулина (Сбербанк)
Суровый опыт Поднебесной

«ДАВАЙТЕ НЕ БУДЕМ НАДЕЯТЬСЯ, ЧТО У НАС СРАЗУ ВСЁ ИМПОРТОЗАМЕСТИТСЯ»

BIS JOURNAL ПОПРОСИЛ НАТАЛЬЮ КАСПЕРСКУЮ ПОДВЕСТИ ИТОГИ ПРОШЛОГО ГОДА И ПРЕДСТАВИТЬ СВОЕ ВИДЕНИЕ ГОДА НЫНЕШНЕГО

— Как изменился рынок ИБ за прошлый год?

— Обо всем рынке ИБ сказать не могу, так как у меня нет информации. Могу только рассказать о тех сегментах, в которых мы работаем.

Сегмент защиты от утечек (DLP) вырос незначительно — на 10–12%. Он как рос ранее, так и продолжает расти, рывка мы не заметили. В основном потому что импортозамещение в этом сегменте прошло несколько лет назад, и недавний уход иностранцев на нём никак не отразился. Хотя заказчики стали лучше понимать необходимость в защите информации, т.к. было много громких утечек данных. Просто на бюджетах 2022 года у крупных заказчиков это ещё не успело сказаться. Поэтому мы ожидаем не большого скачка роста в этом году.

На рынке защиты АСУ ТП мы видим резкий всплеск запросов от клиентов и рост интереса, хотя это пока тоже не выражено в деньгах. Потенциальные клиенты спрашивают, изучают, берут систему на пилотное тестирование — количество «пилотов» у нас выросло в 10 раз.

Внезапно появился спрос на те области информационной безопасности, которые традиционно были оккупированы иностранцами, а именно — на межсетевые экраны (МСЭ или файерволы) и DCAP (Data-Centric Audit and Protection), т.е. на аудит данных в файловой системе с анализом прав доступа. В этих сегментах сейчас есть большой спрос на импортозамещение. Многие наши клиенты с началом СВО стали использовать промышленный файервол InfoWatch ARMA для корпоративных нужд. Нам тут же посыпались запросы на его доработку и переориентирование на коммерческий сегмент.

И хотя мы не собирались заниматься корпоративными файерволами, но пришлось. Первую версию выпустили в конце 2022 года, сейчас разворачиваем его продажи.

— Какие процессы в банковской отрасли с точки зрения ИБ вы считаете ключевыми в 2022 году?

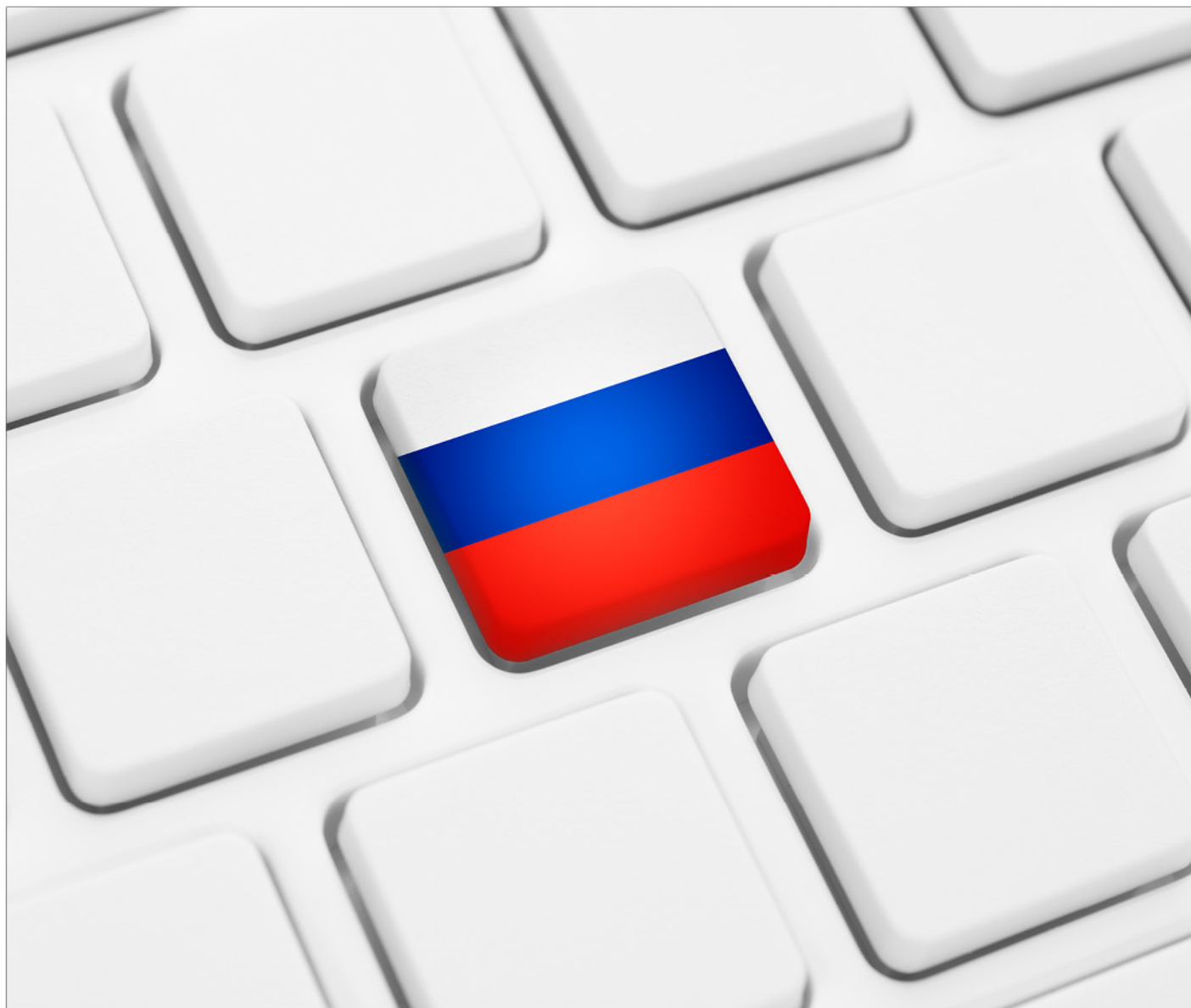
— Не могу говорить о процессах в банковской отрасли, потому что я от неё бесконечно далека. Единственное, о чем я могу рассказать — о ситуации с импортозамещением западного софта в банковской сфере. С момента, когда иностранные производители ушли с российского рынка, перед банками резко встал вопрос — чем это всё замещать. К сожалению, у банков явно не хватает знаний о продуктах, производимых российскими разработчиками.

Поэтому наша Ассоциация разработчиков программных продуктов (АРПП) «Отечественный софт» еще в марте 2022 года озабочилась донесением информации о возможной замене иностранных продуктов отечественными. Для этого мы создали специальный каталог по импортозамещению ПО. По сути, список российских аналогов иностранного ПО.

Банк России осенью 2022 разработал стратегию импортозамещения в кредитно-финансовой сфере на 2022–2024 годы, обсудил ее с отраслью разработки. ЦБ решил привязать вопрос импортозамещения к показателю операционной надежности, который является обязательным для банков. В рамках этого направления ЦБ предлагает очень разумный подход. Они определяют критичный путь для каждого ключевого процесса, на этом пути определяют критичные



Наталья КАСПЕРСКАЯ
президент
ГК InfoWatch,
председатель
правления АРПП
«Отечественный
софт»



софт и «железо». При этом уровень критичности определяется по цветовой шкале, по принципу «светофора» — подход, принятый в информационной безопасности. Соответственно, первыми импортозамещаться должны наиболее критичные процессы и ИТ-системы — те, которые находятся в «красной» зоне. Мне кажется, подход Центробанка к импортозамещению неплохо было бы перенять не только организациям кредитно-финансовой сферы, но и компаниям из других отраслей.

— **Что главное в импортозамещении?**

— Системность. Уж если мы начали им заниматься, то надо продолжать, не бросая, не отвлекаясь и не надеясь, что ушедшие вендоры вернутся. Напомню, что процесс импортозамещения государство начало ещё в 2015 году.

Просто тогда почему-то всем казалось, что это несерьёзно, что риски, про которые говорят скучные безопасники, пройдут стороной и что жареный петух пролетит мимо. А когда петух всё-таки клюнул, все очень сильно расстроились.

Что можно сделать сейчас? Большинство предприятий уже составило списки продуктов на импортозамещение и занимается поиском либо тестированием российских аналогов. Как правило, начинают внедрять то, что проще, а сложные системы (вроде управления предприятием или промышленного ПО) оставляют на потом. Хотя, следуя логике Банка России, замещать надо в первую очередь то, что лежит на критическом пути.

Но тут есть некоторые сложности. Хорошо, если отечественный аналог присутствует в том или ином виде. А что делать, если

отечественного аналога нет? Мне кажется, надо выбирать производителей, которые имеют хоть какие-то наработки в этой сфере и пытаются с ними договариваться, чтобы они «затачивали» продукт под вас. Понятно, что делать импортозамещение в режиме «ошпаренной кошки» сложно. Поэтому давайте не будем надеяться, что у нас всё сразу само собой импортозаместится. Это процесс, он по своей логике растянут во времени и плохо сжимается. Не надо думать, что мы сейчас как-нибудь переживём это непростое время, а потом всё вернётся на круги своя. И мы снова будем спокойно пользоваться импортным ПО. Нет, уже не вернётся.

— Под критическими путями вы имеете в виду замещение в КИИ?

— Нет, я имею в виду процессы, без которых конкретное предприятие жить не может. Для банка, например, таким процессом может быть процесс размещения депозитов, выдачи кредитов или открытия счетов. Если эти процессы встанут и не смогут исполняться из-за отсутствия необходимых ИТ-решений, для банка это может быть болезненно.

— Что вы думаете по поводу миграции ИТ-силы?

— Считать количество уехавших айтишников — бессмысленное занятие. Если все уехавшие — из иностранных компаний, которые свернули здесь свою деятельность, то их отъезд повлияет разве что на сбор налогов. И никак не повлияет на реализацию критичных для страны ИТ-проектов. Если же предположить, что все айтишники уехали с предприятий-субъектов КИИ, это была бы уже совершенно другая, серьезная проблема. Но я, честно говоря, об этом не слышала.

Весной 2022 года мы делали опрос по АРПП — тогда отъезд из компаний-российских разработчиков был очень незначительным — менее 1%. Очевидно, что доля уехавших работников иностранных компаний была выше.

Если мы говорим в среднем — «уехало столько-то», это не много и не мало, это никак. Средняя температура по больнице. Надо понимать, смогут имеющиеся кадры закрыть «дыры» в ИТ или нет. Для этого нужно провести аудит технологий, которые требуются для обеспечения функционирования ИТ страны и цифрового суверенитета, выявить потребность в доработках или разработке нового, оценить потребность в программистах и ресурсах, необходимых для создания этих технологий. И только тогда можно будет понять, хватает айтишников или нет.

Не надо думать, что мы сейчас как-нибудь переживём это непростое время, а потом всё вернётся на круги своя. И мы снова будем спокойно пользоваться импортным ПО. Нет, уже не вернётся

— Какими Вы видите перспективы рынка ИБ в 2023 году?

— Я думаю, что давление на страну будет усиливаться — и с точки зрения компьютерных атак, и с точки зрения воздействия на критическую инфраструктуру. И нам, конечно, надо готовиться к худшему. Поэтому безопасность должна стать неотъемлемой частью даже тех предприятий, которые о ней ранее не думали. Будет ли при этом рынок больше, не знаю, это вопрос вторичный, потому что первично для нас — осуществление безопасности и недопущение нанесения неприемлемого ущерба РФ. Мы со своей стороны стараемся все сделать, чтобы снизить те риски, которые умеем снижать.

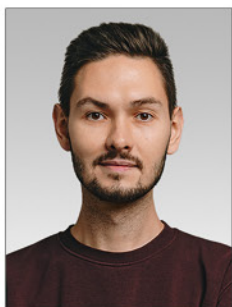
— Назовите, пожалуйста, основные драйверы развития рынка ИБ в 2023 году.

— Во-первых, это импортозамещение, причем, в двух ипостасях. Первая — отечественные вендоры будут «переезжать» на отечественные платформы. Вторая — отечественные вендоры будут производить те продукты, которых раньше не было, например, файерволы, DCAP-системы и другие.

Во-вторых, это необходимость выработки комплексных решений по отражению атак. У нас, к сожалению, ИБ-рынок очень разрознён. Перед ведущими игроками ИБ-рынка сегодня стоит много задач, которые ни одна компания в одиночку решить не в состоянии. Возможно, нам стоит подумать о том, как решать эти задачи сообща.

Что касается ГК «ИнфоВотч», то для себя мы наметили активную работу по развитию своего файервола и расширение функционала решения по защите АСУ ТП промышленных предприятий. Также у нас много работы по развитию технологий контроля информации, так как методы воровства чувствительных данных из российских организаций, банков и страховых компаний становятся все более изощренными. Соответственно, на это нам приходится реагировать, увеличивать количество задач. Так что пока мы хотим сосредоточиться на существующих решениях, сделать их максимально эффективными и отвечающими новой ситуации.

Вопросы задавала
Оксана Дяченко



Ярослав БАБИНСКИЙ
CEO Standoff 365

ВЗЛЁТ БЕЛОЙ ШЛЯПЫ

ПЕРСПЕКТИВЫ РАЗВИТИЯ РЫНКА BUG BOUNTY В РОССИИ

Во всём мире растёт популярность программ bug bounty, в ходе которых компании привлекают исследователей безопасности (этичных хакеров¹) к поиску уязвимостей в своём ПО за вознаграждение. В отличие от пентестов, в bug bounty оплачивается не время, потраченное специалистами, а результат — описанная и подтверждённая уязвимость, при этом от её опасности зависит размер вознаграждения, которое может получить исследователь. Отсутствие временных рамок и обращение к самым квалифицированным специалистам на рынке выгодно компаниям, а возможность заработать, тестируя надёжность популярных онлайн-платформ и сервисов, привлекает независимых исследователей.

СОСТОЯНИЕ МИРОВОГО РЫНКА

Согласно отчёту популярной международной платформы HackerOne, 92% её исследователей способны обнаруживать уязвимости, которые не замечают сканеры. В 2022 году исследователи платформы нашли 65 000 уязвимостей. Хотя большинство (70%) этичных хакеров работают в программах bug bounty помимо своей основной занятости, 47% из них заявили, что в прошедшем году они уделяли хакингу больше времени, чем в 2021-м.

Центр маркетинговых исследований AllTheResearch прогнозирует рост международного рынка bug bounty до 5,5 млрд долларов к 2027 году.

Разработчик платформы Standoff 365 Bug Bounty, компания Positive Technologies совместно с TAdviser исследовала мировой и российский рынок агрегаторов программ

поиска уязвимостей за вознаграждение. Лидер по количеству крупных платформ bug bounty — Азиатский регион, где располагаются 38% проанализированных ресурсов. Платформы Североамериканского и Ближневосточного регионов занимают 21 и 8% рынка соответственно. Европейский регион, куда входит Россия, находится на втором месте рейтинга и включает в себя треть исследованных платформ, в том числе такие крупные, как Intigriti, YesWeHack, Zerocopter и Standoff 365 Bug Bounty.

ПОЛОЖЕНИЕ В РОССИИ

Российский рынок bug bounty активно формируется. В 2020 году Россия вошла в тройку стран с самым высоким уровнем дохода багхантеров, обогнав Китай и Германию. В разное время порядка 40 отечественных компаний (например, VK, Yandex, Tinkoff) запускали открытые программы bug bounty.

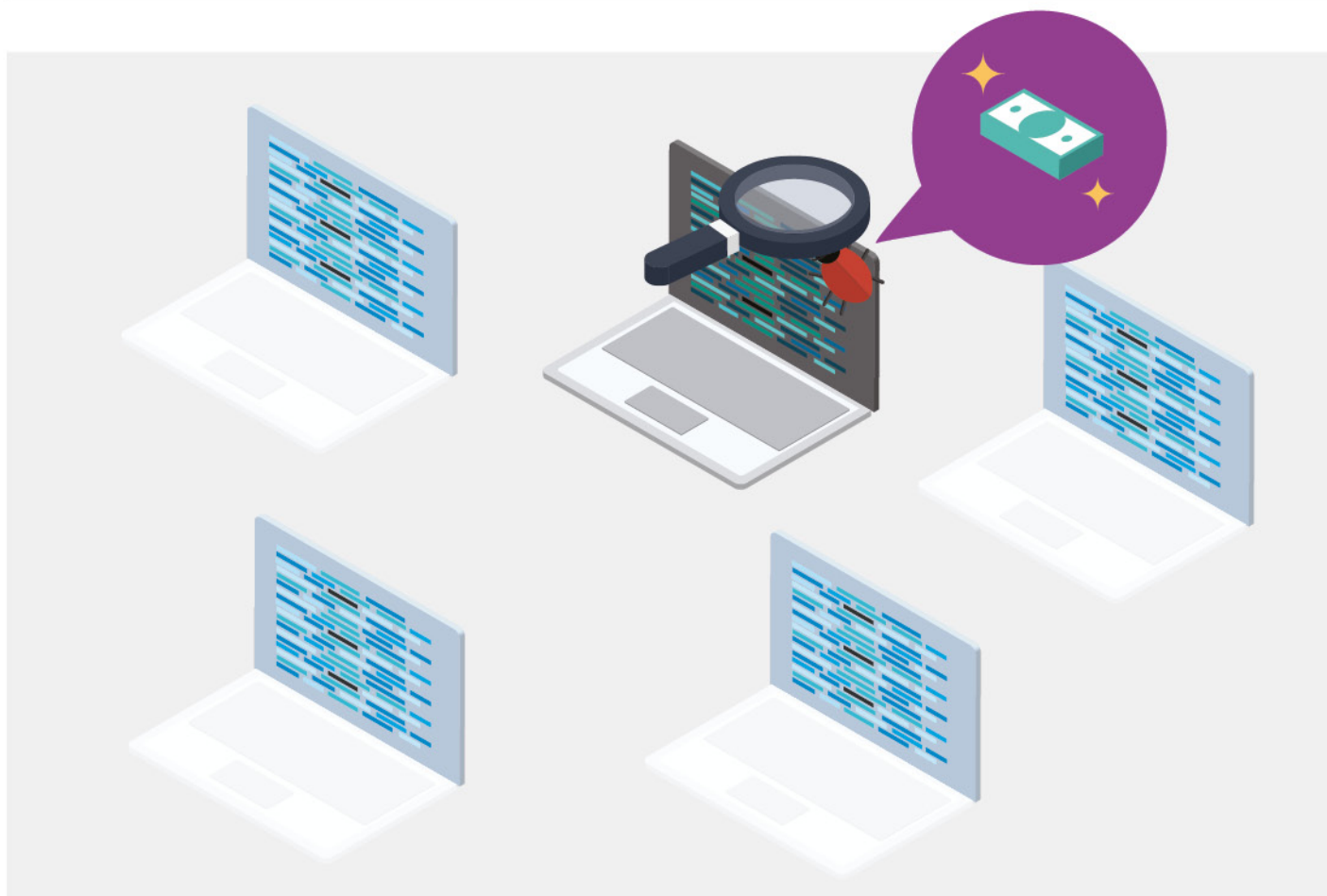
Кроме того, в России на фоне кибератак последнего года появился запрос на повышение киберустойчивости организаций в целом. Всё больше компаний понимает, что кибератаки могут приводить к неприемлемому для бизнеса ущербу, и готовы тестировать свои IT-системы, чтобы убедиться в их защищённости. Программы bug bounty — часть этого процесса: только с помощью bug bounty можно на практике проверить, что конкретное недопустимое событие невозможно реализовать.

Заметна и необычная динамика: если раньше такие программы запускали представители крупного бизнеса, то теперь привлекать на свои сервисы сторонних исследователей безопасности начинают и небольшие организации, а также компании госсектора.

КОМУ И ЗАЧЕМ НУЖНЫ BUG BOUNTY

Сегодня основные заказчики программ bug bounty в России — крупный бизнес, имеющий большое количество клиентов или пользовате-

¹ «Этичный хакер, или белый хакер, а также на сетевом сленге белая шляпа (от англ. White hat) — специалист по компьютерной безопасности, специализирующийся на тестировании безопасности компьютерных систем. В отличие от чёрных шляп (чёрных хакеров), белые хакеры ищут уязвимости на добровольной основе или за плату с целью помочь разработчикам сделать их продукт более защищённым». Википедия



лей: банки, интернет-сервисы, электронная коммерция и ретейл, разработчики IT-продуктов. У таких компаний высоки финансовые и репутационные риски, а также, как правило, есть собственные отделы разработки ПО и возможность оперативно устранять найденные уязвимости.

Компании получают от программ bug bounty следующие выгоды:

- ◆ привлечение к процессу поиска уязвимостей сотен и тысяч специалистов с различным опытом и квалификацией;
- ◆ непрерывное исследование ИТ-инфраструктур на прочность и безопасность;
- ◆ возможность оперативно устранять уязвимости до того, как ими воспользуются злоумышленники;
- ◆ экономическая эффективность, в том числе в долгосрочной перспективе.

СЛОЖНОСТИ РЕАЛИЗАЦИИ ПРОГРАММ BUG BOUNTY

Несмотря на значительные преимущества программ bug bounty, не все компании могут позволить себе их проведение. Среди причин могут быть:

- ◆ сложности с определением исследуемых информационных активов и границ исследований;

- ◆ необходимость привлекать внимание этических хакеров к своей программе;

- ◆ трудности в отслеживании показателей эффективности программы;

- ◆ отсутствие специалистов, способных проверять присланные отчёты, отсеивать сообщения об уязвимостях с низким уровнем опасности и выстраивать эффективную коммуникацию с исследователями;

- ◆ необходимость построить процесс исправления уязвимостей.

ПЛАТФОРМЫ BUG BOUNTY

Часть этих сложностей (и координацию в вопросах, которые должны быть решены внутри компании) могут взять на себя платформы bug bounty — агрегаторы, на которых размещены программы поиска уязвимостей, предлагаемые различными компаниями, а исследователи могут выбрать интересующую. Платформы bug bounty удачно объединяют в себе сообщество этических хакеров и команду экспертов по кибербезопасности, которые выстраивают коммуникацию между компаниями и исследователями, организуют процесс выплат, а по запросу занимаются проверкой отчётов и верификацией обнаруженных уязвимостей.

Исследователи, ищущие уязвимости на платформах, придерживаются принципа ответственного разглашения, так что компании могут рассчитывать на сохранение информации о найденной уязвимости в тайне от общественности и получают время на её устранение.

В УСЛОВИЯХ ИМПОРТОЗАМЕЩЕНИЯ

В марте 2022 года международные платформы поиска уязвимостей прекратили выплаты пользователям из России, а российские компании, среди которых были Mail.ru, Ozon, «Лаборатория Касперского», «Авито», утратили возможность размещать на платформах свои программы.

Анонсированная за полгода до этих событий платформа Standoff 365 Bug Bounty появилась как раз в этот непростой момент. Отечественные компании обрели возможность проверять защищённость своей инфраструктуры с помощью независимых исследователей, а последние получили предложение выплат, сопоставимых с уровнем международных платформ.

В настоящий момент, помимо Standoff 365 Bug Bounty, существуют платформы BugBounty.ru и BI.ZONE Bug Bounty. При этом половина программ bug bounty в России закрытые, то есть количество исследователей в них ограничено и заранее оговорено. Российские компании готовы платить багхантерам от нескольких десятков до сотен тысяч рублей за найденную уязвимость. В отдельных случаях выплаты достигают 1 млн рублей и более. Например, средняя выплата за критически опасную уязвимость на Standoff 365 Bug Bounty составляет 420 тыс. рублей, что сопоставимо с выплатами по миру.

За шесть месяцев работы платформы Standoff 365 Bug Bounty багхантеры прислали 860 отчётов, найдены и исправлены более 190 уязвимостей, за которые участникам назначено вознаграждение в размере более 11 млн рублей. По числу участников и программ платформа стала лидером среди российских аналогов: на ней зарегистрировались уже более 3300 человек, запущено 36 программ (в том числе «Азбука вкуса», RuStore, «ВКонтакте», «Дзен», Mail.ru, Rambler&Co).

BUG BOUNTY НОВОГО ТИПА

В ноябре 2022 года Positive Technologies объявила о запуске программы bug bounty нового типа, которая ориентирована не на поиск сутубо технических уязвимостей во внешних сервисах компании, а на реализацию действительно

критически опасного для компании события — хищения денег со счетов Positive Technologies. Это новаторский подход к поиску уязвимостей: теперь исследователю нужно разобраться с тем, как выстроены бизнес-процессы компании, обойти системы защиты и продемонстрировать факт хищения денег. Но и объявленное вознаграждение в 10 миллионов рублей также беспрецедентно для России.

В отличие от классических bug bounty, этичным хакерам разрешено использовать для проникновения практически любые способы проведения удалённых атак (включая социальную инженерию). Программа не ограничена по времени и будет действовать вплоть до совершения названного недопустимого события.

Мы считаем такой подход к программам bug bounty новым витком в развитии индустрии кибербезопасности, так как это единственный способ для руководителя компании контролировать и убедиться, что система защиты работает.

ЧТО ДАЛЬШЕ?

Рост киберугроз и возрастание их сложности, вовлечение всё большего числа компаний в вопросы кибербезопасности и недоступность в России многих мировых сервисов позволяют ожидать бурного роста российского рынка bug bounty в ближайшее время.

Этому определённому будет способствовать устранение юридических барьеров, над которым сейчас работают Минцифры и ФСТЭК.

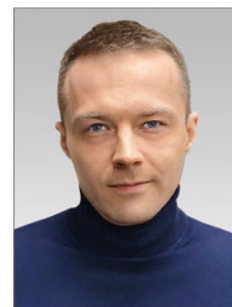
Программы поиска уязвимостей появятся в организациях из различных отраслей экономики, что органически расширит рынок. В программах bug bounty уже сейчас заинтересованы объекты критической инфраструктуры (КИИ), чья деятельность подпадает под действие Указа Президента РФ № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

При этом пул этичных хакеров, к которым могут обращаться российские организации, уменьшился на фоне санкций и отказа иностранных платформ работать с россиянами. Некоторые из них уехали из страны, и в небольшом сообществе экспертов по ИБ не приходится ждать притока специалистов.

Решением «кадрового вопроса» на рынке bug bounty могло бы стать развитие сотрудничества с паназиатским рынком, что подразумевает в первую очередь возможность осуществлять платежи. Мы в Standoff 365 Bug Bounty работаем над увеличением исследовательской аудитории и анонсируем новые возможности уже в 2023 году.

ОСОБЕННОСТИ DDoS-АТАК В 2022 ГОДУ

НА СМЕНУ АТАКУЮЩИМ КОНДИЦИОНЕРАМ И МУЗЫКАЛЬНЫМ КОЛОНКАМ ПРИШЛИ ЛЮДИ



Данила ЧЕЖИН
директор
по продуктам
компании
Servicepipe

2022 год изменил многие базовые принципы, которые лежали в основе проведения DDoS-атак. В итоге вынуждены были перестраиваться и те, кто от них защищается, и те, кто эту защиту обеспечивает.

У подавляющего большинства DDoS-атак на онлайн-ресурсы российских организаций до начала 2022 года был ряд общих черт. Используя эти особенности, можно было выстроить эффективный контур защиты, с чем успешно справлялись разработчики решений в сфере ИБ, провайдеры услуг защиты и интеграторы. К таким типовым чертам относятся следующие:

- ♦ Большинство вредоносного трафика шло из-за рубежа, главным образом с территории США, Германии и Азии.
- ♦ Источники — простейшие боты и скрипты. Генерируемый такими алгоритмами трафик относительно легко отделим от пользовательского.
- ♦ Генераторы трафика — серверы за прокси-сетями и IoT, в частности арендованные вычислительные мощности в облаках, дешёвые

роутеры, камеры, телевизоры и даже кондиционеры или музыкальные колонки, которые имеют выход в интернет.

♦ Явные всплески трафика — большинство атак создавали явные статистические аномалии, на порядки превышая по объёму нормальную загрузку атакуемых ресурсов.

В первом квартале 2022 года ситуация изменилась. Начала прослеживаться более чёткая и масштабная координация атак на онлайн-ресурсы, в том числе сайты и мобильные приложения компаний разных сфер бизнеса, СМИ, госструктур. Кроме того, выросли компетенции тех, кто организует, проводит и координирует эти атаки. Благодаря этому широкое распространение получил доступный пользователю любой подготовки инструментарий для участия в атаках, в том числе атакующие сайты с казуальными играми.

Список целей обновлялся ежедневно, при этом явная логика в его формировании отсутствовала. Таким образом организаторы атак воздействовали не только на ИТ-инфраструктуру организаций, но и на психологию их владельцев

Ключевые метрики

- Тип — HTTPs
- Объем — до 17 млн запросов
- Доп. векторы — UDP, TCP flood
- Длительность — 80+ часов

AS	Request count
Anchorfree GMBH	18%
GIGANET-UA-AS	16%
Citadel Crimea Ltd.	16%
TDV "Teleradio company "Yalta"	8%
M247 Ltd Moscow	7%
MT FINANCE LLC	5%
Telefonica LLC	4%
Anchorfree GMBH	4%
PJSC MegaFon	3%
Network of data-centers "Selecte	3%

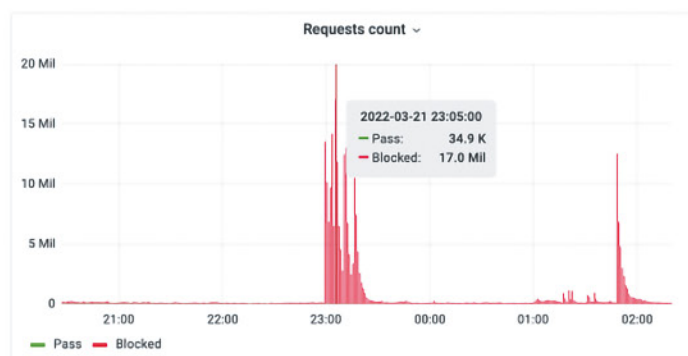


Рисунок 1. Пример DDoS-атаки — пик 21.03.2022. Клиент из сектора СМИ

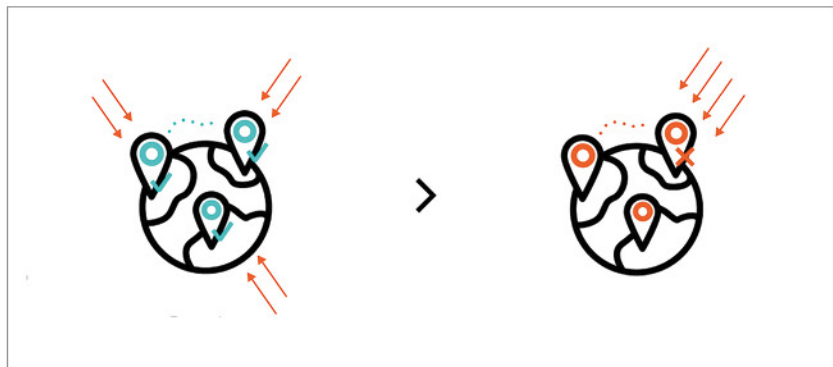


Рисунок 2. Паразитный трафик не балансируется по всей структуре фильтрации, а мощностей отдельных узлов может не хватить для его блокировки. Следом за отказом ближайших к источникам локаций может произойти «веерный» эффект и отказ всей инфраструктуры. Блокировки по гео неприменимы, так как источник атак находится внутри РФ

и руководителей: пусть сегодня нас не атаковали, но нервы потрачены всё равно.

НОВОЕ В DDoS

В итоге привычные для DDoS-атак черты сменились новыми. В частности, источники вредоносного трафика в значительной степени стали локализованы на территориях Украины, а также России, откуда к ресурсам обращаются обычные пользователи. Это делает невозможным ограничение доступа к ресурсам по географическому признаку и сильно затрудняет блокировку атак, поскольку системы фильтрации создавались для распределённых по миру источников и были рассчитаны на фильтрацию меньших объёмов паразитной нагрузки в каждой локации (рис. 2).

Сегодня непосредственными исполнителями атак стали чаще становиться люди, а не боты, точнее, к ботам добавились люди, добровольно предоставляющие свои устройства и для их генерации. При этом некоторые из ботов стали убедительнее имитировать поведение реальных людей, что усложняет их фильтрацию. Простота и удобство инструментов

позволяют принять участие в атаках любому. Исполнителей ищут через массовую рассылку в соцсетях плюс собирают группы в телеграм-каналах и помимо финансовой составляющей подключают идеологическую. Выросла и длительность атак, которые теперь могут длиться до нескольких суток, при этом к ранее атакованным целям возвращаются повторно. Блокировки по IP потеряли эффективность, так как с одного устройства обычного пользователя может идти и легитимный, и паразитный трафик одновременно на один ресурс.

ПО НОВЫМ ПРАВИЛАМ

Эти изменения привели к тому, что применяемая защита на базе привычных зарубежных решений стала неэффективна. Контур безопасности необходимо выстраивать с прицелом на то, что сейчас происходит смена направления атак с недоступности ресурсов на финансовый ущерб бизнесу, также есть тренд на использование DDoS как прикрытия целевых атак, направленных на взлом.

Для противодействия внешним угрозам теперь необходимо использовать более продвинутое решение, которые способны максимально точно блокировать паразитный трафик, не касаясь легитимных пользователей. В реестре российского ПО недавно появилась технология DosGate, разработанная с учётом новых реалий. В зоне повышенного риска сейчас находятся те организации, для которых сайт и приложения — это основной способ коммуникации с пользователями и покупателями. В первую очередь это маркетплейсы, финтех-организации, сетевые и онлайн-ритейлеры, туроператоры (рис. 3). Таким компаниям следует провести аудит безопасности, создать или актуализировать план реагирования на атаки с учётом новых реалий и устранить хотя бы критичные для бизнеса уязвимости и слабые места в периметре защиты.

- 60% пользователей за последние 30 дней совершили как минимум одну покупку онлайн
- 83% трафика генерируют мобильные устройства
- каждый IP-адрес мобильных сетей — десятки тысяч пользователей
- 37% трафика в Интернет генерируют боты
- публичные API — уязвимы для атак
- новые типы ботов виртуозно имитируют реальных пользователей

Рисунок 3. Онлайн-ритейл растёт из года в год. Мы всё чаще вводим свои данные в интернете — и тем чаще они попадают в руки мошенников

ВОСТРЕБОВАННЫЕ ИНТЕГРАЦИИ

В ЧЁМ ПРОФИТ ТЕХНОЛОГИЧЕСКИХ ПАРТНЁРСТВ

Рынок ИТ-систем и, в частности, систем обеспечения информационной безопасности испытывает не самые простые времена. Дело не в том, что нет финансирования, скорее в том, что потребности заказчиков сформированы некогда доминирующими иностранными решениями, многие из которых сейчас недоступны для российского рынка.

Пришло время отечественных решений. Одни вендоры реализуют требования заказчиков самостоятельно, другие идут по пути интеграции и технологических партнёрств, чтобы обеспечить максимальное закрытие потребностей с минимальными затратами ресурсов.

ИНТЕГРАЦИЯ ДОЛЖНА БЫТЬ ВЗАИМНО ПОЛЕЗНОЙ

Вопрос технологических интеграций не всегда стоял остро: когда мы в «АйТи БАСТИОН» только реализовывали первые сценарии для наших заказчиков, некоторым коллегам-партнёрам приходилось подробно рассказывать о выгодах такого подхода. Сейчас ситуация изменилась.

РАМ-решение — специфичное средство защиты, стоит на стыке пользователя и информационной системы. Специфика заключается в том, что мы работаем с объектами, которые маркируются как «привилегированные» и «критические». Если упростить, то пользователи с высоким уровнем привилегий могут делать опасные для критических систем вещи вплоть до полного выведения их из строя. Это, разумеется, недопустимо.

Отсюда и вытекает наше видение процесса интеграций. В первую очередь мы внимательно изучаем то, какие смежные с нашим продуктом СКДПУ ИТ системы обладают функционалом, позволяющим решениям быть взаимно полезными.

Сейчас мы сфокусированы на решениях отечественных производителей, которые могут помочь закрыть задачи наших заказчиков и которые мы не решаем в рамках своего продукта. Например, расширенные средства многофакторной аутентификации, информация о локальных входах на критические узлы,

изменение конфигурации систем и средств защиты и многие другие.

Кроме непосредственно функциональных интеграций, мы проводим проверки и тестирования на совместимость продуктов. Купить продукт, который ты потом не сможешь использовать, — неприятная ситуация. Так мы не только снижаем риски заказчиков, но и упрощаем поиск и выбор подходящих решений для них.

ИДЕЯ ЗАКАЗЧИКА КАК ОСНОВА ТЗ ДЛЯ ИНТЕГРАЦИИ

Драйверов развития всегда два — внешний и внутренний. Внутренний — наши команды развития продукта, аналитики и инженеры. Внешний — наши заказчики. Даже большинство внутренних идей проходит проверку через мнение заказчиков. Наполнить продукт массой функций, которыми заказчики не будут пользоваться, — значит просто потерять время.

На технологических партнёров мы смотрим через призму уникальности и востребованности их продукта. Даже если решение не очень популярно, но может принести реальную пользу, мы будем работать над интеграцией. Конечная цель, как я уже говорил, — закрыть потребность и увеличить полезную нагрузку от внедрения решений.

Мы можем разрабатывать свой продукт, но иметь результат завтра либо интегрироваться с компанией, имеющей большую экспертизу и доверие заказчика в своём классе решений, и помочь заказчику уже сегодня. Это не значит, что мы останавливаемся в собственном развитии. Это означает лишь то, что мы готовы идти в одном направлении с нашими заказчиками, обмениваться опытом и реализовывать действительно нужные функции прямо сейчас.

Мы внимательно изучаем то, какие смежные с нашим продуктом СКДПУ ИТ системы обладают функционалом, позволяющим решениям быть взаимно полезными



**Константин
РОДИН**

руководитель
направления
по развитию
продуктов
ООО «АйТи
Бастион»



BAIDU ПРОТИВ OPENAI

Китайская компания Baidu уже в марте планирует представить потенциального конкурента ChatGPT от OpenAI — собственный чат-бот на основе ИИ.

Сначала Baidu выпустит его в качестве отдельного приложения, а потом собирается встроить в свою поисковую систему. ИТ-гигант, по заявлениям источников агентства, хочет, чтобы наравне со ссылками на сайты в поиске отображались релевантные ответы от чат-бота.

Ранее стало известно, что у Microsoft есть планы встроить ChatGPT в свой поисковик Bing, а Google в 2023 году представит версию поисковой системы с функциями уже «авторского» чат-бота.

СОЗДАСТ ЛИ ПРОБЛЕМЫ УХОД INGENICO?

Французский производитель терминалов для приёма платежей Ingenico, работающий в России с 2007 года, может уйти из страны. Источники утверждают, что это случится уже в начале марта, а техподдержка самих устройств прекратится в конце того же месяца.

России сейчас нет ни среди партнёров компании, ни в списке офисов, а в местном юристе Ingenico, отвечающем за оптовую торговлю, назначен ликвидатор (что является внешним признаком процесса прекращения бизнеса).

Доля действующих в РФ терминалов Ingenico составляет около 50%. Устройства компании занимают основную долю в POS-сетях Сбера, ВТБ и Промсвязьбанка, и в случае исхода игрока останется возможность ремонтировать французскую технику через посредников, однако неясно, будут ли доступны запчасти.

РОЖДЕНИЕ НАЦИОНАЛЬНОГО ЦЕНТРА КРИПТОГРАФИИ

Минцифры и ФСБ создают Национальный технологический центр цифровой криптографии. Его запуск планируется в 2024 году.

Основная цель АНО «НТЦ ЦК» — популяризировать и внедрять криптографические методы защиты. Также среди задач АНО «НТЦ ЦК»:

- ◆ развитие здоровой конкуренции у отечественных производителей средств криптозащиты;
- ◆ производство компонентов средств защиты персональных данных;
- ◆ ведение реестра производителей средств криптозащиты;
- ◆ практическое обучение ИБ-специалистов;
- ◆ определение стандартов в области криптографии и защиты информации.

Планируется привлечь крупнейшие отечественные компании в области разработки средств криптозащиты: «ИнфоТеКС», «КРИПТО-ПРО» и «Код Безопасности». «Мы стремимся

к тому, чтобы производители средств защиты были мотивированы создавать более качественные продукты, а будущие ИБ-специалисты могли учиться на программах, ориентированных не только на теорию, но и на практику», — сказал замглавы Минцифры А. Шойтов.

На данный момент АНО «НТЦ ЦК» уже зарегистрирована как юрлицо.



НА «ГОСУСЛУГИ» С УЛЫБКОЙ

С 1 февраля российские пользователи могут попасть на портал госуслуг не только с помощью пароля, но и с применением биометрии — по желанию.

Для этого гражданину необходимо пройти регистрацию в Единой биометрической системе (ЕБС) и дать своё согласие на использование сервиса. Сегодня зарегистрироваться в ЕБС можно в отделениях кредитных организаций, а в будущем — как ожидается — в МФЦ или с помощью

мобильного приложения. В последнем случае также потребуется загранпаспорт нового поколения и смартфон с NFC-модулем.

Аналитик MForum Analytics Алексей Бойко не исключает возможность доступа киберпреступников к сервису при подключении биометрии: «Я бы предпочёл иметь возможность запретить доступ к своему аккаунту на „Госуслугах“ по биометрии, оставив традиционную двухфакторную аутентификацию».



С КОНФИСКАЦИЕЙ ИМУЩЕСТВА

Комитет Госдумы по госстроительству и законодательству одобрил в первом чтении законопроект о конфискации имущества, полученного в результате киберпреступлений.

Ранее инициативу депутатов во главе с председателем Комитета ГД по

безопасности и противодействию коррупции Василием Пискаревым и сенатором Андреем Клишасом одобрил Кабмин — с некоторыми замечаниями: правительство попросило обосновать необходимость предложенных изменений в УК и указать конкретные примеры нарушений.

Василий Пискарев напомнил о росте мошенничества в кредитно-финансовой сфере, который привёл к ощутимым потерям для граждан. Особенно пожилых. Кроме того, по данным МВД, в 2021 году было совершено 6354 киберпреступления. Это незаконный доступ к компьютерной информации, создание, использование и распространение вредоносных программ, нарушение правил хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, незаконное воздействие на критическую информационную инфраструктуру РФ и т.д.



ЗАПРЕТ СНИМУТ

Из утверждённой Стратегии развития финрынка до 2030 года стало известно, что обсуждается возможность снятия запрета на открытие филиалов банков из «дружественных» стран в России. По мнению властей, это поспособствует привлечению иностранных инвестиций.

Инициативу поддержали и в АРБ. Снятие упомянутого запрета разовьёт конкуренцию на рынке, а это мотиватор снижения стоимости продуктов, отметил президент АРБ Гарегин Тосунян. Плюс мера поможет российскому бизнесу проводить трансграничные сделки и расчёты в эпоху санкций. При этом Тосунян считает, что желающих открыть филиалы вряд ли будет много — из-за угрозы вторичных санкций.



XVI Межотраслевой форум директоров
по информационной безопасности

CISO-FORUM 2023: МОБИЛИЗУЙСЯ!

14 апреля 2023 г., Холидей Инн Сокольники, Москва

● **ЕДИНСТВЕННОЕ МЕРОПРИЯТИЕ, СДЕЛАННОЕ CISO ДЛЯ CISO.**
1000 УЧАСТНИКОВ,
20+ ОТРАСЛЕЙ ЭКОНОМИКИ

● **БУТИК АТМОСФЕРА.**
ГЛАВНЫЕ ТРЕНДСЕТЕРЫ РОССИЙСКОЙ
КИБЕРБЕЗОПАСНОСТИ В ЗАЛЕ И НА СЦЕНЕ

● **ДЕНЬ ЗА ДВА! ВСЕ ТРЕНДЫ И ПЕРСПЕКТИВЫ ОТРАСЛИ ЗА ОДИН ДЕНЬ:**
ТРИ ТРЕКА, 15+ ПРАКТИЧЕСКИХ СЕССИЙ,
ПЛЮС ВЕЧЕРНИЙ ПРИЕМ

● **ПРОВЕРЕНО ВРЕМЕНЕМ.**
ФОРУМУ 16 ЛЕТ.
НАС РЕКОМЕНДУЮТ 92% УЧАСТНИКОВ СОБЫТИЯ!

INFOSECURITY-FORUM.RU

ШПИОНСКИЕ СТРАСТИ

Национальный центр кибербезопасности Великобритании выпустил предупреждение об участвовавших в попытках кражи информации у групп и отдельных лиц, которые занимаются исследованиями в отношении Ирана и России.

Отмечается, что кибератаки нацелены на политиков, журналистов, активистов и аналитические центры. Операционный директор NCSC охарактеризовал хакерские группы как «безжалостные» в преследовании своих целей.

На данный момент от группировок пострадали несколько человек, ущерб оценивается как незначительный. Официально официальные лица не обвиняют Россию и Иран в причастности к шпионажу, но распространено мнение, что две хакерские группы, о которых они предупреждают, связаны с этими государствами.

44 ТЫС. ЖАЛОБ

Как сообщила пресс-служба Роскомнадзора, за прошедший год в ведомство поступило 44 269 обращений россиян, касающихся неправомерной обработки персональных данных. По информации ведомства, это на 0,8% меньше, чем годом ранее.

«38 188 из поступивших обращений — жалобы на действия операторов, осуществляющих, по мнению заявителей, незаконную обработку персональных данных (на 0,3% меньше, чем в 2021 году). 535 записей внесено Роскомнадзором в Реестр нарушителей прав субъектов персональных данных (на 11,5% меньше, чем в 2021 году)», — заявили в РКН.

Также представители ведомства отметили, что наибольшее количество жалоб поступило на действия кредитных учреждений и организаций ЖКХ.



13 РАССЕРЖЕННЫХ СПЕЦСЛУЖБ

Деятельность группировки Hive пресечена в результате совместной операции спецслужб 13 стран. Ключевую роль в операции сыграли США, ФРГ и Нидерланды.

Министерство юстиции США сообщило о прекращении работы серверов хакерской группировки Hive после совместной операции правоохранительных органов США и ФРГ. В результате операции были сорваны требования о выплате \$130 млн, которые программа-вымогатель предъявила сотням жертв по всему миру.

В июле прошлого года сотрудники ФБР проникли на веб-сайт группировки и перехватили 300 ключей дешифрования. Они были переданы жертвам кибератак в 80 странах. В список пострадавших входили больницы, школы, финансовые компании и объекты критической инфраструктуры.

Ликвидация сети произошла в результате расследования прошлогодней

кибератаки. Киберспециалисты из полиции города Эсслингген (ФРГ) проследили путь хакеров до серверов Hive и дали международным партнёрам «важную подсказку», говорится в заявлении прокуратуры Штутгарта. Следственная группа во главе со специалистами ФБР проникла в сеть Hive, наблюдала за её деятельностью и перехватила ключи шифрования.



НА ЧЁРНОМ РЫНКЕ РАСТУТ ЦЕНЫ НА БАНКОВСКИЕ КАРТЫ

С 2021 года средняя стоимость реквизитов пластиковых банковских карт на чёрном рынке выросла вне зависимости от целей их применения.

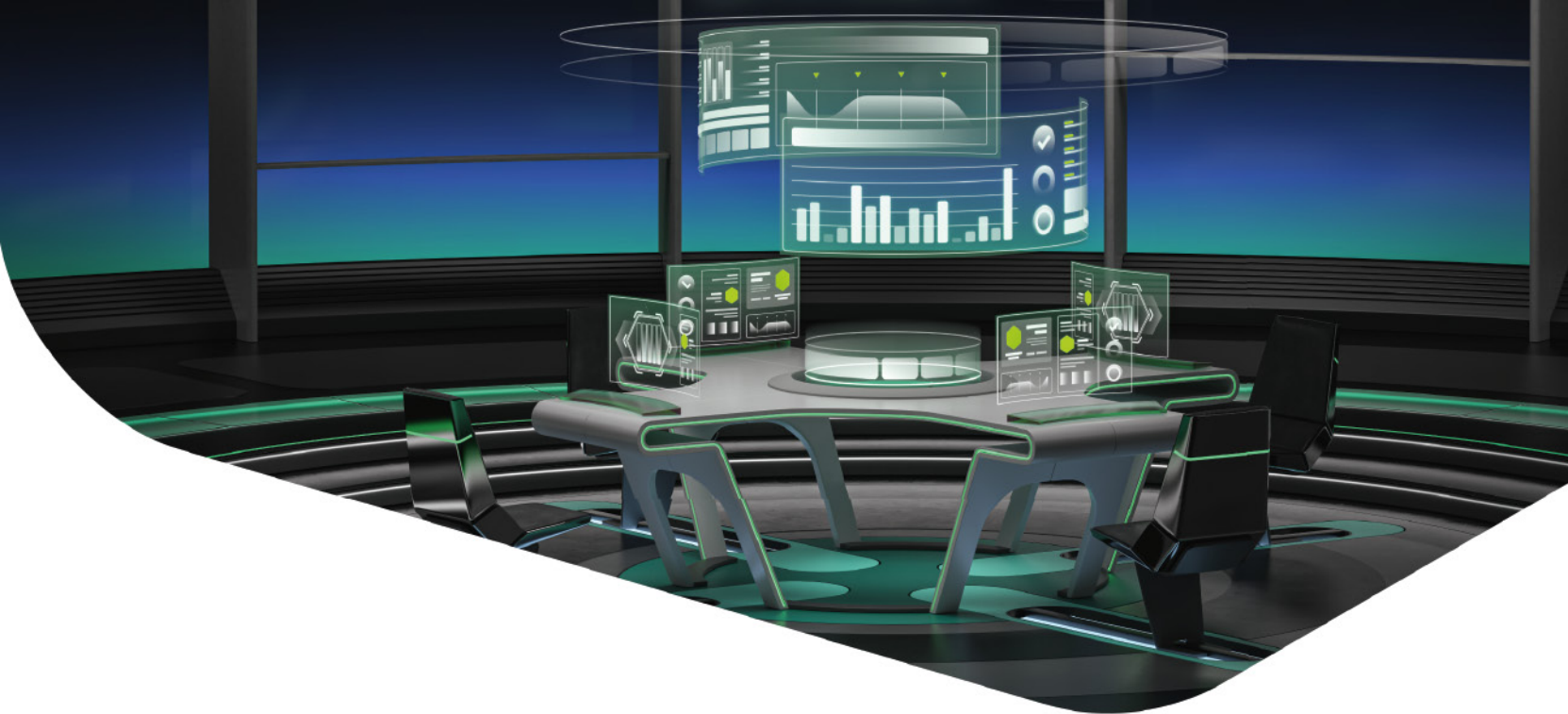
В марте 2021 г. на чёрном рынке банковского «пластика» для дропов классические карты Сбера предлага-

лись по цене 9 тыс. рублей за штуку, золотые — от 14 тыс., а премиальные — от 18 тыс. рублей. К ноябрю 2022 г. цены значительно выросли. За классические карты стали просить от 12 тыс. рублей, за золотые — от 40 тыс., а стоимость премиальных доходит до 100 тыс. рублей.

Дроп-карты других банков стоят дешевле: если «пластик» Сбера продаётся за 30 тыс. рублей, то карты «Райффайзена» — за 22 тыс., «Уралсиба» и ОТП Банка — по 18 тыс.

Тенденция обусловлена мероприятиями, проводимыми банком, по снижению числа дропов среди своих клиентов, в т.ч. благодаря антифрод-механизму и системной работе по борьбе с дроперами, говорится в исследовании. По оценкам Сбера, число граждан по всей России, имеющих признаки дропов, составляет около 500 тыс. человек — банк уже поставил на дополнительный контроль более 35 тыс. таких клиентов.





Kaspersky Anti Targeted Attack

Специализированная защита от целевых кибератак

- Защита основных точек входа потенциальной атаки
- Повышение эффективности процесса реагирования на инциденты
- Целостная картина происходящего в инфраструктуре
- Сбор, хранение и предоставление информации об инцидентах для соответствия требованиям законодательства
- Вместе с Kaspersky EDR составляет решение класса Extended Detection and Response (XDR)

kaspersky АКТИВИРУЙ
БУДУЩЕЕ

kaspersky.ru/enterprise

ДиалОгНаука

СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

dialognauka.ru

УЗНАВАТЬ, ЧТОБЫ ЗАЩИЩАТЬ

РОЛЬ КИБЕРРАЗВЕДКИ НА ДАННОМ ЭТАПЕ ЭВОЛЮЦИИ ИБ



Елена
ПОКАТАЕВА
обозреватель
BIS Journal

Вопрос превентивной защиты корпоративных информационных систем становится всё более актуальным. Один из подходов к её обеспечению заключается в использовании методов киберразведки. Какие инструменты, изначально создававшиеся для нишевых специальных задач, могут быть использованы для обеспечения информационной безопасности в корпоративном секторе? И какие особенности интеграции киберразведки в традиционно оборонительный арсенал ИБ придётся учитывать?

Вместе со всем ИТ-рынком отрасль информационной безопасности проходит очередной этап жёстких испытаний на прочность информационных бизнес-систем и вызовов, открывающих новые горизонты. Предыдущим таким этапом стала пандемия, обернувшаяся в результате мощным взлётом информатизации в русле удалённой работы сотрудников и соответствующих систем ИБ. В феврале прошлого года начался новый виток в развитии информационных систем безопасности бизнеса, вызванный беспримерным санкционным давлением, информационными войнами и многократно усилившимися кибератаками.

У КИБЕРУГРОЗ МЕНЯЕТСЯ ХАРАКТЕР

Одно из ярких проявлений пандемии — всплеск онлайн-мошенничества в банковском секторе. Как отмечают в компании Positive Technologies, в 2021 г. число атак на финансовые компании было сопоставимо с уровнем 2020 г. Но при этом злоумышленники стали обращать меньше внимания на платёжные карты и банкоматы, а в фокусе их внимания оказалось онлайн-мошенничество (кредитный фрод, обход онлайн-проверок, использующих технологии KYC/AML) (рис. 1).

В 2022 г. онлайн-банкинг остался одной из главных целей злоумышленников. Но запомнился этот год в первую очередь как год хакерских атак на отечественные интернет-ресурсы. По оценкам вице-премьера Правительства РФ Дмитрия Чернышенко, было отражено почти 50 тыс. хакерских атак. При этом, по данным компании StormWall, количество DDoS-атак на платёжные системы РФ, совершённых в августе 2022 г., выросло на 126% по сравнению с аналогичным периодом прошлого года. По оценкам специалистов компании, максимальная мощность атак составила 400 тыс. запросов в секунду, а максимальная длительность атак составила 8 часов.

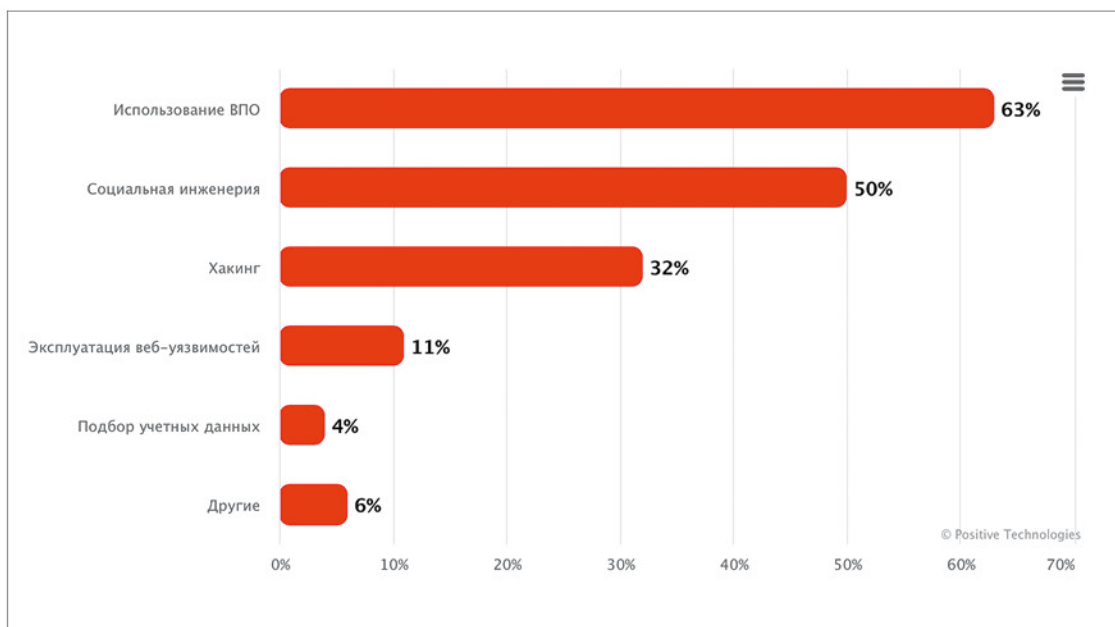


Рисунок 1. Методы атак на компании в 2021 г.
Источник: Positive Technologies, апрель 2022 г.

Примечательно, что мощные DDoS-атаки были организованы группой хактивистов, главной целью которых было не извлечение финансовой выгоды, а нарушение работы российских финансовых сервисов. Замеченная тенденция лежит в русле подготовки к масштабной войне в глобальном киберпространстве.

Об этом говорила директор ДИП МИД России Мария Захарова, комментируя публичный анонс о найме желающих поработать «государственными хакерами», который появился в конце августа в официальном твиттер-аккаунте Кибершколы Министерства обороны США от имени руководителя этой организации Брайана Вайла. «Подобным рекрутингом США на самом деле занимаются давно, но вот открыто термин *nation state hackers* — хакеры, состоящие на службе у государства и осуществляющие атаки от его лица, — публично использовали впервые», — подчеркнула Мария Захарова.

ПРОТИВОСТОЯНИЕ ЩИТА И МЕЧА

А это значит, что вечное противостояние щита и меча продолжается. Согласно отчёту «Атаки на российские компании в III квартале 2022 г.» компании «Ростелеком-Солар», количество инцидентов с высокой степенью критичности, выявленных командой Solar JSOC, сократилось (рис. 2). С одной стороны, это хорошая новость — «градус» инцидентов снизился по сравнению с началом года. С другой стороны, говорят в «Ростелеком-Солар», расслабляться не стоит, так как снижение числа критичных инцидентов не столько говорит о стабилизации ситуации, сколько указывает на то,

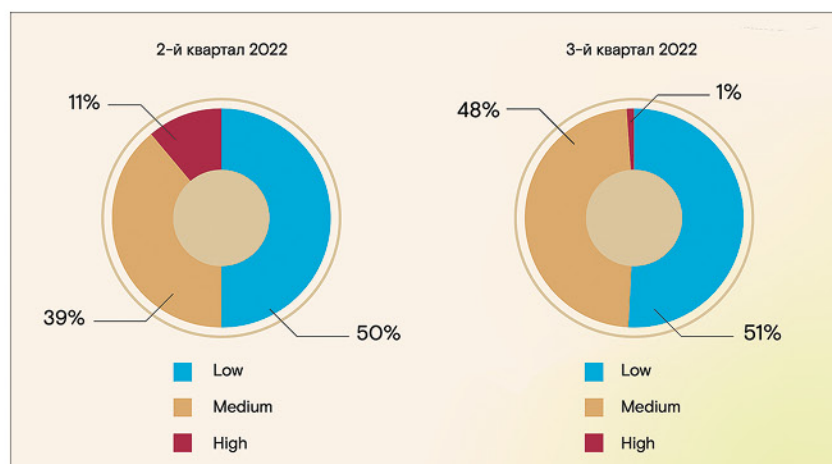


Рисунок 2. Распределение инцидентов ИБ в июле — сентябре 2022 г. по степени критичности. Источник: «Ростелеком-Солар»

что злоумышленники концентрируют усилия на определённых целях и более сложных подходах к атакам: «DDoS- и веб-атаки сделали своё дело, и теперь злоумышленники активно применяют различное ВПО. Фишинг будет одним из двух основных векторов проникновения в инфраструктуру компаний в ближайшие месяцы».

ДАННЫЕ — НАШЕ ВСЁ

С 2018 г. основной мотив атак преступников — получение данных. Согласно исследованию Positive Technologies, в 2021 г. две трети атак на организации были совершены именно с этой целью. В том числе атакам подвергались и производители решений для хранения данных (рис. 3).

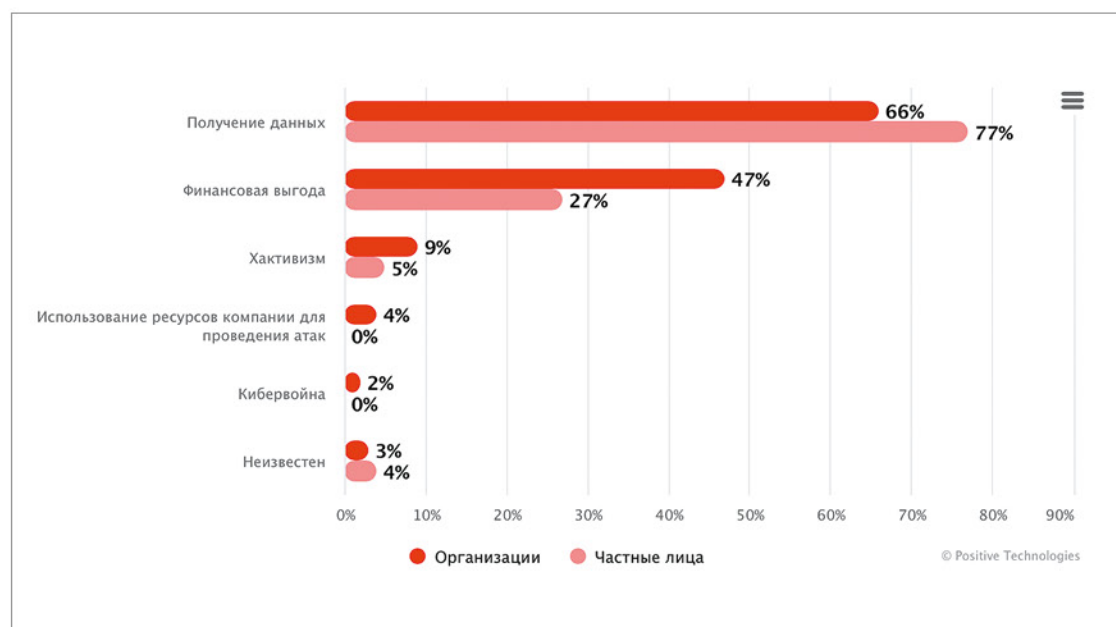


Рисунок 3. Мотивы кибератак (доля атак). Источник: Positive Technologies, апрель 2022 г.

«НОВЫЕ ТОВАРЫ»

Во второй половине прошлого года было отмечено усиление активности киберпреступников в части торговли доступами в корпоративную сеть банков и поиска нелояльных сотрудников. Осенью на «чёрном рынке» интернета новый «горячий товар» — Access-s-a-Service, то есть «доступ как услуга».

Интересная деталь: по итогам первых трёх кварталов 2022 г., подсчитали в Positive Technologies, общее количество атак на российские финансовые организации снизилось на 16% по сравнению с аналогичным периодом 2021 г., что стало результатом усилий по обеспечению информационной безопасности банков. При этом общий объём продаж в даркнете доступов к корпоративным сетям банков вырос в два раза. Естественно, рука об руку с этими процессами идёт постоянный активный поиск сотрудников банков, готовых предоставить доступ к системам или конфиденциальную информацию.

По сведениям Роскомнадзора, с начала спецоперации России на Украине произошло более 140 утечек персональных данных в Сеть, в интернет попало 600 млн записей о россиянах: клиентах сети «Спортмастер», страхового маркетплейса maifin.ru, покупателей ювелирной сети ADAMAS, пользователей услуги аренды самокатов и т.д.

Понятно, что всё обилие данных, связанных с бизнесом компаний, которые циркулируют в интернете, можно использовать для уточнения потенциальных угроз. Причём можно анализировать содержимое и публичного интернета, и его «тёмной части».

OSINT НА МАРШЕ

Аббревиатура OSINT (Open Source INTelligence), подразумевающая сбор данных по открытым источникам интернета, сегодня становится всё более известной в бизнес-среде. OSINT — это фактически бизнес-разведка, которая обеспечивает специалистов по ИБ самой разной информацией, почерпнутой из публичного интернета, например:

- ♦ Метаданные файлов. Можно найти дату создания документа, имена пользователей, модели принтеров, ПО, установленное на компьютерах, иногда данные геолокации.

- ♦ Конфиденциальные документы. Они не должны попадать в публичный интернет, но всё же регулярно там обнаруживаются. Нужно только уметь их искать, говорят специалисты по технологиям OSINT.

- ♦ Данные о корпоративном домене. Можно узнать не только адреса электронной почты и

телефоны, но и, например, технологии, на которых построен сайт, а также криптографические сертификаты, которые используются на конкретном домене.

Кстати, технологии OSINT видятся перспективными и профессиональным разведкам. Например, Эми Зегарт, старший научный сотрудник Института Гувера, говорит в своей статье «Открытые секреты. Украина и следующая революция в разведке»: «Развитие разведывательных возможностей США для XXI века требует создания чего-то нового: специального разведывательного агентства с открытым исходным кодом, ориентированного на изучение несекретных данных и определение их значения». (Статья опубликована в новогоднем номере (2023 г.) журнала Foreign Affairs, а Владимир Овчинский сделал её перевод с комментариями для ресурса zavtra.ru.)

Здесь под агентством с открытым исходным кодом подразумевается государственная разведслужба, которая специализируется на обработке открытой информации в сети Интернет, получаемой с помощью добровольных помощников — «граждан-сыщиков».

В утилитарных целях для поиска разнообразной корпоративной информации, оказавшейся в открытом доступе, компаниям доступен широкий спектр инструментов OSINT, например:

- ♦ Shodan — поисковик по устройствам, подключённым к сети, в том числе камер видеонаблюдения, оборудования интернета вещей и др.

- ♦ Spyse — поисковик по технической информации веб-сайтов. С его помощью можно обнаружить разнообразные данные, например уязвимости, IP-адреса, субдомены и SSL/TLS.

- ♦ Опенсорсная утилита Maigret (форк программы Sherlock) проверяет наличие определённого ника (имени пользователя) на более чем 2500 сайтах.

- ♦ Foca — программа, помогающая анализировать удалённый веб-сервер.

- ♦ MaltegoMaltego — ПО, которое визуализирует собранные данные в виде дерева, выстраивающего в единую систему IP-адреса, почтовые адреса, телефоны, домены и т.д.

- ♦ Lampruge — инструмент для поиска и визуализации найденных данных со встроенными шаблонами для поиска MongoDB, анализа социальных профилей, розыска пользователей сети Интернет по их частичным идентификаторам.

КУДА ВЕДЁТ ТРЕНД ПОИСКА В ОТКРЫТОМ ИНТЕРНЕТЕ

Мощный тренд услуг поиска информации в публичном интернете подпитывает индустрию

деанонимизации. Пожалуй, наибольшую известность у нас получил телеграм-бот «Глаз Бога» (Eye Of God BOT) — он обещает поиск точных либо возможных взаимосвязей об искомом объекте по имени, телефону, адресу электронной почты, фотографии, номеру автомобиля и его окружению в соцсетях. Однако услуг такого рода гораздо больше: услуги деанонимизации составляют отдельный большой рынок.

РЫНОК ДЕАНОНИМИЗАЦИИ НА ЗАПАДЕ

Так, западный рынок услуг деанонимизации во многом построен вокруг связки параметра MAID (Mobile Advertising ID — некий ID пользователя, который не содержит его личных данных, его фиксирует практически любое приложение с рекламой на мобильном телефоне) и персональными данными пользователей (Personally Identifiable Information, PII). На сопоставлении баз данных MAID и PII специализируются многие американские компании — дата-брокеры. Самые известные из них:

- ◆ BIGDBM. Содержит более миллиарда адресов электронной почты, постоянно анализирует новые письма. Компания утверждает, что автоматическая обработка проверки актуальности электронной почты BIGDBM может увеличить успех почтовых рекламных кампаний в несколько раз.

- ◆ FullContact. 223 млрд элементов данных и профили более 275 млн совершеннолетних пользователей США — это на порядок больше, чем у российских агрегаторов.

- ◆ AGR Marketing. Данные PII могут связываться с любыми демографическими данными, правами собственности, датой рождения, ветеранскими параметрами.

- ◆ Datastream Group. Данные MAID связываются с PII и другими параметрами, например особенностями пользовательского поведения (просмотром информации на телефоне, совершением соответствующей покупки на планшете и т.д.).

- ◆ Techsalerator. Глобальная база данных потребителей Techsalerator (1 млрд записей) охватывает демографическую и контактную информацию потребителей по всему миру (249 стран) с точностью 95%.

Параметры услуг поражают воображение: от сотен миллионов до миллионов миллиардов записей (например, 100M Billion у AGR Marketing) о людях, месяцы и годы исторических данных, процент совпадений: 95–100%. И при этом вполне демократичные расценки. Например, ценник Datastream Group (900 миллионов записей, 48

месяцев исторических данных, процент совпадений — 100%) начинается с 1,90 долл.

В РОССИИ

В России рынок деанонимизации представлен так называемыми услугами пробива по базам. В январе сервис DLBI провёл ежегодное исследование этого рынка, которое включало анализ предложений почти 80 посредников, осуществляющих торговлю такого рода услугами, предоставляемыми на теневых форумах в интернете, даркнете, среде Telegram.

Выяснилось, что стоимость банковского пробива за год практически не изменилась и составляет 25,4 тыс. руб. за выписку по счетам/картам клиента за один месяц. При этом объём предложения сокращается второй год подряд — крупнейшие коммерческие банки один за другим исчезают с этого рынка в результате принятых мер по борьбе с инсайдерами. Стабильное предложение присутствует только по Сбербанку, отмечают аналитики DLBI, которому, судя по всему, пока не удаётся справиться с данной проблемой. Количество посредников, предлагающих банковский пробив, также сокращается и составляет на январь 2023 г. менее 27% от всех игроков этого криминального рынка.

Однако в целом медианная стоимость пробива всех типов выросла на 22% по сравнению с 2021 г. При этом мобильный пробив за год вырос в цене на 60% — до 27 тыс. руб. за месяц детализации звонков и СМС абонента. Причём у «Билайна», МТС и Tele2 стоимость пробива выросла в два раза и более, достигнув 15, 40 и 28 тыс. руб. соответственно, а у «Мегафона» осталась практически на прежнем уровне — 25,5 тыс. руб.

«Мы видим, как банки, хоть и после нескольких лет скандалов, занялись проблемой и добились результатов. Несмотря на то что полностью искоренить пробив невозможно, цена на него растёт, что сужает возможности преступников, — говорит Ашот Оганесян, основатель сервиса DLBI. — Также мы видим, что начали решать проблему и мобильные операторы».

ПРАВОВОЙ АСПЕКТ

У тренда деанонимизации есть существенный аспект — правовой. На Западе дата-брокеры, по сути, научились обходить требования европейского законодательства о защите персональных данных (GDPR) и американского акта CCPA (California Consumer Privacy Act), который вступил в силу в 2020 г. Правда, они стараются не афишировать свою деятельность и с этой целью предоставляют услуги исключительно по корпоративным контрактам в секторе B2B.

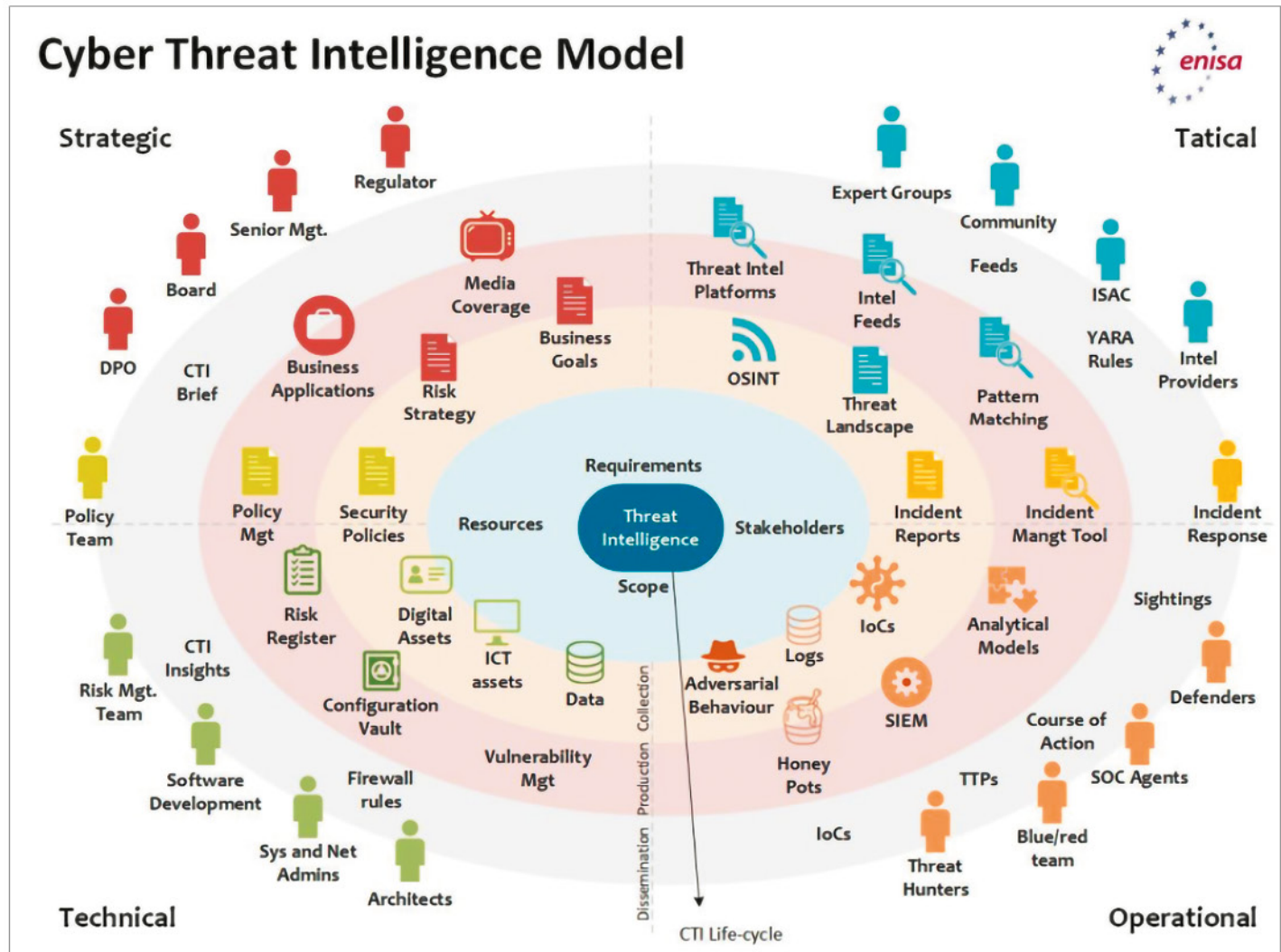


Рисунок 4. Архитектура системы Threat Intelligence, согласно стандартам ENISA (European Network and Information Security Agency — европейское агентство сетевой и информационной безопасности, ведущая организация Евросоюза, ответственная за проведение киберучений). Источник: www.anti-malware.ru, сентябрь 2022 г.

В России сервисы пробива, которые предлагаются российским клиентам, находятся в «серой» бизнес-зоне после того, как 1 марта 2021 г. вступили в силу очередные поправки к закону о персональных данных.

ПРОЗРАЧНАЯ ЭКОНОМИКА ТЁМНОГО ИНТЕРНЕТА

В даркнете работает настоящая теневая экономика, в которой действуют привычные бизнес-цепочки, состоящие из производителей товара (хакеров), оптовых покупателей и дистрибьюторов, потребителей, которые приобретают данные с целью использования их для совершения кибератак.

Согласно исследованию компании Arstechnica, опубликованному в декабре, 2158 продавцов предлагают в даркнете более 96 тыс. наименований «товаров» из украденных данных на 30 торговых площадках. Доход поставщиков за 8 месяцев 2022 г. составил более 140 млн долл. При этом на три крупнейших

торговых площадки — Apollon, WhiteHouse и Agartha — приходится 58% всех продавцов.

Доходность предприятий теневой экономики позволяет отнести их к «крепким предприятиям» среднего бизнеса, отмечают исследователи из Arstechnica. Например, доход Agartha — самой коммерчески успешной площадки — достигает 91,5 млн долл.

КАК ИСПОЛЬЗОВАТЬ ВСЕ ДОСТУПНЫЕ ДАННЫЕ?

Для обеспечения превентивного анализа угроз компаниям необходимо идти на шаг впереди злоумышленников, предвидя возможность осуществления кибератаки в недалёком будущем. На практике для этих целей предлагаются инструменты класса Threat Intelligence (TI), которые нередко называют инструментами киберразведки. Действительно, с информационной точки зрения, основа киберразведки — это знания о происходящем вокруг объекта интереса, а ПО Threat Intelligence подразумевает активный

сбор информации об угрозах как внутри ИТ-инфраструктуры, так и за пределами её периметра.

На нижнем уровне платформы ТИ находятся данные об угрозах — так называемые ТИ-фиды, то есть потоки данных, которые поступают от внешних поставщиков. Но главный результат работы системы ТИ — это аналитические суждения, помогающие специалистам компании принимать верные управленческие решения по поводу выявляемых угроз.

Аналитические возможности ТИ опираются, в частности, на формализованные знания о совершенных кибератаках, применяемых техниках и методах аналитики, например, о техническом «почерке» тех или иных АPT-группировок и профилях атакуемых компаний, а также методах вывода похищенных денежных средств. Эти знания формируются во многом за счёт мониторинга и анализа крупных теневых форумов и интернет-площадок.

С точки зрения структуры, системы Threat Intelligence принято представлять в виде трёх уровней: стратегического, операционного и тактического (рис. 4).

На стратегическом уровне решения принимают топ-руководители бизнеса и эксперты, которые оценивают всю совокупность

существующих киберугроз и их влияние на бизнес. На операционном уровне действует средний менеджмент компании — он обеспечивает выполнение поставленных задач и вносит коррективы в операционную деятельность. Здесь, в частности, используется популярный инструмент — матрица MITRE ATT&CK. На тактическом уровне представлены сведения о группировках злоумышленников и конкретные тактические приёмы, методики и процедуры, помогающие распознавать угрозы и противостоять им (рис. 5).

В декабре 2022 г. глобальная исследовательская компания Market Research Future опубликовала исследование мирового рынка решений Threat intelligence с прогнозом до 2030 г. Ожидается, что до этого времени глобальный рынок ТИ будет уверенно развиваться с двузначными цифрами роста — в среднем 15,7% в годовом исчислении.

Комплексный подход к угрозам, который реализуется в решениях Threat Intelligence, обуславливает специфические особенности внедрения и практического использования таких решений. В первую очередь речь идёт о поддержке аналитической составляющей и правильном выстраивании соответствующих бизнес-процессов.

Рисунок 5. Какие уровни Threat Intelligence реализуются в российских компаниях? Источник: онлайн-опрос www.anti-malware.ru, сентябрь 2021 г.

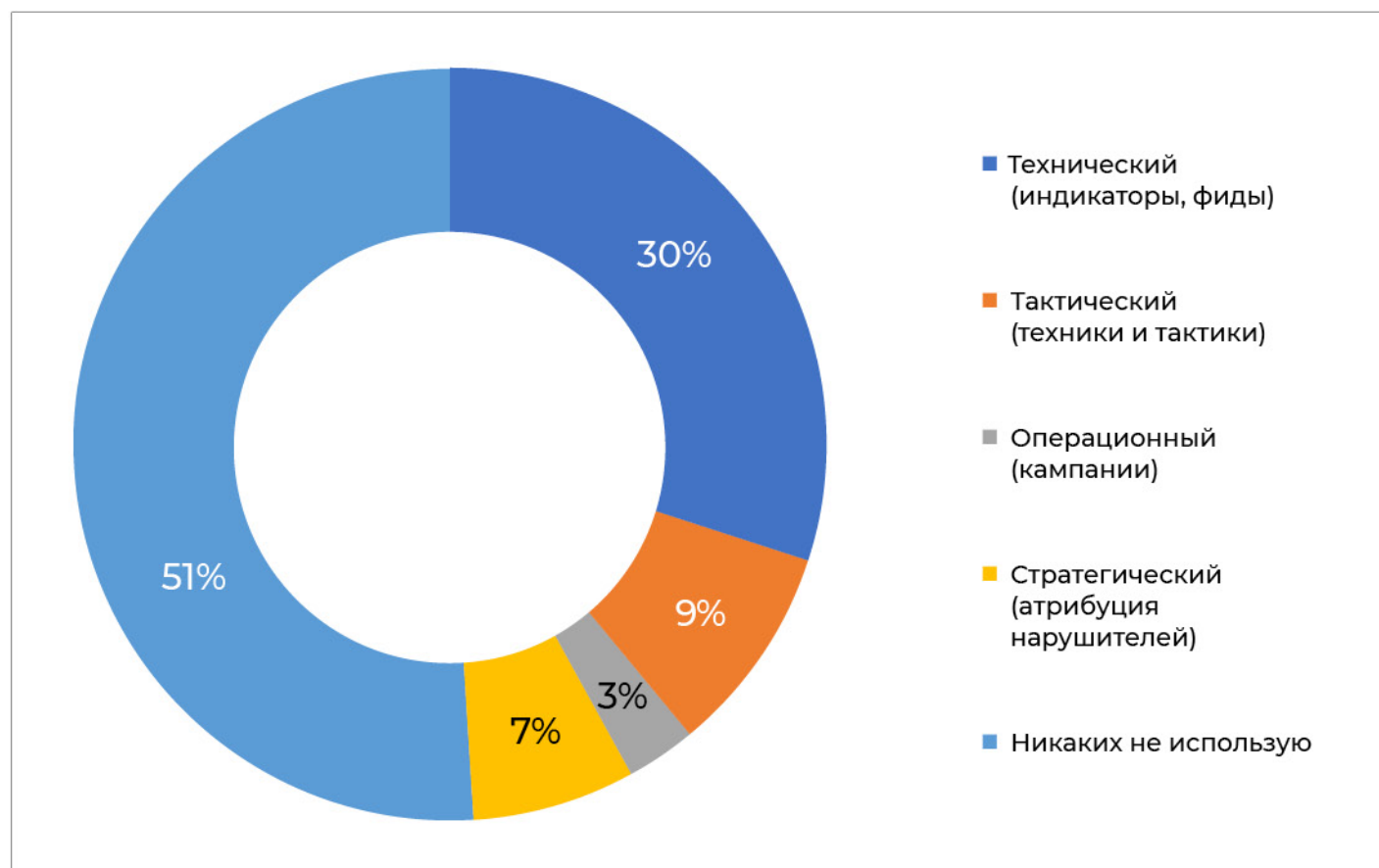


Рисунок 6.

Основные функции систем SOAR/COAP.

Источник:

www.anti-malware.ru,
2020 г.

ЭВОЛЮЦИЯ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сегодня на рынке можно найти решения и сервисы буквально по каждому направлению корпоративной безопасности, как традиционной ИБ, так и физической безопасности, а также различных аспектов безопасности бизнеса. По большому счёту, цифровизация становится неким общим знаменателем, который способен объединить разные системы технических решений информационной безопасности на логическом уровне принятия решений. Действительно, помимо киберугроз, приходящих извне, для компании имеют значение аспекты экономической безопасности (например, происки конкурентов в виде «чёрного PR», утечки базы клиентских данных), кадровой безопасности (фальшивые аккаунты ведущих сотрудников или сведения об активном поиске работы ключевыми специалистами), безопасности бренда (появление фальшивых сайтов и аккаунтов соцсетей) и т.д. Все эти сведения можно найти в разных сегментах интернета, если грамотно использовать методы киберразведки.

В конечном итоге всё уходит в некоторую цифру. Но эти «цифры» разные. Наиболее продвинутой сферой с точки зрения сбора и анализа данных является область технических решений. Например, системы класса SOAR (Security Orchestration Automation and Response Market) умеют не только интегрировать данные об

угрозах безопасности из разных источников, но и автоматизировать этот процесс (рис. 6).

По сути, традиционная ИБ превращается в Информационную Безопасность (с большой буквы), пронизывающую все аспекты безопасности бизнеса. Но сегодня мы находимся в начале этого пути — для охвата всех аспектов безопасности бизнеса в их информационной ипостаси важны, во-первых, аспекты логической интеграции разнородных данных, с точки зрения оценки соответствующих рисков и угроз. Во-вторых, связь получаемых данных с деятельностью организации: бизнес-процессами, направлениями развития бизнеса, конкурентной средой, кадровым потенциалом и т.д. При этом для полномасштабной реализации этих аспектов требуется участие человека-профессионала, и даже не одного.

Какие конкретные задачи в русле информационной интеграции решений безопасности сегодня могут решать российские организации? Какие методы и технические возможности им доступны и каких результатов позволяют добиться? Как будут выглядеть следующие шаги по автоматизации поддержки принятия решений для обеспечения безопасности бизнеса? Своими мнениями по этим вопросам с BIS Journal поделились российские эксперты.

ПРЕВЕНТИВНЫЙ УДАР

БИЗНЕС ХОЧЕТ ЗНАТЬ О ГОТОВЯЩИХСЯ КИБЕРАТАКАХ ЗАРАНЕЕ

На фоне беспрецедентного роста кибератак в 2022 году и ухода из России иностранных вендоров мы в Group-IB наблюдали повышенный (а весной и летом — просто ажиотажный спрос!) со стороны бизнеса на данные Threat Intelligence (киберразведки). Компании хотели заранее узнавать о готовящихся кибератаках, оперативно получать индикаторы компрометации и фиды, чтобы превентивно защититься от актуальных киберугроз.

БИЗНЕС ХОЧЕТ ЗАЩИТИТЬСЯ

Несомненно, «благоприятной» средой для размножения киберпреступности являются военные конфликты и сопутствующие им политико-социальные и финансово-экономические кризисы. Киберугрозой номер один для бизнеса остаются программы-вымогатели. Группы операторов шифровальщиков быстро развиваются с помощью партнёрских программ.

Второй по значимости угрозой являются стилеры — вредоносное ПО, которое похищает данные пользователей. Стоит отметить, что злоумышленники начали использовать данные со стилеров не только для совершения классических хищений денег с банковских аккаунтов, но и для поиска доступов на устройства сотрудников для дальнейшей атаки на сами компании.

Мы прогнозируем, что украденные с помощью стилеров данные станут основным способом доступа в сети атакуемых организаций. К примеру, за период с 1 июля 2021 г. по 30 июня 2022 г. в продаже было обнаружено более 280 тыс. веб-шеллов (вредоносных скриптов, которые используются злоумышленниками для управления чужими сайтами и серверами).

Подавляющее большинство утечек баз данных российских компаний, которые появлялись в 2022 году на андеграундных форумах и тематических телеграм-каналах, были выложены бесплатно в публичный доступ. На фоне текущего геополитического кризиса у киберпреступников изменился мотив: не заработать, а нанести репутационный или экономический

ущерб российскому бизнесу и его клиентам. Антирекорд 2022 года по числу утечек баз данных российских компаний в наступившем году может быть побит, а целевой фишинг и таргетированные атаки на сотрудников компаний снова будут в тренде.

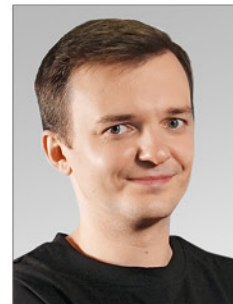
В целом, для того чтобы защититься от кибератаки, необходимо понимание, кто, с помощью каких методов и по каким причинам атакует конкретную компанию и индустрию, где она работает. И Threat Intelligence (TI) отвечает на эти вопросы, предоставляя подписчикам оперативный доступ к аналитике как о самих атакующих — финансово мотивированных хакерах, прогосударственных атакующих (APT), хактивистах, мошенниках, так и об их тактиках и инструментах.

ОТ БУМАЖНОЙ ИБ — К РЕАЛЬНОЙ

Традиционно информационная безопасность в крупных российских компаниях создавалась с учётом соблюдения стандартов и требований со стороны регуляторов. Без «бумажной» безопасности не обойтись, но на практике лучшим решением для построения эффективной ИБ является фокусировка на основных киберугрозах, которые актуальны на данный момент для региона, индустрии или самой организации. Как раз здесь помогают решения TI. Как известно, они поддерживают анализ данных в трёх разрезах: стратегическом, оперативном и тактическом.

На стратегическом уровне компании получают информацию о злоумышленниках, текущих трендах, типах атак и т.п., которые связаны с определённым регионом, индустрией или самой компанией. Обычно на этом уровне формируется ландшафт киберугроз, которые представляют опасность для организации. Всё это позволяет топ-менеджерам или CISO в компании правильно планировать бюджеты и развитие компании.

Простой пример: организация решает, где лучше открыть новый бизнес: в регионе А или регионе В? Анализируя стратегический срез информации, можно будет понять, где и какие



Дмитрий ШЕСТАКОВ
руководитель
департамента
Threat Intelligence,
Group-IB

Количество информации, полученной из darkweb, может быть очень большим и анализировать его своими силами может оказаться крайне ресурсозатратным мероприятием

атаки встречаются чаще всего, какова будет цена защиты против таких атак и прочее, чтобы не реализовывать везде одни и те же дорожные защитные меры.

На операционном уровне CISO или ИТ-команда может с помощью матриц MITRE проанализировать основные сочетания тактик, техник и процедур (TTP, Tactics, Techniques and Procedures), которые используются злоумышленниками, нацеленными на организацию, и сфокусироваться на защитных мерах именно против этих техник. Например, если компания видит, что чаще всего злоумышленники в их регионе или индустрии используют фишинговые рассылки, то, вероятно, стоит приобрести решение, которое позволит анализировать все письма и выявлять потенциально вредоносные.

Кроме того, на операционном уровне потребители ТИ узнают, например, об основных уязвимостях, которые эксплуатируют злоумышленники для атак на их индустрию. Если у компании не хватает времени или бюджета на обновление всей инфраструктуры, то, вероятно, следует сфокусироваться именно на исправлении критичных уязвимостей в инфраструктуре, которые злоумышленники используют против них.

Тактический уровень ТИ обычно связан исключительно со сбором индикаторов компрометации (IoCs). Однако его тоже можно использовать более целенаправленно, например, не сгружать все индикаторы злоумышленников, которые могут периодически фолсить (давать ложные сигналы), а использовать их только в том случае, когда вы уведомлены об атаке или ожидаете её. Например, если у вас есть информация о том, что та или иная группировка злоумышленников в данный момент начала DDoS-атаку вашей компании или смежной индустрии, то стоит обновить правила на файрволах с теми ргоху, которые обычно использует именно эта группа, а после атаки отключить лишние правила.

ИНТЕРНЕТ + DARKWEB

Одним из источников данных о текущих трендах злоумышленников и их атаках может стать

darkweb. Это понятие описывает любые ресурсы, которые используют злоумышленники для осуществления различной противозаконной деятельности. Это может быть и обсуждение уязвимостей, и продажа эксплойтов к ним, продажа баз данных, доступов, вредоносного ПО, и просто публикация данных, как делают операторы шифровальщиков. По этой причине darkweb охватывает как классические андеграундные форумы, так и андеграундные маркеты, а также интернет-мессенджеры (Telegram, Discord, Jabber) и иные ресурсы, которыми пользуются злоумышленники.

Своевременное получение данных об угрозах из этих источников очень полезно. Например, злоумышленники часто используют андеграундные форумы для продажи доступов к корпоративным сетям. В недавнем аналитическом отчёте «Эволюция киберпреступности. Анализ, тренды и прогнозы 2022/2023» отмечается, что Group-IB обнаружила 380 брокеров по продаже доступов к скомпрометированной инфраструктуре компаний, которые опубликовали более 2300 предложений на даркнет-форумах. Самыми активными были злоумышленники под никами Novelli, orangecake, Pirat-Networks, SubComandanteVPN, zirochka — их предложения в сумме составили 25% от всего рынка продажи доступов.

Своевременное использование подобных данных позволяет предотвратить дальнейшее проникновение и шифрование инфраструктуры компании.

Другой пример — получение информации о текущих трендах и потенциальных новых атаках. Например, в ходе текущего кризиса на многих специализированных площадках злоумышленники обсуждали уязвимости, которые были найдены в тех или иных компаниях, и делились ими. Кроме того, тренд на новые DDoS-атаки также зародился в андеграунде.

Информация об утечках в других компаниях также может быть крайне полезной, учитывая, что это могут быть компании-интеграторы, которые разрабатывали то или иное ПО для внутренних информационных систем компании. Информация о подобных атаках должна быть сигналом команде ИБ внутри компаний для проверки, где и какое ПО используется и не могли ли у скомпрометированной компании остаться какие-либо доступы к внутренним системам.

Отдельно отмечу, что количество информации, полученной из darkweb, может быть очень большим и анализировать его своими силами может оказаться крайне ресурсозатратным

мероприятием. Поэтому использование такой системы ТИ, которая предоставляет компании ещё и экспертизу аналитиков, способных найти в этом объеме данных угрозы именно для этой компании, может сильно упростить построение системы безопасности и своевременное реагирование на внешние угрозы.

Для большей сфокусированности своего ИБ-подхода также можно использовать информацию из darkweb. Так, если ТИ сообщает вам об угрозах в виде различных вариантов предоставления конфиденциальной информации из ваших систем, то необходимо нацелить свои силы на борьбу с инсайдерскими угрозами и разграничение прав доступа.

В целом ключевую функциональность решений ТИ можно описать на примере Group-IB Threat Intelligence:

- ♦ выявление фактов взлома компаний благодаря мониторингу преступных групп, бот-сетей и теневого интернета;
- ♦ обнаружение недетектируемых атак с помощью уникальных индикаторов компрометации;
- ♦ атрибуция, приоритизация угроз и более быстрое реагирование за счёт данных об атакующих, их инструментах и тактиках;
- ♦ создание правил корреляции и детектирования угроз, специфичных для их клиентов, за счёт оперативных бюллетеней о новых угрозах, вредоносных кампаниях и группах;
- ♦ оптимизация процесса управления уязвимостями за счёт сведений об активно эксплуатируемых уязвимостях, наличии эксплойтов, обсуждений на хакерских форумах. Все данные собраны в подробные профили уязвимостей;
- ♦ обогащение индикаторов компрометации и используемых средств защиты с помощью встроенных аналитических инструментов, например Graph и Malware Detonation Platform.

АВТОМАТИЗАЦИЯ АНАЛИТИЧЕСКИХ ПРОЦЕССОВ

Человек будет оставаться ключевой фигурой при принятии решений о реакции на ту или иную угрозу. Однако сбор и оценку угроз можно автоматизировать, чтобы упростить человеку-аналитику дальнейшую обработку потенциального инцидента.

Обычно все данные киберразведки привязаны к определённой группировке, которая, кстати, может состоять из одного человека. Для сопоставления данных с той или иной группировкой используется идея о том, что отдельные злоумышленники в своей деятельности используют схожие TTP, вредоносное ПО и т.д., что и позволяет классифицировать их в отдельные блоки.

Данный подход очень удобен, так как позволяет фокусировать внутреннюю безопасность против специфичных угроз, а не всех сразу.

Для обогащения и консолидации таких данных используются ТИ-платформы: аналитики ТИ постоянно изучают новые атаки, инструменты и атрибутируют их в отношении тех или иных злоумышленников. Например, если в атаке на ту или иную компанию был обнаружен новый троян удалённого доступа (RAT), то обычно для управления таким ПО необходимы C2-сервера инфраструктуры управления и контроля. Под новые вредоносы можно написать YARA-правила (описание сигнатур целевых атак и вторжений в ИТ-инфраструктуру организации) для процесса хантинга (то есть создания правил корреляции путём анализа скрытых или ранее неизвестных индикаторов и признаков атаки) на них. Поскольку настройка и установка серверов также происходит схожим образом у разных групп, это позволяет написать правила для хантинга и на них. В результате это даёт возможность аналитикам ТИ узнавать об угрозах заранее и уведомлять об этом своих клиентов.

ОСНОВНАЯ ЦЕЛЬ

Надо подчеркнуть, что основная цель ТИ заключается в том, чтобы предоставлять данные проактивно. А для этого необходимо знать об атаках ещё до момента их совершения. С этой целью можно использовать разные способы.

Например, нашим аналитикам и клиентам доступен аналитический инструмент «Граф», который изначально создавался для автоматизированного графового анализа сетевой инфраструктуры злоумышленников. Эта система собирает большой массив данных о состоянии глобальной сети в разные моменты времени и позволяет выявлять скрытые связи между различными элементами. На данный момент система агрегирует данные из различных источников ТИ и других продуктов, что позволяет строить более сложные связи и, что более важно, — выявлять различные паттерны, которые используют злоумышленники. Благодаря этим паттернам мы можем выявлять новые управляющие C2-сервера и другие индикаторы, которые могут помочь предотвратить атаку ещё до её совершения.

Основная цель ТИ заключается в том, чтобы предоставлять данные проактивно. А для этого необходимо знать об атаках ещё до момента их совершения



**Владимир
Ульянов**
аналитик
по кибербезопасности

«НА УРОВНЕ ОРГАНИЗАЦИИ КИБЕРРАЗВЕДКА НЕЦЕЛЕСООБРАЗНА»

НА УРОВНЕ КОРПОРАТИВНОЙ ИБ

Если размышлять о том, каким образом повысить осведомлённость специалистов компании о происходящем в сфере корпоративной ИБ, стоит принимать во внимание ряд соображений.

Во-первых, роль человеческого фактора. Часто именно люди становятся тем фактором, который приводит к краже или компрометации корпоративных данных. Поэтому повышение именно их осведомлённости должно стать одним из обязательных инструментов ИБ. Причём работу следует вести по нескольким направлениям сразу. С одной стороны, рассказывать об угрозах ИБ, о методах, используемых злоумышленниками, о том, как их можно избежать, как проверять получаемую информацию. С другой стороны, информировать об ответственности за утечку информации, об использовании средств контроля информационных потоков. Вместе это должно удерживать от неблагоприятных поступков как халатных сотрудников, так и нелояльный персонал, готовый сливать данные.

Во-вторых, не стоит преувеличивать значение данных, добываемых с помощью технических систем, например, за счёт анализа ресурсов darknet и открытого интернета — всего того, что сегодня называют киберразведкой.

Киберразведка — это специфическая деятельность, требующая ресурсов и особых компетенций от сотрудников. На практике она не всегда целесообразна и часто не окупается. По крайней мере, не для каждого вендора и не для каждого сегмента. Если же говорить о борьбе с внутренними угрозами, гораздо полезнее будет информация из курилки. Ежедневная деятельность специалистов по ИБ не требует глубокого погружения в тему киберразведки и постоянного мониторинга даркнета. Даже если это

реализовать, не будет много пользы от полученной информации.

Гораздо интереснее выглядит идея объединения сведений из различных источников в рамках центров реагирования на киберугрозы, к которым подключено значительное число крупных организаций. Вероятность довести нужные сведения до целевого адресата в этом случае будет гораздо выше.

В-третьих, помимо киберугроз, приходящих извне, для компании имеют значение различные аспекты экономической безопасности. Идея объединения разных аспектов безопасности под единым «зонтиком» одной системы вполне логична: смешение функциональности продуктов различных классов и даже размытие границ самих классов представляется мне естественным в стремлении обеспечить комплексную защиту корпоративных ресурсов.

ВЕКТОР ИНТЕГРАЦИИ СИСТЕМ

Сегодня стоит говорить о векторе создания экосистем для обеспечения безопасности от различных угроз. Никаких методологических препятствий для этого я не вижу. Наоборот, это правильно, поскольку помогает выстраивать бесповоротную защиту, обогащать данные, а использование общих архивов данных ещё и позволяет экономить на создании и обслуживании хранилищ.

Это не только даёт единый для всех продуктов интерфейс и политики безопасности, но и в некоторых случаях обеспечивает синергический эффект. Как, например, использование DLP и DСАР-систем: от них можно получить пользу и по отдельности, но лишь совместно они дадут полную картину использования корпоративных данных, а также помогут защитить их от широкого спектра внутренних угроз.

Что касается конкретной конфигурации технического решения, предназначенного для сбора информации о различных угрозах, она будет разной для разных организаций. Вряд ли можно предложить универсальный набор, который закрывал бы все потребности разных компаний и при этом не был избыточным для тех или иных организаций. Высокая стоимость не только самих инструментов ИБ, но и особенно

Киберразведка — это специфическая деятельность, требующая ресурсов и особых компетенций от сотрудников. На практике она не всегда целесообразна и часто не окупается

их эксплуатации неприемлема для многих компаний и требует избирательного подхода к выбору средств.

О ПРОБЛЕМАТИКЕ ДАННЫХ

Отдельный вопрос — структурирование потоков разнородных исходных данных, приходящих из различных источников. Технически можно объединить потоки под одной оболочкой, но собранные в рамках киберразведки сведения сами по себе являются очень разными, не всегда понятна их применимость, а потому будет затруднено и структурирование данных. Здесь одна из ключевых проблем — формализация самой информации. Плюс консолидация и взаимное обогащение данных.

Обогащение данных — один из трендов корпоративной безопасности — часто используется для получения дополнительной информации. В данном случае сопоставление может происходить на базе любых идентификаторов, адресов, событий, географии и др.

Однако сам выбор полезных потоков данных (фидов) представляет собой отдельную задачу. Я уверен, что только опыт может дать ответ, какие полезны, а какие нет. Причём это зависит не только и не столько от самих фидов, сколько от организации, их использующей, профиля её деятельности, сценариев использования. То, что будет полезным для одних, может оказаться ненужным для других. При этом я бы предостерег от сбора избыточных данных, подписки на множество источников, особенно при ограниченности собственных ресурсов. Специалисты просто не будут успевать обрабатывать полученную информацию. Можно привести пример с подписками в мессенджерах: вначале радуется обилие полезных каналов, но в какой-то момент перестаёшь их отслеживать, и вся информация уходит мимо.

ПРО АВТОМАТИЗАЦИЮ ИНТЕГРИРОВАННОЙ АНАЛИТИКИ

При всех достижениях в области сбора и обработки данных из различных источников человек остаётся важнейшим компонентом системы анализа всех собираемых данных, особенно в случаях, когда обрабатывается плохо формализуемая информация. Однако полагаться только на возможности человека нельзя, ведь объёмы получаемой информации часто превосходят ресурсы обычного специалиста, с учётом кросс-задач, усталости и других человеческих факторов. Поэтому оптимальный подход предполагает автоматизацию базовых рутинных процессов и интеллектуальную работу специалистов.

А для обеспечения оперативной реакции на выявленные потенциальные угрозы нужно выполнить несколько базовых условий:

- а) отработанные правила реагирования для различных ситуаций;
- б) корректно настроенные автоматизированные сенсоры, которые бы создавали тревожные оповещения (alerts);
- в) квалифицированные специалисты, наделённые нужными полномочиями.

Этого во многих случаях будет достаточно.

СПЕЦИФИКА ВНЕДРЕНИЯ АНАЛИТИЧЕСКИХ РЕШЕНИЙ

Специфические особенности организации сказываются, в частности, на внедрении аналитических решений безопасности в существующую структуру ИТ-систем. Более того, вряд ли при этом можно говорить о каких-либо типовых решениях. Условно «типовые» системы — это скорее удел слаборазвитых систем корпоративной безопасности. А в большинстве организаций — свои системы и свои подходы к её обеспечению. Так, для крупного рознично-ориентированного бизнеса и небольшой производственной компании результаты работы аналитических систем и вложений в киберразведку могут кардинально различаться.

Внедрение аналитических, да и любых других, компонентов в уже выстроенную экосистему почти всегда будет нетривиальной задачей. Возможно, удастся отказаться от некоторых избыточных и дублирующих компонентов, но это не будет просто даже на уровне переучивания персонала, который с ними работает. Более того, на практике встречаются ситуации, когда некоторые классы корпоративной ИБ, имеющие схожую функциональность, продолжают работать в общей среде. Это всё — издержки насыщения инструментами безопасности корпоративных сетей и использования продуктов разных разработчиков. А в отдельных случаях дублирование выстроено намеренно для повышения общей устойчивости системы.

Аналитические решения сложно отнести к классу утилитарных инструментов, коими являются многие продукты корпоративной безопасности. Их внедрение говорит об особом подходе, который принимает организация. Поэтому в большинстве случаев потребуются изменения в регламентах и квалифицированные кадры для работы. Эффективными же они могут быть, если организация ясно представляет, какую информацию планирует собирать и как её использовать. В противном случае вся затея может оказаться пустой или даже обременительной тратой денег.

«В ЗАВТРАШНЕМ МИРЕ БУДЕТ ТОЛЬКО ОДНА БОЛЬШАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УПРАВЛЯЕМАЯ ИИ»



Вячеслав ПАНКРАТЬЕВ
заведующий
кафедрой
безопасности
Университета
государственного
и муниципального
управления,
полковник юстиции
в запасе

Понятие информационной осведомлённости (awareness), которое появилось в области управления ИТ-рисками и информационной безопасности, всегда имеет прикладной характер. В рамках аналитической работы на уровне обеспечения безопасности бизнеса основная задача — понять, что будет происходить завтра, какие планы имеются у тех или иных сторон, организаций, персон в отношении конкретной компании. Сложность этой задачи связана, в числе прочего, с тем, что повышение уровня осведомлённости не сводится к простому увеличению объёмов информации, доступной для анализа и прогнозирования. Более того, сегодня область ИБ всё больше включает в себя защиту от манипулирования данными, фейков, недостоверной информации, то есть защиту ОТ информации.

В целом информатизация в той или иной степени проникла во все системы безопасности, и уже можно говорить о том, что все направления безопасности бизнеса сливаются в одну большую Информационную Безопасность. Но есть нюансы.

СЛОЖНОСТИ МНОГОУРОВНЕВОЙ ИНТЕГРАЦИИ

Обеспечение безопасности бизнеса — это процесс стратегического уровня. По большому счёту, он включает две составляющие:

- ♦ требования безопасности, предусматриваемые законодательством (ответственный за пожарную безопасность, ответственный за антитеррор, ответственный за промышленную безопасность и т.д.);

- ♦ риски для юридического лица. Управление рисками организации — это внутрикорпоративный процесс, осуществляемый советом директоров, менеджерами и другими работниками. Он начинается в ходе разработки стратегии развития бизнеса и затрагивает всю деятельность организации.

Если рассматривать безопасность как бизнес-функцию, то в системе риск-менеджмента экономической безопасности предприятия технические и технологические риски (аварии, сбои, устаревшее оборудование, нарушение технологий и т.д.) — это только один из видов

рисков. Помимо него, есть ещё солидный перечень рисков, включающий, в частности:

- ♦ экономические (макроэкономические риски, связанные с экономикой страны и мира, зависимость от импорта, пандемия, ориентировка на экспорт и т.д.);

- ♦ политические (административный ресурс, взаимоотношения с государственными контролирующими и правоохранительными органами, принятие политических решений, государственная монополизация отдельных отраслей, санкции, импортозамещение и т.д.);

- ♦ юридические (изменение законодательства, оформление разрешительных и правоустанавливающих документов, первичная приватизация, условия договора и т.д.);

- ♦ предпринимательские (взаимоотношения с контрагентами, конкурентами, изменение спроса и предложения, локдауны и т.д.);

- ♦ финансовые и инвестиционные (отсутствие финансирования, валютные риски, кредиты, налоги, штрафы, дебиторская задолженность и т.д.);

- ♦ информационные и репутационные (разглашение информации, недостоверная информация, отсутствие информации, манипулирование, чёрный PR, информационное противоборство, риски, связанные с ИТ и ИБ и т.д.).

В части риск-менеджмента есть и направление, связанное с разведкой и аналитикой, — анализ надёжности контрагентов и безопасности коммерческих предложений. В этой области решаются задачи конкурентной разведки, включая предвидение изменений на рынке, предвидение действий конкурентов, изучение их успехов и неудач, сбор компромата, выявление новых или потенциальных конкурентов, предоставление руководству информации для проведения переговоров, мониторинг изменений в политической, законодательной и регулирующей областях, влияющих на бизнес, изучение новых инструментов управления.

Система управления рисками строится на базе методик анализа. Их разработано немало: SWOT-анализ (Strengths, Weaknesses, Opportunities, Threats), PEST-анализ (Political, Economic, Social, Technological), PESTLE (PEST плюс юридический и экологический анализ), STEEPLED (PESTLE плюс образовательный и

демографический анализ), диверсионный анализ, предполагающий моделирование нежелательных явлений, анализ сценариев, опирающийся на стратегию развития компании, и др.

Важно понимать, что в области ИТ развиваются процессы автоматизации управления рисками. Есть соответствующие программные средства, в том числе российские.

Так, на нашем рынке представлены ИТ-решения для автоматизации антикоррупционных мероприятий: вычисление конфликтов интересов, аффилированности, личных выгод, откатов, автоматизации закупок, проверки контрагента, противодействия утечкам корпоративных данных (DLP) и т.д. Все они относятся к области информационной безопасности и представляют собой даже не отдельную часть безопасности бизнеса, а конкретные инструменты. Бесспорно, там тоже идёт постоянное развитие, поскольку появляются новые технические решения.

Скажем, на сцену выходит цифровой рубль, он поменяет правила игры в финансовой сфере, и отрасль ИБ будет активно заниматься безопасностью этого цифрового рубля. Раньше охрана периметра объектов была выстроена, грубо говоря, вокруг забора, окружающего этот объект, а сегодня в небе летает всё больше БПЛА, способных решать разные задачи: от разведывательных до диверсионных. Соответственно, появляется ещё одна подсистема сбора и обработки данных в системах безопасности. Когда в компаниях появятся квантовые компьютеры, ИБ-решения будут развиваться исходя из этого.

Однако возможности объединения различных направлений безопасности бизнеса на базе «общего знаменателя» — цифровых данных — в высокоуровневую ИТ-систему обеспечения безопасности бизнеса сегодня весьма ограничены. Пожалуй, в качестве попытки реализации такого подхода можно рассматривать ИТ-системы управления рисками класса SOAR (Security Orchestration, Automation and Response), предназначенные для оркестровки систем безопасности, то есть координации их совместной работы.

ПРО АВТОМАТИЗАЦИЮ

Успехи в цифровизации различных аспектов безопасности бизнеса сформировали общий тренд — внедрение развитых умных технических решений, которые дают возможность удалить из операционных процессов человека. И это неплохо получается. Скажем, человек может анализировать одновременно до 10 мониторов с информацией, а для технических

средств никаких ограничений нет. Для обоснования выбора того или иного поставщика умная программа может проанализировать огромные объёмы данных, неподъёмные для человека. И это в корне меняет процессы, например, торгов и конкурсов, где по традиции — сплошная коррупция. Пусть ИИ выбирает, кто будет поставлять гвозди на стройку. По крайней мере, не будет вопросов об откатах, аффилированности и т.п.

Но здесь есть важный нюанс — он связан с поддержкой принятия решений. ИБ не занимается информационной поддержкой принятия решений. Этим занимается специалист по информационно-аналитической работе, использующий разные методы анализа. Автоматизация его работы в части поддержки принятия решений — вот наш завтрашний день.

Думаю, что в нашем завтрашнем информационном мире будет только одна большая Информационная Безопасность, управляемая искусственным интеллектом, а все остальные блоки безопасности бизнеса станут её частями. Можно предположить, что многие специалисты по безопасности останутся без работы, а остальным придётся активно изучать информационную безопасность. И здесь, кстати, главным коррупционером будет вовсе не лицо, принимающее решения. Главный коррупционер — ай-тишник, который будет настраивать этот искусственный интеллект для правильного принятия решений.

ГЛАВНЫЙ ВЫЗОВ ТЕКУЩЕГО МОМЕНТА

Несмотря на то что область ИБ развивается быстро и за ней — будущее в поддержке принятия аналитических решений, главный вызов сегодня лежит не в сфере сбора и обработки данных, а в изменении структуры и содержании рисков безопасности бизнеса. Фактор СВО переназначил риски и приоритеты.

Яркий пример: сегодня для рынка стала менее актуальна тема террористических рисков и законодательства по противодействию терроризму, потому что идёт движение в сторону совсем другого закона — о военном положении, где применяется понятие не теракта, а диверсии.

Вот это, пожалуй, можно назвать главным трендом корпоративной безопасности 2022 года — безопасность перестраивается с учётом реальной ситуации. Тогда, образно говоря, для предприятия ОПК гораздо важнее не сорвать гособоронзаказ, чем выбрать наилучшего контрагента в отношении антикоррупционного комплаенса. Также

существенно повысился приоритет непрерывности бизнес-процессов: пусть контрагент далёк от идеала, но если других нет, то надо работать с ним, потому что это позволит обеспечить непрерывность бизнес-процессов.

В русле изменения приоритетов корпоративной безопасности меняется и нормативно-законодательная база. Все нормативы позапрошлого года в 2022-м уже не работали. Практически все документы по безопасности либо переделывались, либо перестали работать, и временно включалось «ручное управление».

Так, с сентября прошлого года произошёл ряд изменений в законодательстве о персональных данных (ПД). В частности, из закона о ПД исключили большинство случаев, когда организациям не нужно уведомлять Роскомнадзор о намерении начать обрабатывать ПД, усилены обязанности оператора в случае компрометации ПД. С 1 марта 2023 г. изменяется порядок трансграничной передачи ПД — о таких ситуациях требуется уведомить Роскомнадзор.

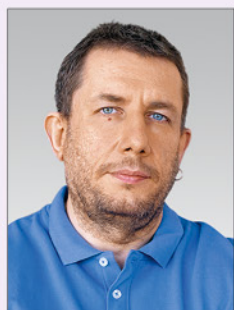
В связи с мобилизацией и добровольным содействием СВО произошли изменения в кадровой работе. Так, в Трудовом кодексе РФ появилась новая статья 351.7 — «Особенности обеспечения трудовых прав работников, призванных на военную службу по мобилизации или поступивших на военную службу по контракту...». Претерпела изменения система

контроля за персоналом: теперь контроль осуществляется не по процессам, а по результатам. Идёт тенденция на увеличение гражданско-правовых отношений с физическими лицами и уменьшение трудовых отношений. Различия существенные: если трудовые отношения предполагают выполнение трудовой функции в рабочее время, то гражданско-правовые отношения — это оказание услуги (выполнение задач) в поставленные сроки.

В части противодействия коррупции в 2020–2022 гг. появилось законодательство о цифровых финансовых активах — они приравнены к имуществу и подлежат декларированию в справках о доходах-расходах, вышли методические документы Минтруда РФ по противодействию коррупции в закупках, принят Национальный план по противодействию коррупции на 2021–2024 гг., создана государственная информационная система «Посейдон».

КОРПОРАТИВНАЯ БЕЗОПАСНОСТЬ В БЛИЖАЙШЕМ БУДУЩЕМ

К чему приведут изменения, происходящие сегодня в сфере корпоративной безопасности? Это нам ещё предстоит узнать. Всё будет зависеть и от результатов СВО, и от макроэкономических условий, которые сложатся на момент окончания СВО. Можно только выделить два важных момента.



Ашот ОГАНЕСЯН
основатель
сервиса разведки
утечек данных
и мониторинга
даркнета DLBI

БИЗНЕС ПОПАЛ... В «НОЖНИЦЫ» УГРОЗ

Идею интегрированного и суперглобального подхода к киберугрозам можно отнести скорее к категории мечтаний ИБ-специалистов, которые хотят не просто заполучить новые бюджеты, но и перейти от обеспечения защиты своих работодателей к бесконечному изучению окружающих ландшафтов, исключаяющему ответственность за реальное положение дел.

ПОСМОТРИМ ПРАВДЕ В ГЛАЗА

А перед российской ИБ-отраслью сегодня стоит огромная и насущная проблема: СВО и появление украинского «хактивизма» показали, что реальный уровень защиты информационных систем оказался крайне невысоким,

особенно для тех средств, что были на него затрачены.

Вушедшем году мы увидели, что сети крупнейших российских компаний, банков и госведомств ранее были защищены не столько закупленными за астрономические деньги ИТ-решениями, сколько известной неформальной договорённостью «не работать по .RU». Но после отмены этой договорённости оказалось, что средства защиты часто не могут противостоять банальному password reuse, а социальная инженерия легко «пробивает» не только рядовых сотрудников, но и айтишников и даже самих специалистов в области информационной безопасности.

При этом одновременно резко усилилось регуляторное давление — появились требования

Во-первых, цифровизация безопасности будет продолжаться. Вопрос в том, с помощью каких средств и чьего производства мы будем это делать.

Во-вторых, мир сейчас вступил в полосу неопределённости, где плюсы и минусы разных ситуаций запросто меняются местами. А это значит, что придётся строить управление безопасностью в условиях динамического хаоса и неопределённости. Хаос здесь понимается как математический аппарат, описывающий поведение нелинейных динамических систем.

Надо сказать, что мир вступил в эпоху хаоса и неопределённости ещё в пандемийном 2020 году: тогда было непонятно, когда закончится пандемия, какова её глубина и возможный размах. Было сложно просчитать решения, принимаемые государственными органами, административные запреты и ограничения менялись практически каждый день. Компаниям требовалось принимать управленческие решения, в том числе в части корпоративной безопасности в условиях неопределённости. Управление безопасностью в таких условиях означает, в частности, что предприятие работает в отсутствии долгосрочных планов.

Следует отметить, что в условиях хаоса значительные изменения претерпевают системы контроля, функции которых часто берёт на себя безопасность. Классические системы

контроля процессов и регламентов становятся неэффективными в связи с быстро меняющейся обстановкой. На первый план выходит контроль выполненных задач, а также контроль и управление изменениями (трансформациями).

В условиях хаоса и неопределённости как никогда большое значение имеет оперативный доступ к информации и умение её анализировать. В современном мире, как отмечалось ранее, наблюдается переизбыток ненужной информации, в связи с чем специалисты по безопасности концентрируют усилия на верификации и оценке информации, особенно той, которая будет использована для принятия управленческих решений. В состоянии динамического хаоса время жизни информации очень мало, поэтому период, отведённый для её проверки, становится предельно малым. Мониторинг и оценка информации в реальном режиме времени — это уже не экзотическая прихоть, а жизненная необходимость каждой компании.

В числе наивысших приоритетов оказывается способность быстро ориентироваться в ситуациях и принимать (менять) решения в зависимости от обстановки. Происходит переход от планирования к постановке задач, ключевое значение приобретают антикризисные планы (планы действий в чрезвычайных ситуациях, действий при наступлении определённых событий, мобилизационные планы и т.д.).

к раскрытию информации об атаках на критическую инфраструктуру, приготовились вводить оборотные штрафы за утечки персональных данных и многое другое, что сделало действия злоумышленников действительно болезненными для участников рынка. В процессе, в частности, выяснилось, что сами компании чаще всего могут зафиксировать только факт атаки и практически никогда не понимают, оказалась ли она успешной и что именно и в каком объёме попало в руки взломщиков.

В результате попавшему в эти «ножницы» бизнесу приходится одновременно с попыткой защитить данные искать уже случившиеся утечки и пытаться выкупать их у взломщиков, а также закрывать уязвимости, связанные с использованием этой информации для дальнейшего проникновения в свои системы.

РЕАЛЬНЫЙ ДРАЙВЕР

Это, действительно, резко увеличило спрос на системы мониторинга интернета и даркнета,

в том числе такие, как наш сервис DLBI (Data Leakage & Breach Intelligence), предназначенный для разведки уязвимостей данных, а также мониторинга утечек в даркнете и на хакерских ресурсах. Однако нужно отдавать себе отчёт, что реальный драйвер этой ситуации — никакой не новый уровень ИБ в компаниях, а фактическая неработоспособность большинства существующих систем.

Нет никаких оснований считать, что в ближайшем будущем ситуация улучшится. Число хакерских атак не демонстрирует тенденции к снижению. Одновременно приходится импортозамещать многие ИБ-решения, делать это второпях и в условиях уменьшившихся бюджетов. Кроме того, на криминальный рынок возвращаются украинские мошенники, формирующие спрос на хищение персональных данных, особенно баз финансовых организаций. В условиях непростой экономической ситуации и снижения доходов населения это подхлестнёт и инсайдерские утечки.

«КИБЕРРАЗВЕДКА ПОМОГАЕТ ЗАКРЫТЬ МНОЖЕСТВО ИБ-ЗАДАЧ»



Алексей ПАВЛОВ

директор по развитию бизнеса центра противодействия кибератакам Solar JSOC компании «РТК-Солар»

Чтобы построить эффективную защиту организации, необходимо понять, какой уровень квалификации может соответствовать атакующей стороне и какие техники и тактики могут использовать злоумышленники. Важную роль в этом играет киберразведка, помогающая организации взглянуть на себя глазами киберпреступника.

КЛАССИКА

Исходя из квалификации злоумышленника, киберзащиту организации можно разделить на несколько уровней. Базовый уровень включает исследование собственного периметра и уязвимостей на нём (Vulnerability Management, VM), повышение осведомлённости сотрудников о киберугрозах (Security Awareness, SA) и тестирование на проникновение (пентест). Таким образом компания сможет защититься от двух самых популярных методов проникновения: фишинга и эксплуатации уязвимостей.

Если компания уверена, что на неё направляется целевая атака, то базовый уровень стоит дополнить CPT (Continuous Penetration Testing). Это более продвинутый вариант VM, позволяющий проверить применимость и актуальность конкретного вектора атак. Ещё один важный инструмент — OSINT, то есть разведка по открытым источникам. Она позволит нивелировать риски, связанные с утечками баз данных, скомпрометированными аккаунтами, адресами электронной почты и т.п.

Также для выявления сложных атак с использованием ВПО стоит подключить Sandbox, а обычный SA дополнить Assumed Breach, то есть проверкой навыков ИБ-команды через имитацию атаки злоумышленника определённого уровня.

А для защиты от группировок, действующих в интересах иностранных государств, и сложных АРТ-атак потребуются полноценные тренировки команды защиты в части противодействия внешним злоумышленникам (Red Teaming, Purple Teaming, Киберучения), а также организация собственной команды исследования угроз.

ИНСАЙДЕРЫ И УТЕЧКИ

Параллельно с классической историей защиты существует и тематика защиты от инсайдера,

экономическая безопасность и проблематика защиты бренда. Если говорить про инсайдера и защиту от утечек, то на помощь организациям приходят решения класса DLP. А для защиты бренда, что крайне важно в контексте репутации, можно использовать системы и сервисы классов DRP, ASM, OSINT.

КИБЕРРАЗВЕДКА. ВЕЕР ВОЗМОЖНОСТЕЙ

Глобально киберразведка помогает закрыть множество ИБ-задач. Эта тематика затрагивает не только интересы информационной безопасности, но и экономическую, и даже HR. Главное — определить, какие задачи нужно решить с помощью разведки.

Например, можно защищать клиентов компании, выявляя и блокируя фишинговые сайты, или выявлять уязвимости на периметре с помощью Shodan и оперативно закрывать их. Можно искать утечки баз данных, выявляя вектор утечки в рамках расследования инцидента, или находить скомпрометированные утечки, принудительно меняя их пароли, чтобы минимизировать вероятность атаки через эти данные, или искать фейковые аккаунты топ-менеджеров в социальных сетях. Наконец, с помощью киберразведки можно мониторить новостной фон и отслеживать негатив в отношении бренда. Последнее стало особенно актуально в 2022 году, который показал, что информационные сбросы иногда имеют больший резонанс, чем реальная ситуация. Основная проблема сейчас связана с поиском утечек, ведь отличить компиляции старых слитых данных или фейковые базы от реальных сложно.

КЛЮЧЕВОЙ ЭЛЕМЕНТ

Ключевой элемент — это экспертная команда. Без профессиональных аналитиков корректно проанализировать собранные данные не получается. В будущем наверняка появятся инструменты автоматизации, но в ближайшие два-три года ключевым фактором всё равно останутся люди. Причём квалификация для OSINT, форензики, SOC совершенно различна. По аналогии со стоматологами: удаляют зубы, ставят пломбы, проводят сложные операции разные специалисты, хотя общее название профессии у них одно.

«ЭВОЛЮЦИЮ НЕ ОСТАНОВИШЬ, А ПОКА... «ТИ РАДИ ТИ», ЧТО НЕ РАЦИОНАЛЬНО»

ТЕНДЕНЦИЯ К УКРУПНЕНИЮ

В последнее время и в России, и в мире наметилась тенденция на укрупнение ИТ-решений безопасности. Так, в конце прошлого года Gartner выявила тенденцию к формированию «нового» класса решений — TDIR (Threat Detection and Incident Response).

Однако с технической точки зрения TDIR — это скорее эволюция текущих наиболее востребованных ИБ-технологий: TI, SIEM, SOAR, UEBA и EDR. Здесь речь идёт не столько о появлении каких-то «новых» фиш в отдельно взятых технологиях, сколько об ином, более совершенном подходе к обеспечению кибербезопасности — созданию экосистем, где все технологии, объединяясь под единым «зонтиком», глубоко интегрированы между собой. Иными словами, простота и прозрачность доступа к технологиям для конечного потребителя возведены на новый уровень.

За счёт такой интеграции и тесной взаимосвязи внутри экосистемы технологии обогащают друг друга дополнительными функциональными возможностями по аналитике, обнаружению, реагированию, расследованию и комплексному управлению ИБ. «Зонтиком» в рамках экосистем может выступать единая консоль управления или супер-апп, которые скорее пока являются дополнительным бонусом. Но, так или иначе, к этому все придут.

ТИ В ПРОЦЕССЕ СОЗРЕВАНИЯ

В настоящее время в русле обсуждаемой идеи активно продвигаются решения класса Threat

Intelligence (TI). Применительно к ним зачастую внимание акцентируется на практических аспектах формирования наборов данных для TI. Так, иногда встречаются рекомендации использовать инструменты open source для самостоятельного создания фидов. Но если в ИБ-штате организации нет достаточного количества сотрудников, способных воспользоваться знаниями об угрозах, то идею с open source желательно отложить до лучших времён и сфокусироваться на коммерческих фидах, а также поиске удобной аналитической TI-платформы.

«Серебряной пули» здесь не существует. В первую очередь важно исходить из реальных аналитических возможностей пользователя этих данных, потому как «ТИ ради ТИ» — это не самый рациональный подход к процессу.

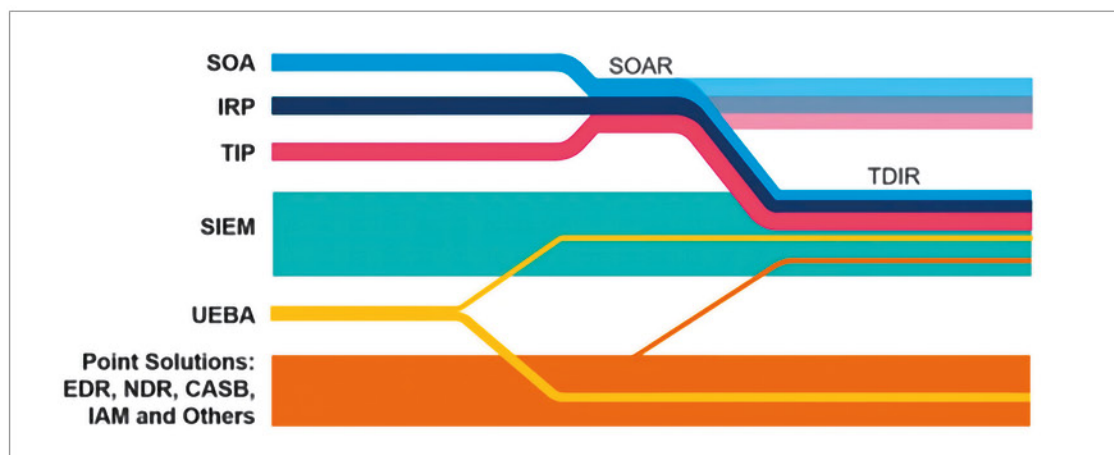
При этом сегодня TI обычно воспринимается как массивы IoC (индикаторов компрометации) и редко рассматривается как что-то большее. Но уже в прошлом году стала намечаться тенденция к применению знаний об угрозах не только на уровне массивов IoC (технический уровень), но и в виде более зрелых подходов к противодействию, основанных на анализе методов работы злоумышленника (тактический уровень).

В ближайшем будущем должна получить развитие практика использования «стратегического TI», в основу которого заложен анализ огромной базы знаний, что позволяет отслеживать тренды и общую картину изменения угроз с течением времени и, исходя из этой информации, анализировать свои возможности.



Григорий РЕВЕНКО

директор центра экспертизы компании R-Vision



«НЕЛЬЗЯ РАЗДЕЛЯТЬ ИБ И IT-OPERATIONS»



Василий ГУРЬЕВ
руководитель
проекта IT Man
(ГК Softline)

Идея создания такой конфигурации ИТ-решений, которая способна обеспечить осведомлённость об угрозах всех типов, вполне реализуема на практическом уровне. В частности, есть работоспособная концепция сбора и совместного анализа соответствующих данных. Она уже апробирована рынком и подтверждает свою эффективность. Суть концепции заключается в том, чтобы объединить данные ИТ-инфраструктуры в одном источнике, из которого они будут поступать для решения бизнес-задач ИТ- и ИБ-департаментов. В основе такого решения — единая платформа, которая соберёт данные и сможет управлять конечными точками. Она может выступать источником достоверной информации для ИТ и ИБ, обеспечивать полноту картины информации об ИТ-инфраструктуре, а также молниеносный ответ на изменение в инфраструктуре для ИТ и ИБ.

КЛЮЧЕВАЯ ПРОБЛЕМА

Такой подход решает ключевую проблему согласования данных ИТ и ИБ. Действительно, пока ИТ и ИБ пользуются разными инструментами, проблема рассинхронизации данных и дублирования никуда не уйдёт, а при использовании единой платформы этого можно избежать. На сегодняшний день это лучшая концепция, её развивают все международные компании, которые так или иначе обеспечивают управление ИТ и ИБ. Пример — решения класса Security Intelligence.

В данном случае Security Intelligence — это концепция, предполагающая возможность собирать данные из разных источников, объединять их и анализировать для целей ИТ и ИБ. Уже есть решения, которые в одном месте самостоятельно собирают данные не только с ИТ-инфраструктуры, но и из различных узлов программного обеспечения, например из файлов, и далее нормализуют и анализируют показатели. Для целей анализа на рынке уже

«ВСЯ БЕЗОПАСНОСТЬ ПОД ОДНИМ «ЗОНТИКОМ» — МЕЧТА ЛЮБОГО ВЕНДОРА. НО ЕСТЬ НЮАНСЫ»



Андрей АРЕФЬЕВ
директор
по инновационным
проектам
ГК InfoWatch

Основная трансформация ИБ на предприятиях связана с изменением ИТ-ландшафта, которое происходит в рамках импортозамещения. Поэтому, на мой взгляд, приоритетом всех отечественных компаний в течение ближайших лет будет адаптация к этому новую ИТ-ландшафту, то есть поиск адекватных ИБ- и ИТ-инструментов для обеспечения безопасности и функционирования предприятий и наработка приёмов работы с ними. Может ли стать таким искомым инструментом система, способная объединить разные аспекты безопасности бизнеса под единым «зонтиком» одной системы или платформы?

Действительно, интернет как среда обитания достаточно агрессивна: социальная инженерия,

кража брендов и их копирование, продажа продукции, похожей на бренды, в нелегальных местах и т.п. — все эти проблемы присутствуют и относятся к области деятельности юристов и экономической безопасности. Объединение большого количества решений в рамках одной платформы и создание набора решений, который закроет 100% проблем заказчиков, — это, наверное, мечта любого вендора. Но есть нюансы.

Во-первых, на мой взгляд, такой подход находится вне зоны интереса компаний-потребителей, потому что использование продуктов только одного вендора обуславливает своего рода зависимость, и в любой форс-мажорной ситуации заказчик может оказаться в ситуации

представлено множество инструментов, для сбора данных решений меньше, но они тоже есть.

СТРУКТУРИРОВАНИЕ ПОТОКОВ

Один из важных элементов искомого подхода — структурирование потоков разнородных исходных данных, приходящих из различных источников. В этой части на сегодняшний день есть четыре задачи.

Первая — нормализация данных. Например, в базе название программного продукта может быть как на русском, так и на английском языке, также могут различаться версии ПО. Для принятия качественных управленческих решений данные должны быть нормализованы.

Вторая — идентификация данных и узлов, то есть технологических ИТ-активов. Она так же решается системами сбора данных и другими способами, в том числе с применением машинного обучения.

Третья задача возникает на стыке двух предыдущих — поддержание стабильности работы процесса по нормализации входящих данных, их идентификация и объединение. Для этого используются решения, основанные на CASE-методах (Computer-Aided Software Engineering) автоматизации проектирований различных

Пока ИТ и ИБ пользуются разными инструментами, проблема рассинхронизации данных и дублирования никуда не уйдет, а при использовании единой платформы этого можно избежать

информационных систем. Они показывают высокий уровень производительности, правда, в процессе работы теряют эффективность. Для того чтобы нивелировать этот недостаток, применяется искусственный интеллект.

Так, согласно опыту применения средств iT-Map, потеря эффективности производительности составляет в среднем за год 40%, а при использовании искусственного интеллекта — 7%. И это без внесения дополнительных изменений в нормализацию, идентификацию активов. Соответственно, если не использовать искусственный интеллект, понадобятся затраты человеческих ресурсов на поддержание системы идентификации и нормализации данных.

Четвёртая задача — связывание неструктурированных данных. Так, при поступлении информации об одном активе её объединяют

утраты безопасности значительной степени. Ставка на моновендора с точки зрения ИБ неразумна. Гораздо правильнее использовать разные стеки решений, в том числе потому, что это осложняет процессы проникновения для злоумышленников и делает компанию более стабильной с точки зрения независимости от одного производителя.

Во-вторых, необходимость анализа даркнета можно существенно снизить, если использовать в целях защиты знания о том, каким образом корпоративные данные попадают на тёмную сторону интернета.

Так, типовой проблемой, с которой сталкиваются крупные компании, является употребление пользователями одинаковых паролей на разных ресурсах, утечки которых (связка логин/пароль) случаются у публичных сервисов, а базы данных с ними размещаются в даркнете. Поэтому первое, что делают злоумышленники, — покупают такие базы данных и пытаются использовать подобные скомпрометированные пароли, применяя их к корпоративным учётным записям. С точки зрения киберразведки,

их использование может приводить к тому, что киберпреступники получают доступ к корпоративным ресурсам. Конечно, при условии, что такие учётные данные одинаковы или похожи.

Также можно воспользоваться подбором по шаблону: если видно, какой шаблон для паролей пользователь применяет повсеместно, не составит труда подобрать сходный пароль к корпоративным ресурсам. Взлом учётных записей — это одна из основных угроз.

Ещё одна угроза — поиск злоумышленниками конфиденциальной информации в результате утечки баз данных из ERP- и CRM-систем или файловых хранилищ. Для служб информационной безопасности такие утечки — это обратная сторона, то есть возможность своевременно предпринять нужные меры. Если есть сведения, что пароль их сотрудника утёк из публичного сервиса, это позволит проинформировать персонал о необходимости его смены.

В любом случае анализ происходящих событий связан с обработкой потоков разнородных исходных данных. Для них уже есть специальное понятие — фид, производное от data feed,

Для эффективного встраивания аналитических решений безопасности в общую структуру необходима система, которая является единым источником информации, основой для сбора данных и управления изменениями в инфраструктуре

с изменениями, которые произошли в другой системе. Например, время старта изменений на одной конфигурационной единице, действия в другой системе и эффект на той же самой конфигурационной единице через определённый промежуток времени. В системах Business Intelligence задача по связыванию неструктурированных данных уже частично решена.

ЕДИНЫЙ ИСТОЧНИК ИНФОРМАЦИИ

В итоге все усилия по обработке данных из различных источников нужны для работы аналитических ИТ-решений. Для эффективного встраивания аналитических решений безопасности в общую структуру необходима система,

которая является единым источником информации, основой для сбора данных и управления изменениями в инфраструктуре, воздействия на внешние системы. Только при её наличии надо начинать строительство всех бизнес-систем и бизнес-решений.

РАБОТА ДВУХ КОМАНД

Компании необходимо сделать аналитическую систему основой, которая собирает данные с инфраструктуры и предоставляет их дальше инструментарию обработки либо сама является платформой, на базе которой можно построить инструменты для ИТ и ИБ. Это потребует внесения изменений в понимание, как надо обеспечивать комплексную безопасность на предприятии: нельзя разделять информационную безопасность и ИТ-operations, отделять их друг от друга. Это всегда совместная работа двух команд: ИТ и ИБ.

Если разделять два этих отдела, появится дублирование и рассинхронизация данных. Если департаменты будут закупать решения и инструменты отдельно друг от друга, это будет малоэффективно для бизнеса. То есть приоритетная необходимость — исключить отсутствие взаимодействия между подразделениями ИТ и ИБ.

обозначает поток информации, например, об уязвимостях или фишинговых сайтах. То есть фид представляет собой относительно структурированную информацию о каких-то проблемных артефактах.

В интернете существуют наборы платных и бесплатных сервисов, предоставляющих фиды, готовые для использования. При этом важно понимать, что при сборе данных о вредоносных сайтах полезно опираться на несколько независимых источников для того, чтобы не стать заложником качества одного источника. Я бы рекомендовал комбинировать сервисы. Если компания дозрела до того уровня, что сама анализирует фиды и принимает решения на основе анализа этих данных, то, возможно, есть смысл оперировать несколькими независимыми источниками. Это позволит получать более объективную оценку.

Однако для того, чтобы собирать фиды из даркнета, нужно обладать большим экспертным опытом, иметь специально раскрытые учётные записи, которые используются для доступа к определённым ресурсам в даркнете. Если

у компании есть бюджет на подобные цели, то использование сервисов по покупке фидов — это более оптимальный вариант.

В ситуации покупки фидов важно использовать такие ИТ-решения, в которые вы сможете интегрировать информацию, полученную из фидов. Иными словами, автоматизированная система, которая понимает в результате анализа, что пользователь пытается перейти на сайт, находящийся в списке вредоносных, и сама блокирует такие попытки, будет эффективнее, чем человек-аналитик, которому приходится принимать решения вручную. Конечно, при этом нужно правильно конфигурировать ИТ-системы с тем, чтобы они самостоятельно принимали технические решения на основе данных и действий пользователей, информируя об этом ответственные службы. Человек, в свою очередь, на основе этой информации сможет актуализировать фиды, либо работать с их качеством, либо работать с качеством принятия решений. Это тот способ, с помощью которого можно решать вопрос угроз.

«БЕЗ НАДЁЖНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ДАННЫЕ ДАРКНЕТА БУДУТ БЕСПОЛЕЗНЫ»

О том, что в новых условиях (особенно после начала СВО) меняется модель угроз и поведение служб безопасности в целом, мы говорили на BISummit в сентябре. Выяснилось, что компании, которые полноценно подготовились в области ИБ, достойно выдержали массированные атаки и не понесли значительного ущерба. При этом их специалисты ИБ не увидели каких-то революционных действий злоумышленников, кроме повышенной активности и изменения пропорций в традиционной картине событий.

Можно ли улучшить состояние ИБ в компании, если использовать системы киберразведки применительно к darknet и открытому интернету? Давайте разберёмся.

ЭКСПЕДИЦИИ НА ТЁМНУЮ СТОРОНУ

Термин «киберразведка», ставший в последнее время популярным, на мой взгляд, включает два уровня. На первом компании, специализирующиеся на ИБ, исследуют угрозы интернет-среды и действия киберпреступников, потенциально опасные для государства и бизнеса. А на втором сотрудники ИБ обычной компании пытаются внедриться в сообщества даркнета, чтобы узнать, например, о споре на закрытые данные своей компании и их наличии на чёрном рынке. С одной стороны, это позволяет зафиксировать утечки данных, выследить инсайдера, проверить уровень защищённости предприятия, а с другой — оценить вероятность будущих атак.

При правильной постановке задачи и высоком профессионализме исполнителей «экспедиции в даркнет» позволяют получать важную информацию, помогающую повысить защищённость компании. Однако нужно понимать, что прежде чем начинать поиск информации в даркнете, стоит изучить открытые данные об актуальных угрозах и уязвимостях. Кроме того, без постоянно обновляемой и хорошо контролируемой системы безопасности полученные на тёмной стороне данные будут просто бесполезны. Поэтому нужно начинать именно с создания такой системы, а уже потом регулярно проверять уровень её защищённости, руководствуясь полученной, в том числе и в даркнете, информацией.

ПРО ИНТЕГРАЦИЮ

Что касается возможности связать всё «защитное ПО» в одну платформу и использовать её в качестве универсального «зонтика». Следует уточнить, что речь идёт не обо всех средствах защиты информации, которые входят в состав классической системы ИБ, а именно о средствах анализа получаемой информации. Также надо понимать, что есть системы, анализирующие чисто техническую информацию (контролируют состояние софта, детектируют попытки подбора пароля), а есть ПО, «заточенное» на смысловые события, как, например, наша DLP-система InfoWatch Traffic Monitor. Она анализирует поведение сотрудников, работая со смысловой компьютерной информацией. Это принципиально разные задачи.

Я предложил бы аналогию с положением различных подразделений служб безопасности в оргструктуре компаний. Где-то службы ИБ, физической охраны и контроля доступа объединены в одно подразделение, а где-то они образуют разные департаменты, но у каждой есть свои технические и ИТ-средства для выполнения своих служебных обязанностей.

Так может обстоять дело и с аналитическими системами. Лично я не стал бы собирать все подобные системы в единую платформу, поскольку их специализация имеет значение. Но если вдруг кто-то захочет создать нечто универсальное, то получившаяся в результате система наверняка будет иметь модульную архитектуру, поскольку ей придётся работать с различными по своей сути событиями и источниками данных. Пожалуй, есть только одно исключение — надстройка над большим количеством разнородных систем для ситуационных центров масштаба региона, отрасли и т.п.



Михаил СМЕРНОВ
директор
экспертно-
аналитического
центра
ГК InfoWatch

При правильной постановке задачи и высоком профессионализме исполнителей «экспедиции в даркнет» позволяют получать важную информацию, помогающую повысить защищённость компании



Анатолий АКСАКОВ
депутат Государственной Думы РФ,
председатель Комитета
Государственной Думы
по финансовому рынку



СВОЕВРЕМЕННЫЕ МЕРЫ

БОРЬБА С СОЦИАЛЬНОЙ ИНЖЕНЕРИЕЙ ВСТУПИЛА
В ЗАВЕРШАЮЩУЮ СТАДИЮ

В IS Journal попросил Анатолия Аксакова подвести итоги 2022 года и наметить перспективы законотворческой деятельности в 2023 году.

ОБ ИЗМЕНЕНИЯХ В ФЕДЕРАЛЬНЫЕ ЗАКОНЫ

— Анатолий Геннадьевич, в конце 2022 года произошло несколько важных событий. Во-первых, создание УБК

МВД РФ, а также внесение изменений в Федеральный закон «О банках и банковской деятельности» позволили банкам и правоохранительным органам оперативно реагировать на преступления в финансовой сфере.

Во-вторых, по инициативе Банка России рассматриваются изменения в ФЗ «О банках и банковской деятельности», которые дадут банкам право блокировать перевод

денежных средств на счета мошенников, несмотря на согласие отправителя. Этот проект закона уже получил положительное заключение правительства, ведутся работы по проработке формулировок статей для исключения двойного толкования.

Расскажите, пожалуйста, в чем состоят изменения в ФЗ «О банках и банковской деятельности»? Какой механизм борьбы с фродом и социальной инженерией они создают?

— Во-первых, да, действительно, Президентом подписан Федеральный закон от 20.10.2022 № 408-ФЗ «О внесении изменений в статью 26 Федерального закона „О банках и банковской деятельности“ и статью 27 Федерального закона „О национальной платежной системе“, который создает условия для автоматизированного обмена данными между Банком России и МВД России, что позволит объединить усилия указанных ведомств в борьбе с кибермошенниками.

Закон будет способствовать повышению скорости расследования дел по фактам мошенничества при денежных переводах. Сейчас при рассмотрении таких дел значительное время уходит на запросы данных и переписку между правоохранительными органами и банками. Закон предусматривает подключение МВД к автоматизированной системе ФинЦЕРТ Банка России, в которой содержится информация об операциях, проведенных без согласия клиентов. Благодаря этому правоохранительные органы смогут практически в онлайн-режиме получать сведения о мошеннических операциях, в том числе о получателях похищенных денег. Обмен данными будет происходить с соблюдением всех норм банковской тайны. МВД России будет передавать в базу ФинЦЕРТ сведения о совершенных противоправных действиях. Банки — участники информационного обмена, в свою очередь, смогут учитывать эти данные в своих бизнес-процессах для предотвращения мошеннических переводов.

Закон вступит в силу через год, в октябре 2023 года, а до этого момента регулятор и министерство заключат двустороннее соглашение, в котором будут определены виды сведений, порядок, сроки и формат их передачи, а также интегрируют информационные системы.

О БЛОКИРОВКЕ СРЕДСТВ

Во-вторых, в Государственную Думу внесен проект федерального закона № 197920–8 «О внесении изменений в Федеральный закон «О национальной платежной системе» (в части совершенствования механизма противодействия хищению денежных средств)».

Согласно указанному законопроекту в целях улучшения действующих механизмов антифрода предлагается обязать не только банк плательщика (как это установлено сейчас), но и банк получателя средств проводить обязательную антифрод-процедуру, т.е. осуществлять проверку операций на признаки мошенничества, включая сверку с базой данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, которую ведет Банк России.

Кроме того, в связи с тем, что у граждан похищают денежные средства чаще всего методами социальной инженерии, при которой лицо самостоятельно переводит деньги мошеннику, предлагается предоставить банкам право не принимать к исполнению распоряжения по явно мошенническим операциям в течение 2 дней, даже несмотря на наличие согласия клиента (в случае, если оператор по переводу денежных средств получил от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, указывающую на операцию без согласия клиента). Как правило, за 2 дня клиент осознает, что деньги перечисляются мошеннику.

Также у банка получателя появляется право приостанавливать использование клиентом электронного средства платежа (ЭСП), если такой клиент или используемый ЭСП находится в базе данных Банка России.

Дополнительно вносятся уточнения в части особенностей операций по переводу денежных средств с использованием платежных карт при проведении кредитными организациями антифрод-мероприятий, позволяющие не приостанавливать операции без согласия клиента, а осуществлять проверку на признаки операций без согласия клиента на этапе до приема к исполнению распоряжения клиента.

Данный законопроект был разработан в тесном сотрудничестве с Банком России и кредитными организациями, полагаем, что он находится в высокой степени готовности. Конечно, ко второму чтению будут некоторые поправки, но, учитывая актуальность темы, мы рассчитываем на его принятие в весеннюю сессию 2023 г.

О ТЕЛЕФОННОМ МОШЕННИЧЕСТВЕ

— Как нам стало известно, проведена и большая работа по борьбе с телефонным мошенничеством. Во-первых, планируется внести изменения в Федеральный закон «О связи» для быстрого и эффективного реагирования на звонки мошенников. Изменения в законодательстве, которые вступили или вступят в силу, обяжут операторов связи верифицировать все звонки в сети, а структурам МВД РФ позволят оперативно получать информацию от банков.

Во-вторых, с января 2023 г. вступили в силу изменения в ст. 13.2.1 КОАП РФ, которые вводят штрафы для операторов связи, не исполнивших обязанности по подключению к системе обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования. Оператор будет обязан передавать абонентам реальные номера звонящих.

В-третьих, согласно изменениям в Федеральный закон «О связи» в обязанности оператора связи войдет необходимость передавать Минцифры всю цепочку связи для установки нарушителя. Планируются также введение уголовной ответственности за нарушения данного закона, аннулирование лицензий. Среди прочих мер рассматривается возможность прекращения обслуживания номеров иностранных граждан при окончании сроков на право пребывания в стране — с номеров,

зарегистрированных на таких абонентов, также поступает много поддельных звонков.

Расскажите, в чем состоят изменения в ФЗ «О связи»? Какой механизм борьбы с фродом и социальной инженерией они создают?

— В настоящее время в Комитете по финансовому рынку ведется активная работа по подготовке текста ко второму чтению законопроекта № 514780–7 о создании информационной системы проверки сведений об абоненте.

Данный законопроект был разработан при активном участии Минцифры России, Банка России и участников финансового рынка в целях обеспечения возможности для любой финансовой организации проверить факт принадлежности конкретного номера мобильного телефона конкретному физическому лицу — клиенту финансовой организации, который клиент использует для дистанционного взаимодействия с финансовой организацией, а также для выявления событий, свидетельствующих о возможной попытке злоумышленника использовать номер телефона клиента для хищения его денежных средств в рамках исполнения требований Федерального закона № 161-ФЗ «О национальной платежной системе».

До сих пор доступ к таким сведениям на основании прямых договоров с отдельными операторами связи имеет лишь узкий круг банков (менее 30), в то время как остальные финансовые организации такого доступа не имеют вследствие избранной операторами связи ценовой политики.

ЕИС ПСА

Для системного решения задачи по противодействию совершению правонарушений с использованием средств связи Законопроектом предусматривается дополнение Федерального закона «О связи» новой статьей 44.3, регулирующей создание Единой информационной системы проверки сведений об абоненте — физическом лице и о пользователях услугами связи абонента — юридического лица либо индивидуального предпринимателя (ЕИС ПСА).

В рамках ЕИС ПСА предлагается установить обязанность операторов подвижной радиотелефонной связи сообщать уполномоченным государственным органам, перечень которых и цели использования которыми ЕИС ПСА прямо закрепляются в законе (это Банк России, Минцифры России, ФСБ России, МВД России и Росфинмониторинг), а также на платной основе кредитным организациям, операторам платежных систем, операторам услуг платежной инфраструктуры, операторам услуг информационного обмена, некредитным финансовым организациям и бюро кредитных историй 7 видов информации:

- ♦ о состоянии идентификационного модуля, в том числе о факте его замены на пользовательском (оконечном) оборудовании абонента,
- ♦ о факте подключения (включения и (или) выключения) абонентом переадресации голосовых вызовов,
- ♦ о факте смены пользовательского (оконечного) оборудования абонента и т.д.

Важно отметить, что в процессе функционирования ЕИС ПСА никакие персональные данные передаваться не будут.

Идентификация клиента — абонента будет производиться по номеру телефона.

В целях защиты информации, передаваемой с использованием ЕИС ПСА, Законопроект включает положения:

- ♦ о запрете получения пользователями ЕИС ПСА, том числе государственными органами, информации в целях, прямо не предусмотренных Законом о связи;
- ♦ о запрете получения финансовыми организациями информации о физических и юридических лицах, не принятых ими на обслуживание;
- ♦ о запрете хранения информации оператором ЕИС ПСА сведений, передаваемых с использованием системы;
- ♦ о полномочиях Минцифры России по согласованию с ФСБ России, ФСТЭК России и Банком России определять перечень угроз безопасности персональных данных, актуальных в случае передаче персональных данных в ЕИС ПСА.

Важно отметить, что ЕИС ПСА сразу создается в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций, что позволит минимизировать затраты всех участников на интеграцию с ней. Оператор ЕИС ПСА будет определен Правительством Российской Федерации.

Банк России также получает полномочие устанавливать случаи обязательной проверки сведений через ЕИС ПСА (это полномочие вступит в силу с 01.01.2024).

Одновременно для операторов связи и финансовых организаций сохраняется возможность получения сведений аналогичных содержащихся в ЕИС ПСА на основании прямых договоров с операторами связи.

ОБ УТЕЧКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

— Ожидается увеличение штрафов за утечку персональных данных. Сегодня за утечку данных предусмотрен максимальный штраф в размере 75 тыс. руб. согласно ст. 13.11 КоАП РФ. Минцифры подготовило законопроект об оборотных штрафах для компаний за утечку персональных данных — до 3% от оборота. Эти меры должны мотивировать компании вкладывать средства в инфраструктуру РБ до киберинцидента.

На какой стадии находится данный законопроект? Какой механизм действий предполагает?

— Данный законопроект пока не внесен в Государственную Думу и находится на согласовании в Правительстве РФ.

Он направлен на усиление защиты персональных данных граждан нашей страны. На проработку этого вопроса дано поручение Президента — до 1 июля 2023 года рассмотреть вопрос об установлении оборотных штрафов в отношении компаний, допускающих утечку персональных данных, а также усилить ответственность за их незаконный оборот.

По моему мнению, введение оборотных штрафов является весьма своевременной мерой, учитывая реальный урон, который наносят утечки персональных данных. И здесь государство безоговорочно встает на сторону граждан, защищая их права.



Сергей КОРЕЛОВ
НКЦКИ



Алексей НОВИКОВ
НКЦКИ

ТРЕНДЫ И КЛЮЧЕВЫЕ ОСОБЕННОСТИ

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ В 2022 ГОДУ

Мы вступили в непростое время, когда результаты работы по обеспечению безопасности информации проходят настоящее испытание. В этой статье обсуждаются вызовы, с которыми пришлось столкнуться в 2022 году, и уроки, которые были извлечены.

Ситуация, с которой пришлось столкнуться, конечно, развивалась не на пустом месте. Чтобы понять, как изменился ландшафт угроз в 2022 году, вначале необходимо упомянуть те тенденции, в рамках которых развивались в 2021 году угрозы и механизмы их реализации.

ТЕНДЕНЦИИ-2021

Скорость реализации угроз. Первая тенденция — скорость реализации угроз. От момента появления сведений об угрозах, например, публикации сведений об уязвимостях программного обеспечения до их практической реализации проходит не более нескольких часов. И очевидным подтверждением тому служат возникавшие и продолжающие возникать случаи появления критических уязвимостей массово используемого программного обеспечения. Сведения о них появлялись в публичном доступе либо практически одновременно с их массовой эксплуатацией, либо вообще после целого ряда инцидентов, произошедших в результате эксплуатации этих уязвимостей.

Совершенствование методов. Следующая тенденция — совершенствование применяемых злоумышленниками средств и методов. Вносит свой вклад в дело вооружения и оснащения злоумышленников повышающаяся доступность инструментария. Регулярными стали публикации исходников средств проведения атак даже уровня АРТ. Кроме того, фактически сформировалось направление предоставления инструментария в рамках сервисной модели. Таким образом, сформированы условия, ког-

да злоумышленники могут быстро (иногда очень быстро) получать действенные средства проникновения в информационные системы.

Повышение уровня квалификации. Ещё одна тенденция — это повышение уровня квалификации злоумышленников. Можно констатировать, что злоумышленники учатся, повышают свою квалификацию, проводят анализ инцидентов, сведения о которых появляются в различных источниках. Если посмотреть на атаки, совершённые с использованием шифровальщиков с целью получения выкупа, то их эволюция наиболее заметна. Год-два назад схема таких атак была проста: злоумышленники пробили периметр, загрузили шифровальщик туда, куда смогли, и ждут выкупа. Сегодня их действия в большинстве случаев намного сложнее. Чтобы увеличить вероятность получения выкупа, они проводят исследование инфраструктуры, определяют наиболее чувствительные для организации ресурсы, анализируют саму информацию, ищут резервные копии. Таким образом, приходится иметь дело со злоумышленником, постоянно совершенствующим свои навыки и средства. И в этой ситуации главная задача — не отстать.

Получение выкупа. Нельзя не упомянуть о том, кто же интересовал злоумышленников. Одним из трендов 2021 года явились атаки, направленные на получение данных, в том числе с последующим использованием шифровальщиков, для получения выкупа. В качестве целей злоумышленники выбирали платёжеспособные организации, в которых шифрование данных может нарушить функционирование основных бизнес-процессов и которые в состоянии заплатить за непубликацию похищенной информации.

Атаки на госсистемы. Ещё одним трендом 2021 года явилось увеличение количества атак на государственные информационные системы. Здесь интерес злоумышленни-



Рисунок 1. Цели атак

ков был направлен на добывание информации. По данным Национального координационного центра по компьютерным инцидентам (НКЦКИ), например, при регистрации в зоне gov.ru нового почтового домена третьего уровня первые целевые специально подготовленные фишинговые атаки начинаются уже в течение нескольких дней.

Интерес к промышленным системам. Всё больший интерес АPT-группировок фиксировался к промышленным системам. И это понятно. В современном мире многие страны уже открыто заявляют о разработке наступательных операций в киберпространстве, создании соответствующих подразделений и оснащении их необходимыми средствами. В этих условиях, конечно, объекты критической информационной инфраструктуры (далее — КИИ), которыми являются объекты промышленности, будут их объектами интереса. Поэтому попыток проникновения с целью организации плацдармов на будущее, отработки способов выведения из строя и сбора интересующих сведений о функционировании объектов КИИ нужно ждать постоянно.

Атаки через цепочку поставщиков. Ещё одной тенденцией явилось заметное увеличение количества атак через цепочку поставщиков. Это и интеграторы, и производители средств защиты, и поставщики услуг, и иные деловые партнёры. Этот фактор в том числе связан с предыдущей тенденцией разработки наступательных операций в киберпространстве.

ТЕНДЕНЦИИ-2022

Тенденции 2022 года начали проявляться уже после 24 февраля. При этом ландшафт угроз и цели (см. рисунки 1–3) в целом практически не претерпели изменений. Эти изменения коснулись в основном повышения интенсивности атак и «широты охвата».

НОВОЕ

В целом все отмеченные тенденции сохранились. Добавились некоторые новые. Проявления вредоносной активности, с которыми столкнулся НКЦКИ в этом году:

- ♦ массированные атаки на корневые DNS-сервера;
- ♦ отключения провайдеров от крупных магистральных каналов;
- ♦ встраивание вредоносного программного обеспечения (далее — ВПО) в широко используемые элементы веб-страниц;
- ♦ массовые отзывы сертификатов;
- ♦ прекращение функционирования целого ряда средств защиты зарубежных производителей;
- ♦ появление вредоносного кода в обновлениях программного обеспечения (как свободно распространяемого, так и коммерческого);
- ♦ а также другие условно «традиционные» атаки.

DDoS-АТАКИ-2022

Например, DDoS-атаки. Их особенностью в 2022 году стало по-настоящему большое количество участников. Участвовали в атаках обычные пользователи со всего мира. Хорошо отлаженные механизмы привлечения обычных людей к проведению атак на российские информационные ресурсы работали эффективно. В кратчайшие сроки были сформированы телеграм-каналы, в которых проводилась агитация, инструктажи участников, координация и целеуказание. В этих же каналах активно распространялись инструменты проведения атак. То, что ещё недавно продавалось за деньги или распространялось в закрытых сообществах, стало доступно массово для использования в атаках.

Была развёрнута серьёзная инфраструктура для проведения таких атак, например сайты-редиректы, позволявшие

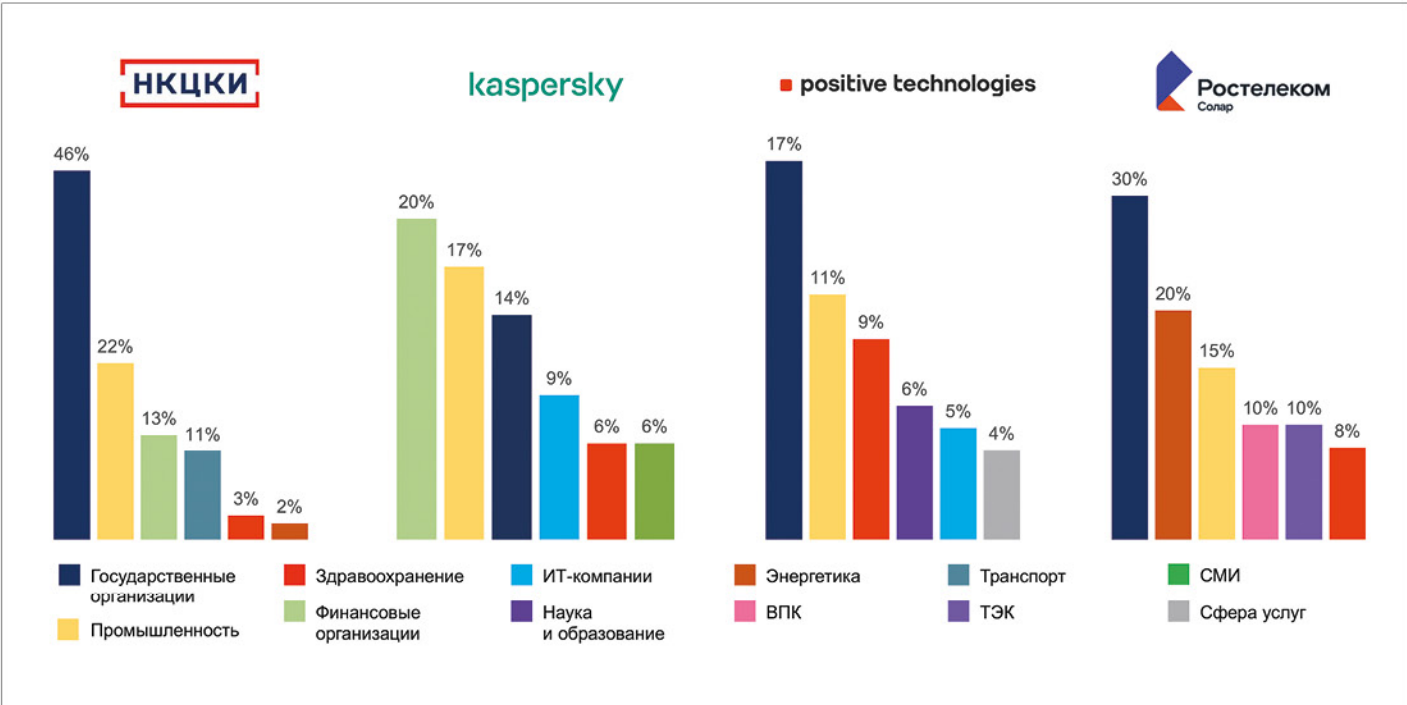


Рисунок 2. Цели атак — инфраструктуры

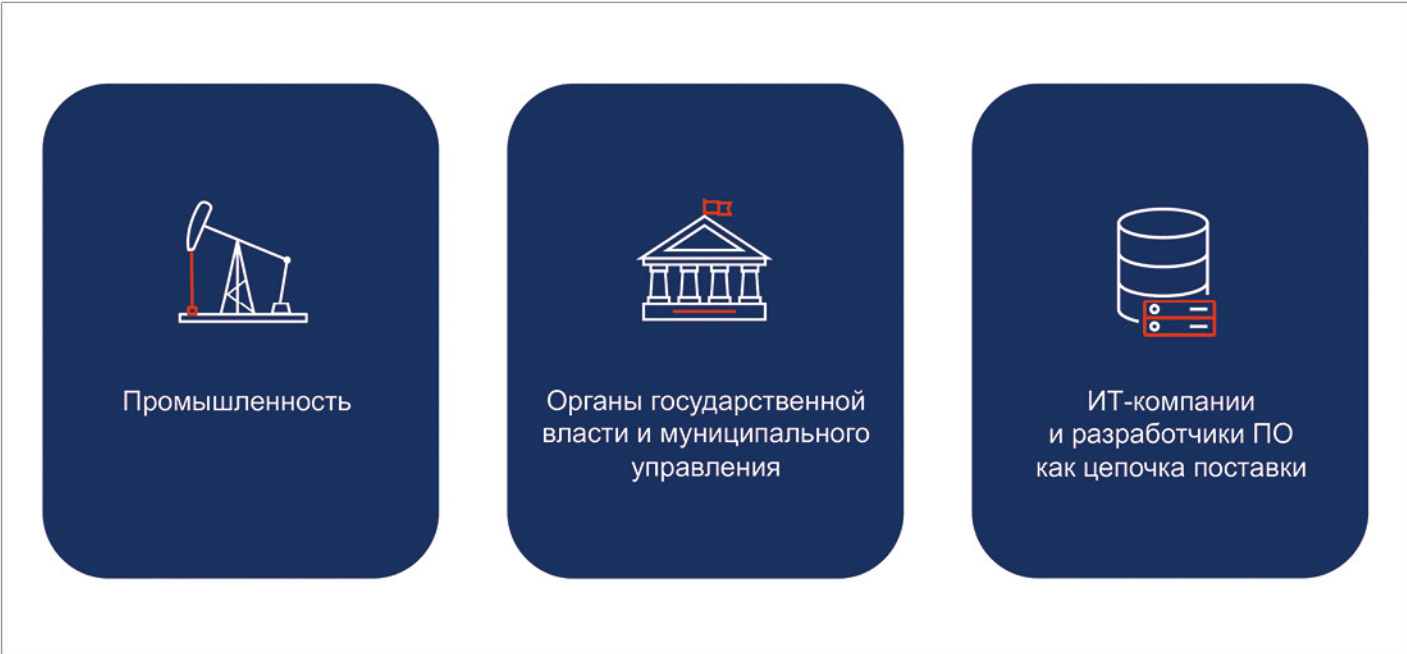


Рисунок 3. Наибольшая зона риска

проводить атаки высокой интенсивности легитимным трафиком. Для противодействия им требовались разработка и реализация дополнительных способов фильтрации.

АТАКИ КАК ПРИКРЫТИЕ

Кроме того, злоумышленники очень активно обмениваются результатами своей работы. Данные о результатах сканирования, найденных уязвимостях, похищенные сведения публикуются для дальнейшего анализа и последующего использования в атаках.

При этом DDoS-атаки стали хорошим прикрытием для более серьёзных воздействий.

Учитывая напряжённую геополитическую ситуацию, большое внимание злоумышленниками уделяется атакам, которые могут иметь общественный резонанс, то есть из которых можно сделать «взрывной» информационный повод.

Это всевозможные дефейсы информационных ресурсов, в результате которых размещаются антироссийские и антигосударственные материалы, а также фейки. Объектами таких атак становились информационные ресурсы средств

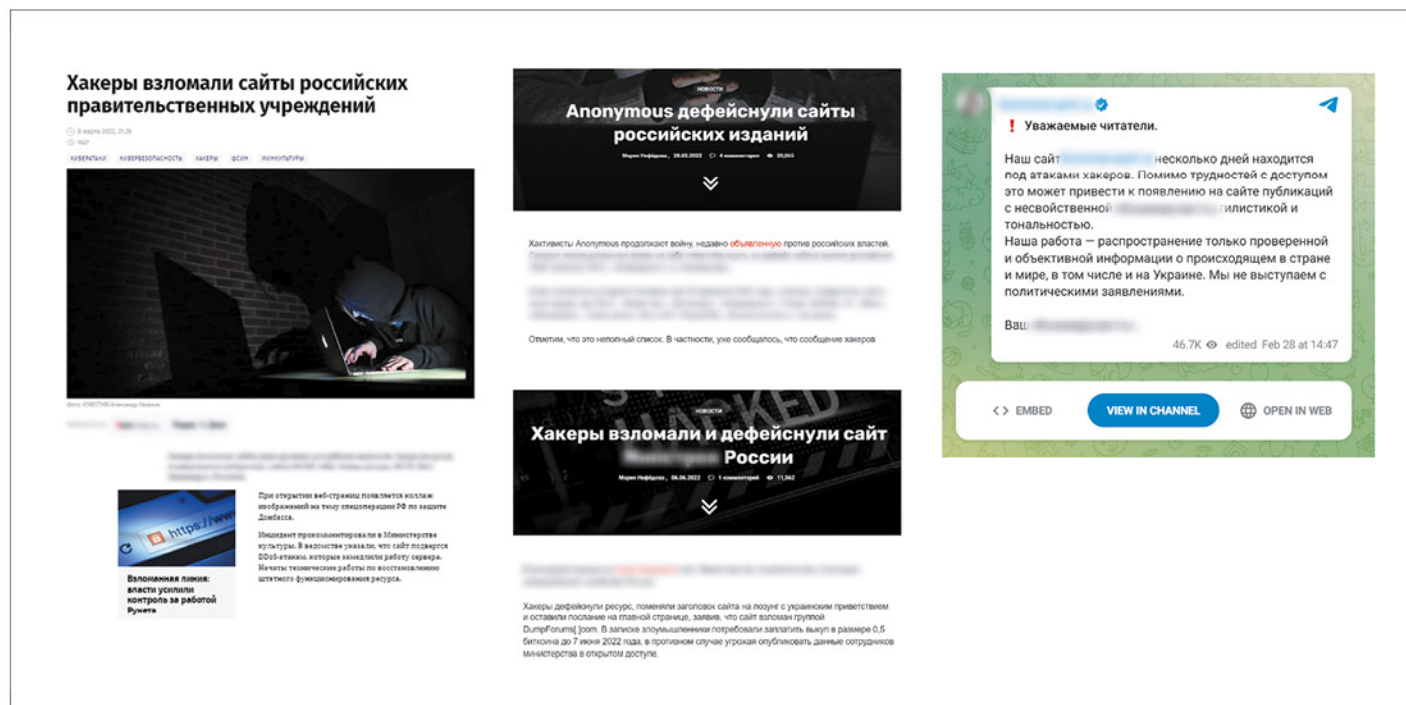


Рисунок 4. Дефейсы информационных ресурсов

массовой информации (далее — СМИ), государственных органов, крупных промышленных организаций. В ряде случаев злоумышленники на сайтах предприятий размещали обращения от имени руководителей организации с антироссийскими и антиправительственными лозунгами, что несло дополнительные риски и для репутации руководства этих организаций. Примеры публикаций приведены на рисунке 4.

ПРОГРАММНЫЕ ЗАВИСИМОСТИ И СТОРОННИЙ КОД

Здесь же проявилась новая специфическая тенденция — использование программных зависимостей и стороннего кода. Например, публикации на целом ряде ресурсов СМИ антироссийских лозунгов были реализованы с помощью подмены кода рекламного баннера его автором. Похожий механизм также был реализован в ходе атаки на счётчик системы Госмонитор. Немало компьютерных атак было направлено на проникновение в системы организаций с целью хищения информации и выведения из строя технологических процессов с последующим преданием гласности этих так называемых успехов.

УТЕЧКИ ДАННЫХ

Много публикуется информации об утечках данных. Вынуждены констатировать, что их следствием в основном является небрежное отношение к сервисам, доступным на периметре. В то же время необходимо отметить, что в погоне за информационным поводом и общественным резонансом злоумышленники очень часто публикуют фейковую информацию об утечках. Используются самые разные способы: например, собирается информация из ранее произошедших утечек и выдаётся как новая; делаются компиляции из данных, полученных из открытых источников или из публично доступной информации. Нередки и случаи, когда кража

данных одной из небольших организаций в результате взлома её ресурсов выдаётся за утечку из одной из ключевых государственных систем или объектов КИИ, тем самым поднимая значимость освещаемого события.

НЕСАНКЦИОНИРОВАННАЯ ДЕЯТЕЛЬНОСТЬ

Ситуация с несанкционированным и неконтролируемым изменением программного кода и вообще деятельностью разработчиков вылилась в целую серию инцидентов и угроз. В первую очередь, множество вендоров средств защиты, программного обеспечения, телекоммуникационного оборудования заявили о прекращении поддержки своих продуктов, отзывах лицензий и т. п. И если в большинстве случаев это не вызывало немедленных серьёзных проблем, средства прекращали обновляться, но время принять компенсирующие меры ещё было, то в ряде случаев устройства просто превращались в «тыкву» и периметр организации рассыпался прямо среди ночи. Очень показательным повёл себя ряд опенсорсных разработчиков, включавших вредоносный функционал в свои обновления.

Совместно со ФСТЭК России и ведущими организациями отрасли был разработан и опубликован порядок принятия решения о целесообразности обновления, учитывающий ряд важных факторов. НКЦКИ предложено пользоваться такой логикой.

УГРОЗА ОТЗЫВА СЕРТИФИКАТОВ

Дальше была серьёзная угроза отзыва всех сертификатов и нарушения работы сервисов. Какое-то время сертификаты продавала только одна организация. НКЦКИ рекомендует перейти на использование сертификатов, выпущенных отечественным удостоверяющим центром, хотя бы на основных доменных зонах. Отечественные браузеры будут их поддерживать, это позволит сохранить работоспособность основных сервисов при самом неблагоприятном раскладе.

НЕДРУЖЕЛЮБНЫЕ ДЕЙСТВИЯ

Отдельно стоит остановиться на недружелюбных политизированных действиях международного ИБ-сообщества. Так, Форум групп реагирования на компьютерные инциденты FIRST приостановил работу с российскими центрами реагирования на компьютерные инциденты. Это решение, а также происходящее в целом в информационном пространстве Российской Федерации только подтверждает неоднократно высказанную НКЦКИ ранее озабоченность о декларативном характере подходов некоторых стран к решению задачи по созданию мирной, стабильной и защищённой мировой ИКТ-среды.

В целом успех многих компьютерных атак, как показал опыт этих дней, обусловлен не каким-то изощрённым способом проникновения, а, к сожалению, недоработками служб информационной безопасности организаций. Недоработками иногда в очевидных местах. Набор рекомендаций по противодействию угрозам НКЦКИ излагает в своих бюллетенях, которые публикуются на сайте safe-surf.ru и рассылаются тем, с кем организовано взаимодействие.

УСТАНОВКА НА РАЗВИТИЕ

Итак, целесообразно отметить, что злоумышленники постоянно совершенствуются, обзаводятся новыми инструментами, адаптируют свою тактику под современные условия. И в этой гонке, на наш взгляд, очень важно успевать вовремя адаптировать и свою тактику защиты. Именно тактику, а не только средства.

НЕОБХОДИМО, НО НЕДОСТАТОЧНО

Дальше остановимся на некоторых из тех основных уроков, которые НКЦКИ вынес из инцидентов этого года. Их анализ показывает, что по-прежнему основные усилия владельцев информационных систем направлены на защиту периметра. Это, безусловно, важнейшая задача: безопасность периметра — краеугольный камень системы защиты. Но к сожалению, сегодня этого мало.

ВЕКТОРЫ АТАК

Для проникновения в инфраструктуру организации в настоящее время злоумышленники используют следующие основные векторы.

- ♦ Взлом сервисов, доступных на периметре. На долю этого вектора, по имеющимся в распоряжении НКЦКИ данным, приходится почти половина всех атак уровня АРТ. Сейчас, наверное, все владельцы информационных ресурсов понимают опасность уязвимостей программного обеспечения, особенно обеспечивающего работу внешних сервисов. Большинство так или иначе организуют работы по отслеживанию появления таких уязвимостей и их закрытию. Но на практике оказывается, что почти треть организаций имеют в своей инфраструктуре уязвимые ресурсы. Ну а когда публикуются сведения о критических уязвимостях в широко распространённых продуктах, у злоумышленников возникают окна возможностей, когда можно успеть скомпрометировать систему до установки обновлений. Например, почтовых серверов с уязвимостями в стране до сих пор далеко не единицы. И многочисленные утечки — отсюда.

- ♦ Второй вектор — фишинговые рассылки. Многочисленные исследования российских и зарубежных специалистов сходятся примерно к одному. В среднем фишинговое письмо открывает каждый седьмой сотрудник. Это с учётом всех организаций, даже тех, которые по уровню зрелости информационной безопасности находятся на высоком уровне. Если говорить про отрасли, в которых традиционно отмечается нехватка кадров и ресурсов, то здесь статистика ещё печальнее: открывается каждое четвёртое письмо.

- ♦ Третий вектор — атаки через подрядчиков. Количество таких атак за год, по имеющейся в распоряжении НКЦКИ информации о компьютерных инцидентах, выросло в два раза. И получив доступ к инфраструктуре подрядчика, злоумышленники оказываются внутри целевой системы.

- ♦ Обычное ВПО — тоже не мелочи. Какое-нибудь всем известное ВПО обычно не вызывает у «безопасников» желания пристально посмотреть на свою инфраструктуру. Часто мероприятия по реагированию ограничиваются лишь устранением самого ВПО. Такое отношение, как показывает опыт, бывает чревато более тяжёлыми последствиями. Получают распространение случаи, когда операторы таких обычных бот-сетей (а они обычно очень большие, используются, например, для DDOS-атак) продают доступ к заражённым машинам организаторам АРТ-кампаний. А дальше всё просто: периметр пробит, система позволяет развить успех внутри инфраструктуры и получить устойчивую точку присутствия.

ПРОПИСНЫЕ ИСТИНЫ

Что же получается? Удержать периметр своей инфраструктуры стало объективно трудной задачей, выполнение которой с заданным уровнем надёжности обеспечить подчас очень трудно. При этом большинство владельцев сосредотачивает свои усилия на защите периметра, и протоколирование осуществляют только на нём. А внутри инфраструктуры не то что противодействия злоумышленнику не предусмотрено, даже протоколирование не ведётся, чтобы проследить за ним.

Известна прописная истина: скорость выявления и принятия мер напрямую влияет на масштаб ущерба и затраты, необходимые для реагирования. Поэтому к инцидентам необходимо готовиться. По нашему мнению, атаки с использованием цепочки поставщиков ещё не достигли своей кульминации. Опубликованные в этом году утечки злоумышленники продолжают анализировать на предмет выявления связей между организациями и для подготовки новых атак.

ПОСЛЕДНИЙ АКЦЕНТ

Не будем в настоящей статье останавливаться на мерах. Об этом говорилось и писалось не единожды. Но ещё раз акцентируем внимание на следующем. Практика реагирования на компьютерные инциденты 2022 года ещё раз подтвердила, что без системного выстраивания и реализации процессов обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты противодействовать злоумышленникам сегодня не получится. Поэтому данное направление становится актуальным для всех владельцев информационных ресурсов.

«БОЛЬШИНСТВО РИСКОВ МОЖНО СНЯТЬ БАЗОВЫМИ СРЕДСТВАМИ ЗАЩИТЫ»

BIS Journal продолжает публикацию интервью с известными CISO банковской сферы. У нас в гостях Дмитрий Стуров, исполнительный директор, начальник управления информационной безопасности Банка Ренессанс. Дмитрий окончил Академию Федеральной службы безопасности РФ и работает в Банке Ренессанс с 2005 года.



ДМИТРИЙ СТУРОВ
исполнительный директор, начальник управления информационной безопасности Банка Ренессанс

О РЫНКЕ

— Дмитрий, что, на ваш взгляд, происходит сегодня на рынке безопасности в России?

— После глобальных перемен, произошедших в прошлом году, рынок пытается найти равновесие между запросами заказчиков и возможностями вендоров их удовлетворить. Но клиенты должны понимать, что российские вендоры в отдельных направлениях пока не достигли уровня своих западных коллег, поэтому теперь могут получить менее зрелые продукты, чем те, к которым привыкли. То есть заказчикам необходимо научиться обеспечивать уровень защищенности на имеющихся продуктах. Это с одной стороны. С другой — и вендорам нужно понимать, что они будут получать повышенные требования от клиентов, привыкших работать с западными технологиями. И в случае возникновения трудностей они будут настаивать на дополнении имеющегося функционала, потому что без этого невозможна полноценная эксплуатация продукта.

Также у вендоров возникло много дополнительной нагрузки. Они, может быть, ей и рады, но переварить её им непросто.

ОБ АТАКАХ

— О каких наиболее актуальных типах атак следует говорить на сегодняшний день?

— Конечно, у всех на слуху DDoS-атаки, обрушившиеся на российские компании. Их особенностью стало то, что раньше они были производными от активности ботнетов, а сейчас они исходят от вполне легальных узлов — тех же домашних ПК, владельцы которых предоставляли их мощности для своих организаций. Поэтому, если компания не научилась защищаться от DDoS, ей сложно в текущих условиях выстраивать защиту.

Атаки были нацелены не на сетевые каналы, это были точечные высокоуровневые удары.

Например, наш банк столкнулся с такой мощной атакой впервые. До этого нам приходилось иметь дело с более простыми угрозами, которые легко фильтровались. Тем не менее доступность сервиса была сохранена. Я знаю, что многие банки тоже испытывали сложности, но всем удалось в той или иной степени от них защититься.

Второй тип атак, ставших актуальным недавно, — это дефейсы. Правда, мне кажется, что они были более заметны в первой половине 2022 года. Затем их эффективность была переоценена (стало ясно, что баннер на сайте не может сильно повлиять на ситуацию), и во второй половине 2022 года мы о таких атаках почти не слышали.

Ещё одним трендом, который нельзя было не заметить, стали атаки на поставщиков и контрагентов. Злоумышленники прицепились к ИТ-компаниям, которые обслуживают сразу несколько организаций. Преимущества тут очевидны: получив несанкционированный доступ к одному подрядчику, хакеры получают доступ к данным всех его организаций-клиентов, среди которых могут быть очень крупные заказчики. Кроме того, небольшие ИТ-компании зачастую не выстраивают полноценных систем безопасности, потому что находятся на невысоком уровне зрелости. Это тоже играет на руку злоумышленникам.

Наконец, наблюдались довольно частые случаи «слива» данных. Тут есть особенность. Ранее утечки информации происходили «тихо»: у данного типа атаки была сугубо утилитарная цель — использовать информацию для дальнейших мошеннических и рекламных звонков и тому подобной активности. Сейчас такие утечки получают большую огласку. Причина — в общем неспокойном информационном фоне, преобладании негативной повестки.

Актуальными я назвал эти типы атак. Однако тревожат не только они: продолжает

появляться большое количество критических уязвимостей в информационных системах, а учитывая проблемы с получением обновлений из-за санкций, это может стать проблемой в ближайшем будущем. Компаниям нужно будет найти способы управления риском отсутствия обновлений — получать их по неофициальным каналам, применять компенсирующие механизмы и т.д.

— Как выглядят на этом фоне проблемы социальной инженерии?

— Случаев социальной инженерии стало больше. Я сам стал получать много звонков от «службы безопасности известного банка». Особенность такого телефонного терроризма в том, что он легко реализуем и не требует больших затрат — нужно просто звонить и играть роль оператора кол-центра, и никаких сложных дорогостоящих схем.

Растёт и количество случаев фишинга — поддельных сайтов, рассылок — с целью кражи карточных данных, проведения мошеннических платежей, кражи паролей. Данные рассылки всегда маскируются под текущие тренды — благотворительность, точечные сборы на нужды военнослужащих. Надо быть очень внимательным и проверять информацию, чтобы не стать жертвой.

ОБ ИЗМЕНЕНИЯХ И ЗАДАЧАХ

— Как происходящие изменения отразились на работе ИБ-команды Банка Ренессанс?

— В первую очередь пришлось активизировать процесс импортозамещения. Раньше этому не уделялось много внимания. При этом все понимали, что рано или поздно нужно будет находить баланс между импортными и отечественными решениями. Однако всё в одночасье изменилось, и теперь мы вынуждены отвлекать ресурсы для переориентирования ряда критичных сервисов банка на отечественные аналоги.

Минус «импортозамещения в авральном режиме» не только в том, что мы утратили возможность пользоваться качественными продуктами. Предположим, что их можно будет заменить на отечественные, которые будут не хуже. Однако всё равно эти продукты нужно выбрать, протестировать, внедрить — и не просто внедрить, а сделать это на том же уровне зрелости, на котором ранее работали продукты западных вендоров. Это занимает и будет занимать много времени и ресурсов.

В результате часть запланированных проектов не была реализована — на них банально

не хватило времени, поскольку пришлось заниматься тестированием пилотных проектов. Конечно, необходимость отражения атак также отнимала ресурсы.

В связи со всеми этими изменениями в конце года нам пришлось корректировать стратегию развития.

— Действительно, 2022 год был тяжёлым во многих отношениях. Наряду с задачами, о которых вы уже упомянули, чем ещё занимается руководитель управления ИБ банка?

— Я решаю достаточно типичные для подразделения ИБ задачи. Оговорюсь, что в наше управление не входит подразделение антифрод, которое работает автономно и занимается расследованием случаев мошенничества, связанного с незаконными платежами.

Моя главная задача — обеспечивать защищённость ИТ-активов банка, всех процессов, которые так или иначе взаимодействуют с информационными ресурсами.

О БИЗНЕСЕ

— Как строятся ваши взаимоотношения с бизнесом, он уже осознал важность информационной безопасности после всех событий?

— Наш банк осознал всю важность информационных технологий несколько лет назад, встав на путь цифровизации. Параллельно с этим пришло понимание, что необходимо обеспечивать ещё и такое качество информационных активов, как безопасность.

Сразу после пандемии, на протяжении 2021 года, у нас были встречи с бизнес-подразделениями, инициатором которых выступал именно бизнес. Они задавали вопросы по безопасности, интересовались, какие процессы в этом плане происходят в банке, как обстоит ситуация с ИБ и т.д. По результатам были внесены изменения в стратегию развития, чтобы сосредоточить внимание именно на тех вопросах, которые интересны бизнесу.

Случаев социальной инженерии стало больше. Я сам стал получать много звонков от «службы безопасности известного банка». Особенность такого телефонного терроризма в том, что он легко реализуем и не требует больших затрат

Сами по себе технологии и системы вторичны, на первом плане — зрелость процессов, выстроенных на этих системах. Поэтому иногда вместо закупки и внедрения продвинутой техники целесообразно повысить зрелость процессов, построенных на классических средствах защиты

Кроме того, в банке появились подразделения, сфокусированные именно на диджитал-продуктах. Их руководители хорошо понимают специфику информационных технологий и информационной безопасности, знают, что происходит в этой сфере, и понимают, какое внимание этому нужно уделять.

О ТЕХНОЛОГИЯХ И ПРОЕКТАХ

— Технологии, которые используются в информационной безопасности, постоянно меняются. Какие из них вы считаете наиболее современными и актуальными и какие предпочитаете использовать?

— Уровень защищённости и зрелости технологий и процессов, которым необходима ИБ, можно представить в виде пирамиды. Внизу базовый уровень защищённости, на верхушке — продвинутый. Получается, что инвестиции идут снизу вверх: чем выше мы забираемся по этой пирамиде, тем система становится дороже.

При этом я считаю, что большинство рисков можно снять базовыми средствами защиты, создав грамотную конфигурацию ИТ-систем и правильно выстроив бизнес-процессы. Я имею в виду, что являюсь поклонником стандартных систем защиты информации, а не «новомодных» решений.

Если пользоваться аналогией закона Парето — 20% усилий дают 80% результата, оставшиеся 20% рисков придётся обрабатывать с гораздо большими инвестициями и затратами ресурсов.

Можно сказать, что сами по себе технологии и системы вторичны, на первом плане — зрелость процессов, выстроенных на этих системах. Поэтому иногда вместо закупки и внедрения продвинутой техники целесообразно повысить зрелость процессов, построенных на классических средствах защиты.

Только в исключительных случаях при наличии должного финансирования и человеческих ресурсов стоит задумываться о внедрении продвинутых технологий, например, XDR, BaAS, CAASM, Deception и др.

При этом хочу отметить, что на российском рынке тоже имеются передовые технологии даже по мировым меркам. Однако в прошлом году мы потеряли базовые системы (из-за ухода западных вендоров), которые необходимо будет заменить в первую очередь, на что, конечно, потребуется время. И только после этого мы сможем вернуться к задачам внедрения продвинутых технологий.

— Какие проекты в сфере безопасности вы внедрили и планируете к внедрению в 2023 году?

— Будем повышать зрелость процессов безопасной разработки в банке. У нас много собственных продуктов и разработок, которые производит ИТ-подразделение, и они должны быть безопасными.

За последние 2–3 года был совершён значительный скачок в объёмах производства таких продуктов. Мы должны поддерживать их качество на всех этапах.

Также будем продолжать работу по повышению уровня защищённости организации, оптимизировать внутренние процессы и внедрять новые технологии после их апробации на пилотных проектах.

О ТРЕНДАХ

— Какие глобальные или локальные тренды будут определять процессы в информационной безопасности на ближайший год?

— Думаю, что в 2023 году атаки на компании продолжатся. Возможно, мы увидим их более продвинутые версии с проникновением в периметр и достижением целей более изящным способом, чем DDoS.

Будет нарастать внимание к атакам на поставщиков услуг. Причём сразу со всех сторон — со стороны злоумышленников, со стороны организаций-получателей услуг и со стороны регуляторов рынка ИБ.

Ещё одним перспективным направлением будет развитие и вовлечение искусственного интеллекта во многие сферы информационных технологий и информационной безопасности. Об этом свидетельствует ажиотаж вокруг нейросетей — ChatGPT, Midjourney, Rytg и др.

Считаю, что будет уделяться внимание безопасности работы персонала. Нормальная практика, когда доступ к критической инфраструктуре возможен только со спота, а не через удалённый доступ из любой точки мира, как это привыкли делать в пандемию. Необходимо ещё раз оценить и проанализировать эту ситуацию, возможно, внедрить какие-то новые инструменты проверки легитимности доступа, внедрить

правило четырёх рук, или вообще запретить этот тип доступа. Свобода удалённой работы, которую подарил ковид и цифровизация, будет сужаться. Конечно, она не исчезнет полностью, но должна дойти до разумных пределов.

О КАДРАХ И УСПЕХЕ В ПРОФЕССИИ

— Насколько остро в банке стоит кадровый вопрос? Как вы его решаете?

— Кадровый вопрос всегда сложный. Талантливых и мотивированных людей найти непросто. Безусловно, на некоторые позиции мы достаточно долго ищем нужных сотрудников. Конкуренция высокая. Мы стараемся привлекать людей интересными задачами, достойным уровнем компенсации и, что точно отличает нас на рынке, доброжелательной и дружелюбной атмосферой.

— Сформулируйте, пожалуйста, общие принципы успеха, которые могут помочь добиться успеха в профессии ИБ-специалиста?

— Информационная безопасность всегда привлекала меня тем, что фронт знаний, который в ней требуется, достаточно широкий. Тут нужно разбираться в очень разных вещах, начиная от технологий и инфраструктуры, заканчивая кодингом, тестированием, процессами разработки и т.д.

В ИТ специалист работает, как правило, по конкретному направлению, а специалист по безопасности такой роскошью не обладает, его знания должны быть многоплановыми и разнонаправленными. Кому-то это кажется сложным, я же считаю преимуществом профессии.

Мне кажется, технический бэкграунд очень важен для специалистов ИБ. Например, обладая широким бэкграундом, можно развиваться как аналитик Security Operation Center (SOC) и выстраивать своё профессиональное образование в этой среде. Но при этом имеющийся базис знаний позволяет через 2–3 года пойти в аудиторы или пентестеры. Я бы сказал, что секрет успеха ИБ-специалиста заключается в том, чтобы такой базис получить.

Кроме того, технический бэкграунд важен ещё и потому, что позволяет быстро и правильно принимать разные решения, что очень важно в области безопасности, где необходимо постоянно оценивать риски.

— Какие вузы вы могли бы порекомендовать молодым людям, которые хотят идти в ИБ?

— Если честно, на собеседованиях я не особо обращаю внимание на вузы соискателей. Я пытаюсь делать корреляцию в этом плане, но мне кажется, это не очень правильный подход.

Думаю, вузовское образование немного архаичное и отстаёт от реальности. Если честно, на собеседованиях я не особо обращаю внимание на вузы соискателей

Рынок ИБ ещё молодой, и здесь многое в стадии формирования. Я думаю, вузовское образование немного архаичное и отстаёт от реальности. Оно никогда и не сможет догнать реальность: пока утвердят стандарты образования и разработают курс обучения по новой теме, она может утратить актуальность и вообще уйти со сцены.

Поэтому в вузе следует уделять внимание базовым вещам: математике и логике, информационным технологиям и администрированию — это тот базис, который даётся во многих технических вузах.

Одновременно можно учиться на онлайн-курсах, которых сейчас множество, в том числе и на английском языке. Знание английского — обязательный фактор. Подавляющее большинство материалов по ИБ доступно именно на английском. Также нужно изучать различные стандарты ИБ, материалы конференций. Самообразование — это, по сути, часть профессии безопасника.

— Как относятся к молодым специалистам в вашем банке?

— Человек может прийти к нам в банк и сказать, что хочет заниматься информационной безопасностью, даже если он пока не определился с конкретной спецификой. И мы можем помочь человеку понять, какое направление ему более интересно.

ОБ УВЛЕЧЕНИЯХ

— Если не возражаете, чем вы увлекаетесь в свободное от работы время, как проводите свой досуг?

— На меня увлечения накатывают как волны: то одно, то другое. Главные — это игра в баскетбол с друзьями и музыка. Я коллекционирую музыку, предпочитаю её электронное направление. Любовь к музыке здорово помогла пережить пандемию и всеобщую изоляцию в 2020 году.

Ещё я очень люблю путешествовать, мне доставляют удовольствие прогулки по городам Европы, посещение музеев, различных памятных мест.

Беседовала
Оксана Дяченко

ЦПК. ПОРА ИЗМЕНИТЬ СТРУКТУРУ ОТРАСЛИ ИБ

ВОПРОС МАСШТАБНЫЙ, НЕОБХОДИМЫЙ И... РЕШАЕМЫЙ.
ПО КРАЙНЕЙ МЕРЕ, ОБСУЖДАЕМЫЙ



Артём
КАЛАШНИКОВ
Газпромбанк

В дискуссии, начатой в прошлом номере BIS Journal (№ 4/2022), Александр Велигура поставил вопрос о создании Центра противодействия киберугрозам (ЦПК), который возьмёт на себя функцию обеспечения ИБ в финансовых организациях, не обладающих для этого ресурсами. А таких в России более 15 000! Участники дискуссии пошли дальше и предположили, что такой ЦПК мог бы обслуживать не только финансовую сферу, но и все компании и организации в стране. Возник образ эдакого СуперкиберМВД или Нью-Васюков в сфере ИБ, но доводы спикеров были спокойны и убедительны, и редакция решила продолжить дискуссию. На возникшие вопросы мы предложили ответить Артёму Калашникову, обладающему опытом создания ФинЦЕРТ Банка России.

ВОПРОС ОТВЕТСТВЕННОСТИ

— Основные возражения по поводу предлагаемого ЦПК касаются его ответственности. Есть ли здесь какой-либо опыт, который можно было бы применить не только к дочерним организациям и филиалам?

— Вопрос ответственности всегда является очень острым. Как мы знаем, регуляторы возлагают ответственность на первых лиц компаний. А по 250-му приказу Президента РФ — на второе лицо компании, специально наделённое полномочиями и имеющее соответствующие компетенции. В финансовом секторе есть документ ЦБ РФ с требованиями к аутсорсингу услуг. Конечно, актуальность его уже не так велика — за счёт появления новых технологий, но я считаю это хорошим опытом и началом для распространения подобных документов на остальные отрасли.

У нас есть много компаний, которые оказывают услуги аутсорсинга, а местами и аутстаффинга. Ответственность там разделяется согласно договору, SLA. Полагаю, такую схему можно распространить и далее. Следует разработать требования к аутсорсингу и аутстаффингу, где будут указаны позиции, которым должны соответствовать организации, оказывающие такие услуги. Далее идёт распределение

зон ответственности между компанией и заказчиком. И такой момент нужно предусмотреть и прописать в законодательстве.

ОРГАНИЗАЦИОННО-ПРАВОВАЯ КОНСТРУКЦИЯ

— Суть некоторых высказанных мнений состоит в том, что выполнения требований существующих стандартов и других документов в основном достаточно для решения задач обеспечения ИБ организационно-административного плана, они требуют скоординированной деятельности подразделений и т.п. Всё это верно, но ведь одной из причин предлагаемого создания ЦПК как раз и является отсутствие ресурсов для решения этих задач собственными силами малой организации, тем более в условиях, когда нет оснований рассчитывать на упрощение требований регуляторов. Опять же возникает вопрос ответственности за состояние ИБ в организации и кто и какую ответственность будет нести в случае инцидента, вызвавшего ущерб, на что совершенно справедливо указывает А. П. Курило.

На эти вопросы, мягко говоря, трудно ответить исходя из нынешней нормативно-правовой базы.

Менять — да, но комплексно. Как справедливо указываете вы в своей предыдущей статье, «это вопрос для отдельного большого обсуждения». Не начать ли такое обсуждение?

Можно ли предложить концепцию нормативно-правового регулирования для эффективного использования ЦПК? Как подойти к решению этой задачи?

— Полагаю, что как раз в организации уже есть ответственные за обеспечение ИБ, а уж в КИИ точно. Вопрос остальных организаций лежит в области внутреннего менеджмента и процессов. Делегирование Указом Президента РФ полномочий за обеспечение ИБ первым лицам организаций решает этот вопрос окончательно.

А широкое обсуждение — это да, его давно пора начать. Необходимо выработать в концепции ЦПК организационно-правовую конструкцию, которая будет проходить «скелетом» через



всю цепочку от регуляторов до потребителей услуг и тех, кто их оказывает. После чего можно подключать к этой конструкции и технические платформы для реализации требований и услуг.

НЕМНОГО ИСТОРИИ

— Представьте, пожалуйста, историю вопроса ЦПК?

— Начиналось всё с примитивного мониторинга в отдельных компаниях. То есть пытались подключать периметр компании к разным ресурсам, чтобы просто мониторить и по телефону потом как-то реагировать в сторону наблюдаемого.

Уже тогда, лет 20 назад, многие компании поняли, что средства защиты достаточно дорогие, а специалистов, которые эти средства должны настраивать и эксплуатировать, днём с огнём не сыщешь, так как в России их просто нет. Остро встал вопрос: что делать? Привлекали людей отовсюду: из ИТ, военных, силовиков — любых, кто хоть как-то понимал технику.

Кроме того, насущной потребностью было понимать и стратегическое направление — чтобы грамотно и логично выстраивать развитие и техническую реализацию ИБ. Для

этого брали западные документы и стандарты, перекладывали их на отечественные реалии, адаптировали к разным секторам экономики. Финансовый сектор тут был пилотом и первопроходцем.

Когда процесс пошёл, стало понятно: не хватает ни кадров, ни средств защиты, ни документов, описывающих и регламентирующих процессы и методологии. Поэтому было много инициатив, связанных с образованием. В итоге многие вузы ввели специальность «информационная безопасность».

Параллельно шло развитие компенсирующих мер — это опечатывание помещений, журналы фиксации доступа к ресурсам и т.д. Всё это делалось в полуручном, а точнее, в ручном режиме. Но постепенно всё автоматизировалось и появились новые риски и угрозы, связанные с ИБ. Соответственно, в обучение стали добавлять предметы, связанные с построением систем, архитектурой, внутренним взаимодействием компонентов и т.д. Начали эволюционировать системы и средства защиты, причём многие очень резко. Особенно те, что связаны с контролем доступа, наблюдением, шифрованием, мониторингом...

И в результате пришли к тому, что обеспечение информационной безопасности для компании — это процесс, требующий централизации, то есть единого центра.

Названия таких центров — SOC и CERT — на Западе тогда уже устоялись и благополучно переключались к нам.

О ЗАРУБЕЖНОМ ОПЫТЕ

— Расскажите, пожалуйста, о зарубежном опыте?

— В Европе первые центры, оказывающие услуги мониторинга и реагирования, появились 25 лет назад. Потом появились сообщества. Одно из них — FIRST, там порядка 2500 центров, которые постоянно обмениваются информацией об угрозах и мерами реагирования. Но есть и опыт азиатского региона, и опыт обеих Америк.

Собственно, весь этот опыт и использовался при построении сначала SOCOв, а потом и CERT в России.

Причём этот процесс пошёл очень быстро. Первый аналог CERTа появился в 2015 году в ЦБ, в 2017 году он вышел на достаточно большое покрытие поднадзорных организаций, а ещё через год вышел на международный уровень, войдя в несколько сообществ объединённых CERT. Это позволяет ему получать информацию о многих угрозах задолго до появления их в России.

ЧТО СЕГОДНЯ?

— Какова ситуация на сегодняшний день?

— Сегодня мы имеем развитую нормативную базу по ИБ, причём довольно жёсткую. Имеем средства обеспечения ИБ, но часть из них очень дорогая. Имеем проблему с кадрами, которые должны управлять этими средствами и обеспечивать информационную безопасность как процессно, так и технически.

В результате налицо большой разрыв между компаниями, имеющими ресурсы на создание и содержание своих центров мониторинга и реагирования, и компаниями, не имеющими таких ресурсов. Вот у вторых-то, а их подавляющее большинство, и возникла потребность в создании корпоративных и отраслевых ЦПК.

— Речь вроде шла о едином государственном ЦПК?

— Есть отрасли, в которых ИБ далеко не на втором и даже не на третьем месте. Есть корпорации, в которых компании до смешного далеки от выполнения нормативов по обеспечению ИБ. И главная идея — создать чётко управляемую структуру снизу доверху. То есть создать узлы на каждом уровне иерархии. На уровне

государства, отрасли, корпорации и дальше до конкретных предприятий и организаций.

— Для чего это нужно?

— Огромный объём информации, который поступает из одной отрасли первично, при суммировании с объёмами информации из других отраслей окажется неподъёмно большим. Он просто завалит весь трафик и все вычислительные мощности государственного Центра. Но всю эту информацию можно обработать и систематизировать на первой линии, где появляется централизация, и дальше, уже очищенную, репортить через отраслевые центры (или параллельно) в государственный Центр.

В случае особой необходимости можно предоставлять полную информацию. Это сейчас предусмотрено на верхнем уровне.

ЕЩЁ РАЗ ПРО РАЗГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ

— Идея, в общем-то, простая... Но есть проблема, которая не позволяет реализовать её в полном объёме, — это разграничение ответственности между центром мониторинга и теми, кто пользуется его услугами. Кто за что отвечает в случае реализации угрозы?

— Эту проблему, повторюсь, нужно решать на уровне государства — через нормативы, законы или подзаконные акты. А возможно, и на уровне регуляторов информационной безопасности.

ПРО КАДРЫ

— А проблема кадров?

— За счёт централизации кадров как раз потребуются гораздо меньше. Необходимые компетенции будут локализоваться в центрах — государственном, отраслевых или корпоративных, — несущих ответственность каждый на своём уровне, в своей сфере.

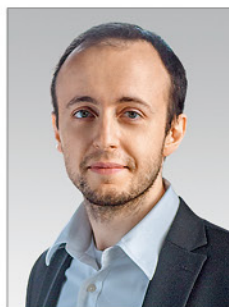
ПРО КАТАСТРОФУСТОЙЧИВОСТЬ

— Но есть ещё проблема катастрофустойчивости?

— Понятно, что каждый центр по сути — это узел. И его отказ, если его «пробьют» злоумышленники, даст пробел во взаимодействии и обеспечении ИБ. Для такого случая хорошо подходит идея построения взаимодействия «каждый с каждым», чтобы техническая информация была у всех. Помимо той, которая явно указывает на отрасль или корпорацию. Эта информация должна храниться на уровне корпоративных или отраслевых центров. И уже внутри средствами резервирования и катастрофустойчивости ей должны обеспечивать постоянную сохранность — целостность — конфиденциальность.



Николай КАЗАНЦЕВ
CEO SECURITM



Рустам ГУСЕЙНОВ
председатель radcop.online

ПРО «НАРОДНОЕ» GRC

МЫ НЕ ДЕЛАЕМ СЛОЖНЫЕ ВЕЩИ ЕЩЕ СЛОЖНЕЕ

Как перестать волноваться и выстроить комплексную систему защиты по десяткам нормативно-правовых актов и стандартов в финансовой организации без космических затрат на дорогостоящие GRC?

ПОСТАНОВКА ПРОБЛЕМЫ

Управление информационной безопасностью в финансовой отрасли сродни балансированию на канате. Классические проблемы планирования, реализации, контроля и совершенствования комплексной системы защиты, которые сложны сами по себе, дополняются непрерывным изменением нормативной базы и ростом объема правовой нагрузки на службы информационной безопасности. Времена положения 382-П давно прошли и сегодня вместо одного положения по защите информации, применимого только для кредитных организаций (КО) и операторов по переводам денежных средств (ОПДС), мы имеем:

- ◆ одно положение для КО (683-П);
- ◆ два положения для ОПДС (719-П, 802-П);
- ◆ одно положение для некредитных финансовых организаций (802-П);
- ◆ положение по операционным рискам для КО (716-П);
- ◆ положения по операционной надежности для организаций всех типов (779-П, 787-П).

А ведь помимо указанных требований любая организация финансовой отрасли — как субъект национальной платежной и банковской систем — является одновременно и субъектом КИИ, и оператором персональных данных, часто имеет лицензию ФСБ, выполняет требования PCI DSS в рамках платежной системы «МИР», регулярно проходит внешние оценки соответствия лицензиатами ФСТЭК, и все это ещё не говоря о внутренних процессах защиты информации, полноту и качество реализации которых необходимо отслеживать, в том числе

путем мониторинга индикаторов и метрик ИБ, собираемых с различных систем автоматически, чтобы своевременно вносить соответствующие изменения в систему защиты.

Таким образом, CISO в роли канатоходца должен искать баланс между реальными рисками безопасности и обеспечением операционной надежности, потребностями и возможностями бизнеса, а также требованиями регуляторов и отраслевых стандартов. При этом, без современных средств автоматизации, служба безопасности рискует увязнуть в рутине и не сумеет вовремя расставить новые приоритеты, обнаружить недостатки в процессах защиты информации, реагировать на инциденты ИБ или заметить отклонение индикаторов от установленных показателей. Чего только стоят постоянные аудиты на соответствие требованиям регуляторов (оценки соответствия), отнимающие недели рабочего времени и, подчас, не приносящие реальной пользы для безопасности организации.

В результате, создаваемые системы защиты обрастают множеством активностей, висящих на плечах CISO и всей организации, сакральный смысл которых давно утерян. Если посмотреть на отдельно взятую область аудитов и контроля соответствия, то ключевыми проблемами являются:

CISO в роли канатоходца должен искать баланс между реальными рисками безопасности и обеспечением операционной надежности, потребностями и возможностями бизнеса, а также требованиями регуляторов и отраслевых стандартов

	ФСТЭК 21	ФСТЭК 239	ISO 27001	SWIFT CSCF	PCI DSS 4	57580-1 ч.7	57580-1 ч.8	57580-1 ч.9	787-П	802-П	719-П	757-П	779-П	683-П
ФСТЭК 21		77	62	45	94	206	5	3	10	21	17	7	10	4
ФСТЭК 239	77		71	39	111	224	19	5	14	17	29	7	16	7
ISO 27001	62	71		36	157	147	10	25	15	16	16	7	13	3
SWIFT CSCF	45	39	36		66	38	5	5	5	11	13	0	5	1
PCI DSS 4	94	111	157	66		244	35	30	15	3	22	5	10	11
57580-1 ч.7	206	224	147	38	244		0	0	6	25	16	7	6	5
57580-1 ч.8	5	19	10	5	35	0		0	0	2	2	20	0	3
57580-1 ч.9	3	5	25	5	30	0	0		8	0	7	6	7	1
787-П	10	14	15	5	15	6	0	8		1	9	1	16	2
802-П	21	17	16	11	3	25	2	0	1		37	14	0	11
719-П	17	29	16	13	22	16	2	7	9	37		26	7	30
757-П	7	7	7	0	5	7	20	6	1	14	26		1	11
779-П	10	16	13	5	10	6	0	7	16	0	7	1		2
683-П	4	7	3	1	11	5	3	1	2	11	30	11	2	

Рисунок 1. Пересечение требований в различных документах по информационной безопасности

1. Ресурсоемкость подготовки к аудитам и их проведения. Каждый аудит является самостоятельным проектом, отнимает много времени, сотрудники отвлекаются от своих задач, бизнес теряет время и деньги.

2. Трудозатратность ежедневного контроля соответствия требованиям и реализации организационных и технических мер системы защиты. Связанная с этими задачами рутина требует времени и сил, а отсутствие единой точки фиксации результатов приводит к необходимости консолидации информации в ручном режиме.

3. Распараллеливание и дублирование процессов контроля и надзора. В среднем организация в течение двух лет проходит от 3 до 10 аудитов по различным стандартам. И хотя многие стандарты говорят об одних тех же мерах защиты, зачастую результаты одного аудита никак не используются в проведении другого и «забываются» сразу по предоставлении их аудитору.

Для решения такого рода задач на рынке существуют так называемые GRC решения. Эти продукты позволяют:

- ♦ выстроить систему организации и управления защитой информации по принципу «единого окна»;
- ♦ собрать на базе централизованной цифровой платформы описания и свидетельства реализации всех мер системы защиты;
- ♦ в режиме реального времени наблюдать индикаторы и метрики управления ИБ;
- ♦ консолидировать коммуникации между структурными подразделениями организации по вопросам управления системой защиты.

Но остается другая проблема — дороговизна GRC платформ, как на уровне стоимости лицензии, так и на уровне сложности настройки, интеграции и сопровождения продукта в экосистеме конкретной организации. Для устранения этих недостатков нами и был разработан SECURITM, отечественное

ПО, позиционирующее как «народное GRC». Обладая достоинствами и функционалом «старших братьев» SECURITM стоит значительно дешевле и отличается гибкостью настроек, простотой внедрения и легкостью в эксплуатации.

РЕШЕНИЕ

Создавая нашу систему управления информационной безопасностью, мы собрали в единую базу знаний отечественные и международные нормативы по информационной безопасности (более 40 документов, включающих нормативно-правовые акты Банка России по информационной безопасности), разбили их на отдельные требования и связали идентичные требования между собой. Так, согласно нашей базе, приказы ФСТЭК № 17, 21, 31, 239 одинаковы на 60%, и только 20% требований в каждом из приказов уникальны. Такая же ситуация с международными стандартами, 60% одинаковых требований обнаружены в ISO 27001, NIST Cybersecurity Framework и CIS Critical Security Controls (рис. 1).

Получается, что выстраивая систему защиты или проходя аудиты по различным нормативам и не учитывая пересечение требований, службы безопасности тратят до 60% времени на одинаковую рутину. То есть около половины времени службы информационной безопасности и проверяющих организаций может быть сэкономлено, направлено на более полезные для безопасности организации задачи.

После сведения требований различных нормативов в единую базу возрастает удобство анализа различных аспектов стандартизации. Например, объединяя схожие требования в группы отдельно по отечественным и международным документам, формируя ТОПы самых популярных требований, можно заметить разницу в подходах. В международных документах чаще встречаются требования в отношении

людей и процессов, например по защите цепочек поставок, работе с персоналом, регулярному пересмотру правил межсетевого экранирования. В отечественной регуляторике упор по-прежнему делается на абстрактную техническую составляющую — внедрить антивирусную защиту, обеспечить обнаружение вторжений, без процессных требований и рекомендаций (рис. 2).

Но для того, чтобы эффективно контролировать соответствие множеству требований и нормативов недостаточно понимать как эти требования пересекаются между собой. Нужно понимать как эти требования исполняются конкретно в вашей инфраструктуре, кто отвечает за них, какие мероприятия и процессы связанные с данными мерами нуждаются в дополнительном контроле. Самым эффективным способом для этого является ведение реестра защитных мер или SoA/ведомости применимости (в терминологии ISO 27-й серии и ГОСТ Р 57580.1–2017 соответственно). Где каждая защитная мера — это описание конкретной активности структурного подразделения организации, целью которой является выполнение установленных требований для снижения рисков информационной безопасности и обеспечения операционной надежности организации. Через защитные меры описывается любая активность: от внедрения антивируса до проведения ежегодных пентестов, от выпуска актов классификации ИСПДн до получения оценки соответствия требованиям к ОУД 4 (рис. 3).

Описание всей активности организации по информационной безопасности в единой базе знаний уже само по себе является ценностью, позволяющей формировать комплексные планы работ и годовую отчетность. Но главная ценность подхода в том, что каждая мера связывается с требованиями регуляторики, на исполнение которых она направлена, а также с рисками безопасности, которые она снижает. Благодаря такой связи служба безопасности может не только ответить на вопрос что она делает, но и зачем она это делает. Причем исполнив защитной мерой требование одного документа, мы косвенно выполняем аналогичные требования из десятка других документов, и система автоматически осуществляет подобные сопоставления. Тогда, при проведении аудитов, в том числе повторных, службе безопасности остается лишь проверить, что связанные с требованиями защитные меры исправно функционируют, что можно делать на той же платформе, используя инструментальный формирования тикетов/задач, в том числе автоматических, возникающих с установленной периодичностью.

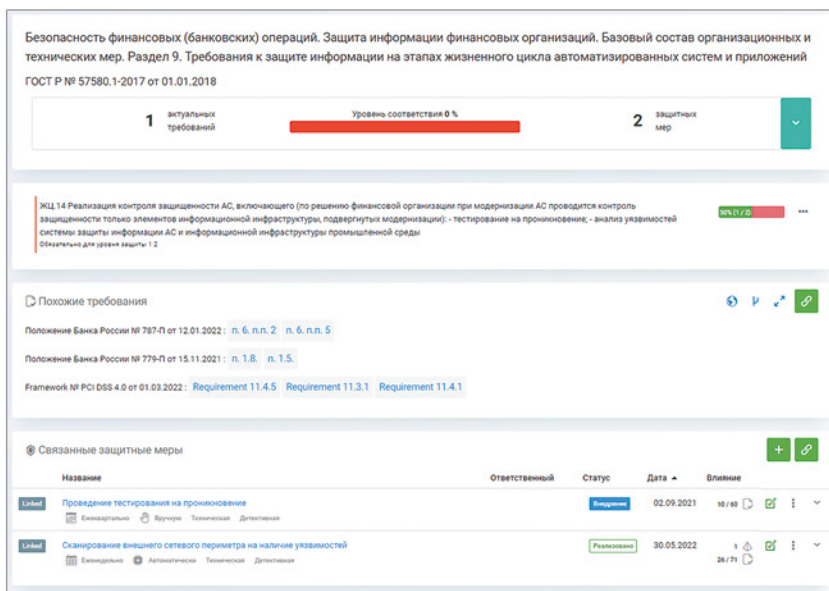


Рисунок 2. Карточка требования

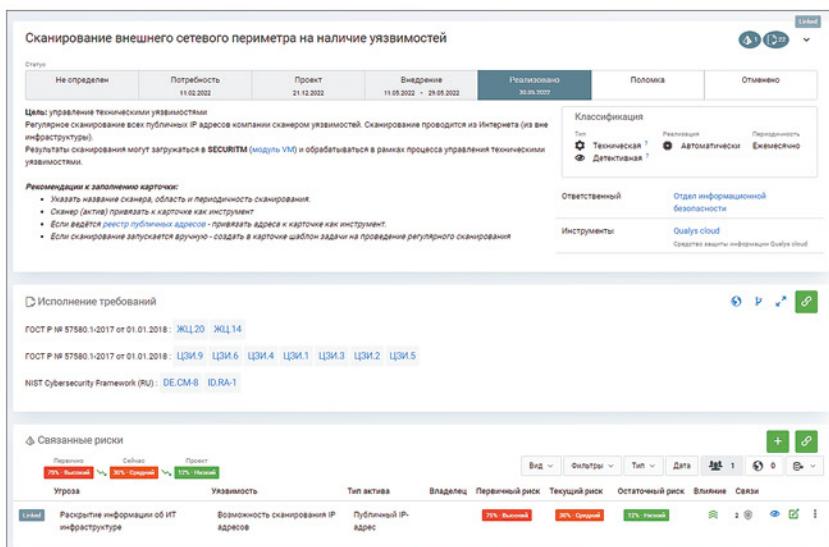


Рисунок 3. Карточка защитной меры

Но процессы защиты информации не ограничиваются лишь одной службой информационной безопасности, в них задействовано множество структурных подразделений с различными ролями: ИТ, риски, юристы, СВА и СВК — все они могут работать на платформе вместе, снижая транзакционные издержки на коммуникацию в почтах, мессенджерах, телефонных звонках и существенно оптимизируя работы всей организации.

В качестве примера рассмотрим требование ЖЦ.14 из ГОСТ Р 57580.1–2017 (рис.2). На карточке требования видны не только все аналогичные требования из других нормативов, взятых организацией на контроль, но и то, через внедрение каких именно защитных мер реализуется данное требование. Если часть мер

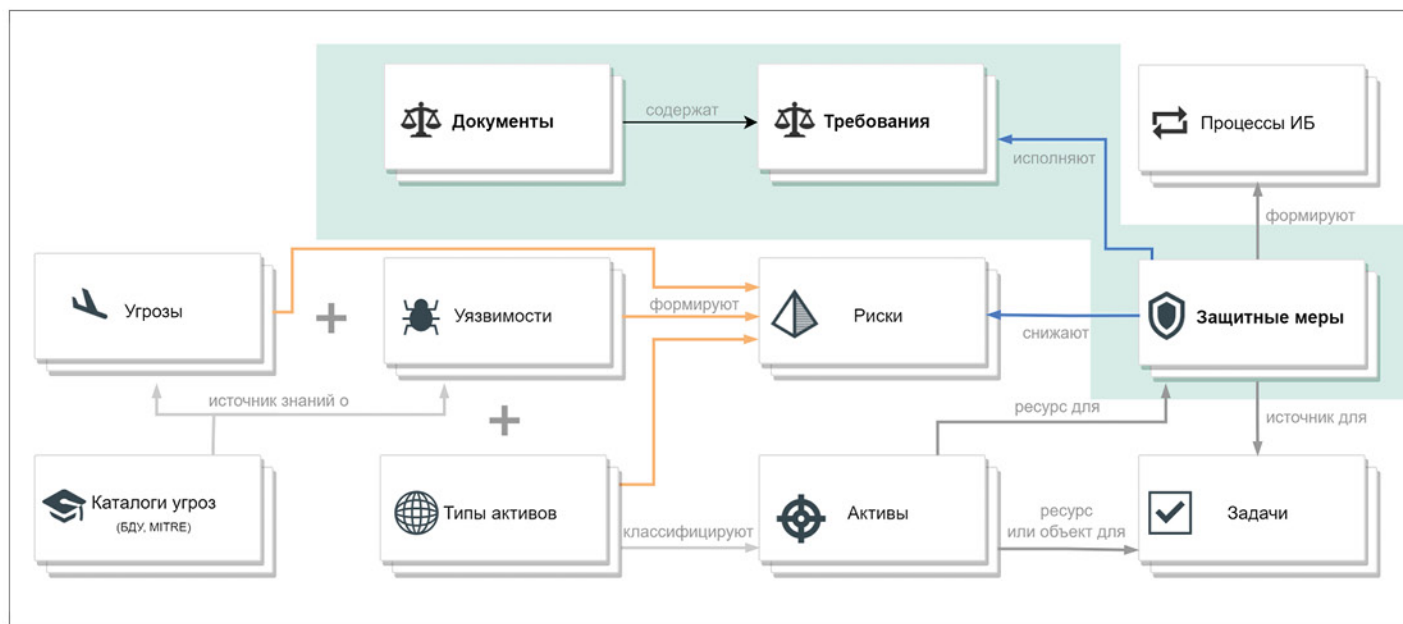


Рисунок 4. Место процесса управления соответствием в управлении безопасностью

еще не внедрена, то требование считается частично исполненным, что динамически отражается в текущих результатах оценки соответствия. То есть на базе продукта мы можем в любой момент времени получить актуальную самооценку по любому набору требований, в том числе комбинированную, основанную на различных наборах требований! Помимо этого, через карточку защитной меры (рис. 3) служба безопасности подробно описывает свою активность, направленную на исполнение требований и снижение рисков безопасности, распределяет ответственность, планирует работы и нарезает регулярные задачи. Таким образом, мы получаем ещё и органайзер задач, который позволяет получать уведомления о невыполненных работах, отслеживать сроки, коммуницировать с коллегами задачи и комментарии, а главное непрерывно оптимизировать систему защиты по заветам Деминга. А так как одна защитная мера может быть направлена на исполнение требований различных нормативов, то мы получаем ещё и экономию человеческого времени и сил, которые можно будет направить на занятия более полезные, чем синхронизацию всех требований всех применимых нормативов и коммуникацию в электронной почте, мессенджерах, телефонных звонках по выполнению всех необходимых контролей и процессов.

Таким образом, службы безопасности и другие структурные подразделения организации оказываются взаимосвязаны на стратегическом, тактическом и операционном уровнях. У каждого действия есть определенная причина и смысл.

И все они взаимосвязаны (рис. 4) по принципу **Документы → Требования → Защитные меры → Задачи и процессы.**

Если что-то выпадает из организованной системы, если какие-то задачи системы защиты не реализуются, если где-то возникают новые требования, система гибко адаптируется к изменениям, осуществляет перерасчет показателей и позволяет минимизировать человеческие ошибки и трудозатраты.

ВЫВОДЫ (РЕЗУЛЬТАТ)

Объединение аналогичных требований из различных стандартов и контроль их исполнения через ведение реестра защитных мер позволяют снизить ручной труд на первичную оценку соответствия, сократить сроки аудитов, минимизировать затраты при проведении последующих проверок, а главное централизовать управление системой защиты на базе единой платформы с базой знаний организации. Понимая чувствительность обрабатываемой в подобных системах информации, мы предлагаем не только облачную установку сервиса, но и возможность размещения копии SECURITM в инфраструктуре финансовой организации.

В результате организация получает процесс управления соответствием и требованиями ИБ, позволяющий:

- ◆ непрерывно контролировать соответствие множеству требований и документов;
- ◆ подтверждать соответствие перед внешними и внутренними аудиторами;
- ◆ избавиться от дублирующих операций, лишних разговоров и переписок, завести все комму-

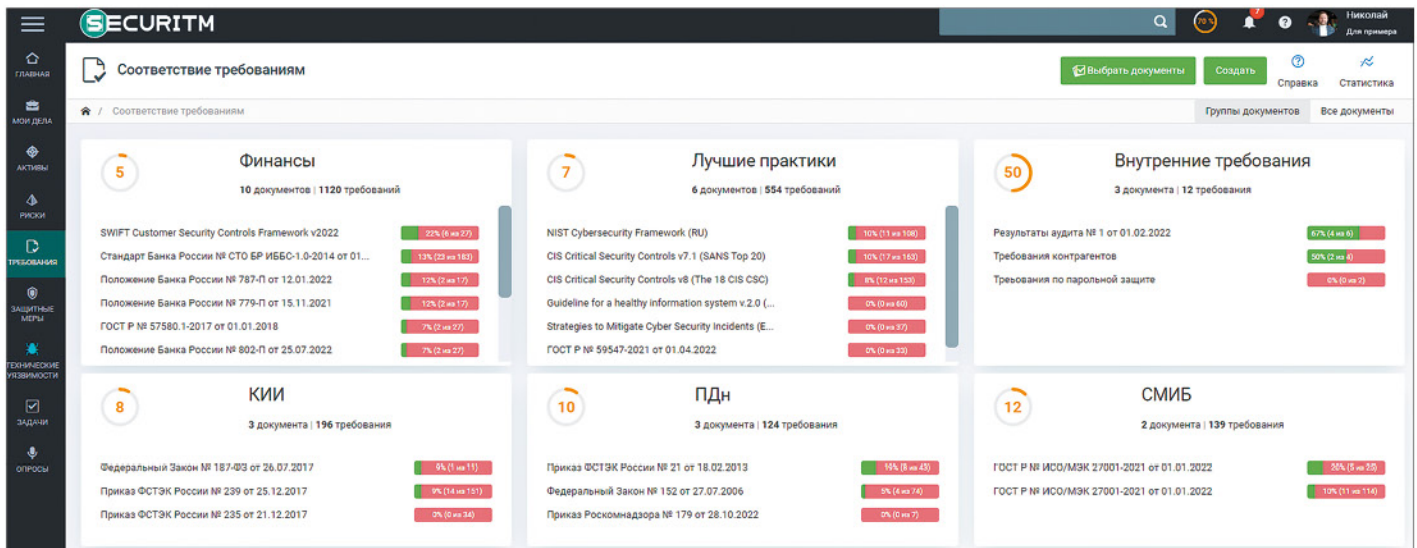


Рисунок 5. Одновременное управление соответствием по различным документам

никации в области ИБ на специализированную платформу, специально созданную для этих целей.

Результаты исследований по корреляции требований различных стандартов размещены в открытом доступе, (без регистрации и смс), это наш вклад в развитие сообщества служб безопасности. Там же размещаются проекты защитных мер и бесплатный доступ к Community версии инструмента SECURITM, на базе которого было проведено исследование.

Предлагаем всем присоединиться к наполнению базы проектов защитных мер, именно

благодаря такому упорядоченному обмену опытом количество переходит в качество, а будни CISO наполняются пользой.

По ссылке <https://service.securitm.ru/compliance> вы найдете инструмент, который сравнивает различные стандарты и формирует ТОП 10 требований (групп требований) по различным наборам стандартов. Он размещен в открытом доступе и теперь каждый может самостоятельно создать набор требований именно по тем стандартам, которые актуальны для его организации (рис. 5).

BIS-КОММЕНТАРИЙ

ПОМОЩЬ БАНКАМ. ОНА НЕ ЗА ГОРАМИ

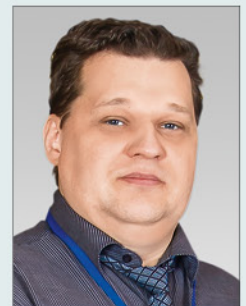
В старые добрые времена я делал многие excel-таблицы по разным нормативкам ЦБ (СТО БР, РС БР, 382-П, ГОСТ 57580, Swift, оценка рисков, СКЗИ и СЗИ и др.). Почти каждый сотрудник ИБ банка ими пользовался при проведении самооценок. А также в своей работе их использовали аудиторы. Но пришло время уступать дорогу.

SECURITM действительно может помочь ИБ-шнику любого банка (от большого до маленького). Чем мне этот продукт понравился? Тем, что он может быть использован не только банками РФ, но и банками СНГ — так как

данный продукт использует много международных требований (ISO 27 серии и др).

Если заглянуть в завтрашний день, то можно расширить данный функционал еще и на местные нормативные документы: Республики Беларусь (комплекс технических требований и правил ИБ: ТТП и других документов), Республики Казахстан (постановления Правления НБРК и др.) и т.д.

Я давно слежу за SECURITM и могу сказать, что команда разработчиков постоянно совершенствует свой продукт, добавляя функционал. Планов много. И это очень радует, что таким продуктом будут пользоваться во многих банках.



Александр ВИНОГРАДОВ
старший научный сотрудник
ФГУП «ЦНИИХМ»



Денис БАТРАНКОВ
член редколлегии BIS Journal

ЧТО ТАКОЕ NGFW

НЕДАВНИЕ КОНКУРЕНТЫ ВМЕСТЕ СОЗДАЮТ НОВЫЕ ПРОДУКТЫ ДЛЯ ЗАЩИТЫ СТРАНЫ

Отрасль информационной безопасности в России, к счастью, оказалась готова к режиму санкций со стороны западных стран. На протяжении последних 20 лет в стране активно развивалось сообщество по информационной безопасности — активными евангелистами «из народа», государством на уровне Государственной думы, Совета Федерации, ФСТЭК и ФСБ и, конечно, нашими разработчиками продуктов и сервисов, которые уже известны во всём мире: Group-IB, «Лабораторией Касперского», Positive Technologies. Поэтому в этой отрасли мы видим огромный рост числа новых решений, которые не уступают продуктам мирового уровня по экспертизе и качеству и готовы защищать как государственные организации, так и коммерческий сектор.

В 2022 году компании стали объединяться и делать совместные решения для защиты российских организаций; эксперты из компаний — недавних конкурентов вместе создают новые продукты для защиты страны. И одним из таких продуктов стал межсетевой экран нового поколения. Экспертность многих российских компаний позволяет реализовать это решение, что, в свою очередь, ведёт к серьёзному укреплению защиты государства. Разберём, что это за решение, более подробно.

НА ЧТО ФОКУСИРУЕМСЯ

Чтобы понять, что такое межсетевые экраны нового поколения (NGFW),

нужно разобраться в нескольких основных аспектах их работы: схема применения;

- ♦ удобство управления, визуализации и просмотра журналов;
- ♦ контроль приложений;
- ♦ контроль пользователей;
- ♦ функциональность сетевой безопасности;
- ♦ производительность.

СХЕМА ПРИМЕНЕНИЯ

NGFW применяется в корпоративной сети для разделения сетей с разными политиками безопасности и управления потоками данных на уровне приложений, включая контроль трафика сотрудников, подключённых по VPN, и трафика от серверов. В нашей модели рисков мы исходим из того, что внутри сети уже есть злоумышленники и взломанные устройства; иногда вредоносные действия совершает сотрудник или хакер от его имени. И NGFW создает среду нулевого доверия, где для совершения вредоносных действий нужны другие привилегии и доступы. А их нет.

С точки зрения сетевой топологии NGFW может выглядеть:

- ♦ как прозрачный кабель,
- ♦ как коммутатор с поддержкой VLAN,
- ♦ как маршрутизатор с поддержкой динамической маршрутизации,
- ♦ как HTTP-прокси или
- ♦ как MTA;
- ♦ как все это одновременно.

Все эти варианты повышают удобство интеграции NGFW в сеть. Сегодня

NGFW может работать на периметре, в ЦОД, с SDN, в АСУ ТП, в виртуализации, в Kubernetes, в облачных хранилищах.

Внутри всех NGFW особое внимание идет на трансляцию адресов (NAT). Это помогает вклиниваться в работу приложений, которые не понимают NAT, и подменять адреса не только на сетевом уровне, но и на уровне приложения. Например, это актуально для протоколов SIP и FTP.

Иногда один NGFW делят на несколько виртуальных: одно и то же устройство имеет разные наборы администраторов, правил и объектов для проходящего через него трафика на разных интерфейсах.

В NGFW чаще всего реализованы функции шлюза VPN, поскольку это помогает подключать своих сотрудников и сразу пропускать их через защитные фильтры устройства. У таких производителей есть собственные VPN-клиенты с расширенной функциональностью проверки клиентских устройств на соответствие политикам компании. Другой интересной особенностью является реализация SSL-VPN-шлюзов. Там клиент, наоборот, не нужен, и человек подключается к корпоративной сети и её приложениям через браузер.

Также существует схема применения NGFW как сервиса, когда провайдер предоставляет все функции защиты из облака как ежемесячную подписку с нужной производительностью. Когда такой NGFW используется для

Receive Time	From Zone	Source User	Destination	Destination Country	To Port	Application	Action	Rule	Session End Reason
03/21 11:23:57	L3-TAP	pancademo\rodney.padilla	72.233.107.115	United States	80	web-browsing	allow	General Web Infrastructure	aged-out
03/21 11:23:57	L3-TAP	pancademo\chris.angiolilli	74.125.164.214	United States	80	google-base	allow	General Web Infrastructure	aged-out
03/21 11:23:57	L3-TAP	pancademo\ruby.clarke	198.189.255.73	United States	80	incomplete	allow	IT Sanctioned SaaS Apps	aged-out
03/21 11:23:57	L3-TAP	pancademo\maria.pimentel	66.114.48.32	United States	80	linkedin-base	allow	Allowed Personal Apps	aged-out
03/21 11:23:57	L3-TAP	pancademo\mary.shishido	67.192.7.192	United States	80	incomplete	allow	IT Sanctioned SaaS Apps	aged-out
03/21 11:23:57	L3-TAP	pancademo\lucas.johnston	70.22.211.108	United States	47737	bittorrent	allow	Watch Risky Apps	aged-out
03/21 11:23:57	L3-TAP		10.154.10.20	10.0.0.0-10.255.255.255	53	dns	allow	Watch Public DNS and SMTP	aged-out

Рисунок 1. Пример журнала NGFW, где показаны аккаунты сотрудников, страны, порты, приложения

удалённого доступа к ресурсам компании и для защиты филиалов, то его называют Zero Trust Network Access (ZTNA).

УДОБСТВО УПРАВЛЕНИЯ, ВИЗУАЛИЗАЦИЯ И ЖУРНАЛЫ

С точки зрения удобства управления самый большой вопрос состоит в том, насколько легко и быстро ваши специалисты разбираются в настройках: и безопасники, и сетевики. Люди часто мне говорят о том, что NGFW помог им понять свою сеть, то есть в нём хорошо реализована визуализация происходящего.

Интерфейсы управления NGFW разных производителей отличаются стратегией обновления функционала. Кто-то сразу продумал структуру меню, и она не меняется уже много версий подряд. Кто-то сразу сделал одинаковым интерфейс локального управления и централизованного управления. Кто-то сделал управление через веб-браузер, а кто-то — из толстого клиента под Windows. Кто-то сделал удобный REST API, и продукт управляется через скрипты. На мой взгляд, удобнее всего управлять NGFW из любого браузера.

Первое, что включает любой пользователь, — запись всего, что видно в сети. Что отображается в журналах:

- ♦ запрещённые в компании приложения, например торрент-клиенты или майнеры;
- ♦ работающие по нестандартным портам приложения, например RDG или Elasticsearch;
- ♦ соединения от имени аккаунтов уволенных сотрудников;
- ♦ туннели разного типа в разные страны;

♦ получение исполняемых файлов из интернета, а не из внутреннего репозитория;

♦ информация о том, сколько сотрудников открывает сайты для поиска работы;

♦ множество вредоносных программ в почте и в вебе;

♦ устройства компании, подключённые к известным бот-сетям.

Я привёл эти примеры, чтобы показать, насколько много функций сегодня в NGFW. И это ещё не всё. У разных производителей разные функции, но при этом каждый называет себя NGFW. И у вас есть выбор: верить или проверить.

Таким образом, важное отличие NGFW от обычных межсетевых экранов — информативные журналы (рис.1). В NGFW каждое соединение сразу обогащено информацией:

- ♦ о пользователе, который его инициировал,
- ♦ странах, откуда и куда идёт подключение,
- ♦ приложении, которое генерирует этот поток,
- ♦ файлах, которые передаются в приложении,
- ♦ URL-категориях в каждом http(s)-запросе,
- ♦ об SSL-сертификатах,
- ♦ об угрозах, которые есть внутри потока данных.

Если вы можете с помощью журнала быстро диагностировать проблемы с сетью и с безопасностью, это то, что вам нужно от NGFW. Как пример неудобства: я знаю производителей, которые до сих пор создают журналы межсетевого экрана в виде TXT-файлов. Назвать этот метод из 90-х годов «следующим поколением» язык не поворачивается. Хотя они смогли.

КОНТРОЛЬ ПРИЛОЖЕНИЙ

NGFW особенно эффективно проявляет себя в анализе идущего из компании в интернет трафика и трафика от удалённых VPN-подключений. Около 25 лет назад было принято решение, что для идентификации приложений будут использоваться порты: 80 — HTTP, 443 — HTTPS, 25 — SMTP, 21 — FTP и так далее. Сегодня ситуация изменилась: внутри этих портов могут «ходить» любые приложения. Для примера: в одной из компаний мне сказали, что по 443-му порту у них выходит в интернет 173 разных приложения — файлообменники, веб-почта, мессенджеры, социальные сети, вебинары, бизнес-приложения и др. И NGFW «раскрасил» соединения по 443-му порту реальной информацией, кто чем из сотрудников пользуется, и позволил точно указать, каким приложениям по этому порту ходить можно, а каким нельзя. Если

Я знаю производителей, которые до сих пор создают журналы межсетевого экрана в виде TXT-файлов. Назвать этот метод из 90-х годов «следующим поколением» язык не поворачивается. Хотя они смогли

	Name	Source	Destination	Application	Service	Action	Options
		Address	Address				
1	Allow VNC and Apple Remote	any	any	apple-remote-desktop vnc	application-default	Allow	
2	Required Infrastructure Apps	any	any	ntp ocsp ping stun	application-default	Allow	
3	SaaS Apps	any	any	boxnet gotomeeting jobvite salesforce	application-default	Allow	
4	Youtube Access	Marketing-Department	any	google-base youtube	application-default	Allow	
5	Allow MS-Lync Only	any	any	ms-lync	application-default	Allow	

Рисунок 2. Пример политики по приложениям в Palo Alto Networks NGFW. Важно, что настройка application-default позволяет разрешить несколько приложений в одном правиле на их портах по умолчанию

у вас портовый межсетевой экран, то он позволит либо запретить все приложения, либо разрешить одновременно по этому порту. В большинстве компаний просто разрешены все приложения наружу по 443-му порту. Раньше пытались решить эту задачу использованием прокси-серверов, но многие приложения через прокси не работают, поэтому в прокси множество исключений. И это прекрасный канал для утечек информации.

Сейчас даже легитимные приложения используют туннелирование через другие приложения. И именно этот аспект начали учитывать межсетевые экраны нового поколения. Они позволяют определить, что по стандартному порту для HTTP (порт 80) сейчас идёт трафик другого приложения, отличный от HTTP, например Skype. NGFW позволяет увидеть туннели внутри DNS и ICMP, распознать трафик сложных приложений типа TeamViewer, Tor, Telegram и явно запретить или разрешить эти приложения и туннели. Такую функциональность

называют Deep Packet Inspection (DPI), что означает, что мы смотрим не просто в заголовки сетевых пакетов, а в их содержимое и понимаем, что там.

Обнаружение приложений есть в отдельных устройствах класса DPI, например компании Allot или Sandvine. Их не называют NGFW, потому что, кроме обнаружения приложений, им нужны ещё другие сервисы безопасности, например идентификация пользователей и IPS. Самый важный критерий для вас при выборе NGFW, что приложение является критерием политики безопасности, а не просто визуализируется. Если критерием политики является порт TCP или UDP, то это обычный портовый firewall.

Обнаружение приложений входит в функциональность Check Point Security Gateway версии 77, но его не называют NGFW, потому что там приложение нельзя сделать критерием политики; приложения там управляются в отдельном окошке — отдельно от основного окна с политиками. Приложения стали

критерием политики безопасности в политиках продуктов Check Point версии 80 и выше. И его уже можно назвать NGFW.

Обнаружение приложений также входит в функциональность файрвола Fortinet в режиме profile mode, однако это не NGFW, поскольку там критерием политики является порт. Приложениям там выделен специальный профиль защиты, но профиль срабатывает, когда трафик по порту уже пропущен. То есть это режим фильтрации по портам, а не по приложениям.

Для фильтрации по приложениям в файрволе Fortinet есть специальный режим NGFW policy mode, в котором приложение является критерием политики безопасности. То есть внутри продукта Fortinet на самом деле прячется несколько типов межсетевых экранов: портовый файрвол, файрвол приложений и HTTP-прокси. Пока мне не встречались люди, кто настроил бы Fortinet в режиме NGFW policy mode. Объявляю вознаграждение — бутылку французского коньяка — тому, кто первым покажет мне, что он настроил Fortinet в режиме NGFW в продуктивной сети. Жду до декабря 2023 года.

Palo Alto Networks была новичком на рынке, и уже в первой версии они сразу сделали NGFW, в котором приложение всегда является критерием политики. Собственно, они и придумали термин NGFW (рис. 2).

Сейчас даже легитимные приложения используют туннелирование через другие приложения. И именно этот аспект начали учитывать межсетевые экраны нового поколения

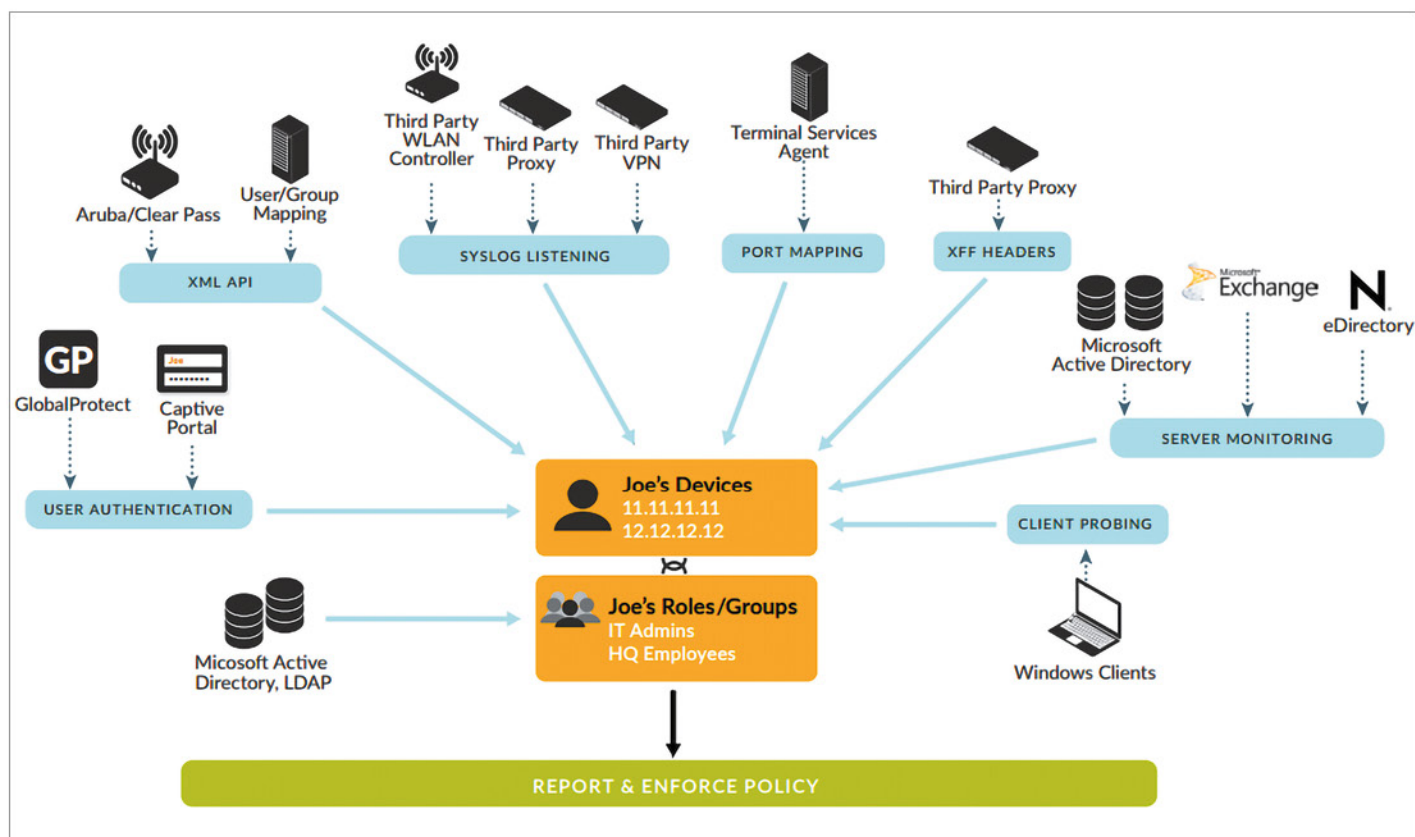


Рисунок 3. Пример источников для получения информации о пользователе, его группе и IP-адресе

КОНТРОЛЬ ПОЛЬЗОВАТЕЛЕЙ

Сотрудники компании перемещаются по миру. Они подключаются через Wi-Fi с ноутбуков, заходят с различных рабочих станций, работают через VDI, подключаются по VPN из дома и в командировках. Однако для одной группы пользователей нужен доступ к серверу «1С», для другой — к маршрутизаторам, для третьей — к базе данных кадровиков и так далее. Чтобы реализовать такой ролевой доступ на сетевом уровне, используются правила по именам и группам пользователей в NGFW. Иногда для такой функциональности встречается термин *identity firewall*.

Для функционирования *identity firewall* в NGFW работает агент, который отслеживает аккаунты сотрудников компании, группы, к которым они принадлежат, и IP-адреса, по которым они сейчас находятся. Чаще всего эту информацию заимствуют из Active Directory, потому что каждый вход сотрудника в сеть журналируется, и в нём записано соответствие аккаунта и IP-адреса.

Если сотрудники работают на терминальном сервере, то получается, что с

одного IP-адреса их будет несколько. Для этого на терминальный сервер ставится агент, который «разбрасывает» пользователей на разные диапазоны портов, и поэтому NGFW тоже может различать пользователей и по адресу, и по порту (рис. 3).

ФУНКЦИИ БЕЗОПАСНОСТИ

Функции безопасности влияют на эффективность защиты и возможности вашей команды управлять рисками в сети. Причём не только рисками при работе браузеров, как это делает прокси-сервер, но и всеми приложениями: голос, видео, управляющие протоколы. И тут важно понимать, откуда ваш NGFW берёт экспертизу: из собственной лаборатории или из покупных баз. Чаще всего, если исследовательская лаборатория у производителя собственная, вы чаще получаете обновления, да и устройство оказывается дешевле.

Основная функциональность, которую используют в NGFW, — функциональность системы предотвращения атак (IPS). Некоторые компании переживают за ложные срабатывания и пользуются NGFW в режиме IDS (без

блокировок). В интернете можно найти тесты качества этой функциональности.

Следующей важной функцией для периметровой защиты является URL-фильтрация по категориям сайтов. Здесь производители идут двумя путями: кто-то реализовал фильтрацию в виде прокси-сервера, то есть терминирует на себе все HTTP-соединения, а кто-то реализует проверку и фильтрацию URL в прозрачном режиме. Как показывает практика, в прозрачном режиме URL-фильтрация работает быстрее. Во многих компаниях HTTP-прокси работает как отдельное устройство защиты. Иметь URL-фильтрацию только через HTTP-прокси не очень хорошо, потому что URL-ссылки встречаются в разных типах трафика: в SMTP, в POP3, IMAP, и их там тоже надо проверять, — это реализовано только в NGFW, но не реализовано в прокси.

Дополнительной функцией является работа потокового антивируса и песочницы. Поскольку NGFW видит файлы в различных протоколах, например HTTP, SMTP, SMB, то он имеет возможность проверять эти файлы имеющимися у него сигнатурами или

хешами. У Fortinet и Cisco используются хеши файлов, у Check Point и Palo Alto Networks используются сигнатуры. Сигнатуры эффективнее: одна сигнатура позволяет обнаруживать множество вариантов вредоносных файлов.

Ещё одна функция — проверка индикаторов компрометации. Поскольку обнаружение бот-сетей по IP-адресу, DNS и URL эффективно работает, так же как и обнаружение других вредоносных ресурсов, то NGFW часто может заблокировать подключения к таким ресурсам, получая фиды с индикаторами от поставщиков threat intelligence.

Многие понимают, что функциональность обнаружения атак и проверки файлов упирается в то, что большая часть трафика на периметре зашифрована TLS-протоколом — до 80%. Поэтому ещё одной важной функцией безопасности NGFW является расшифрование TLS на основе подмены сертификата. Какое-то время эта функция рассматривалась как важная, однако сейчас подмене сертификата TLS сопротивляется всё больше и больше приложений: вы не можете вклиниваться в трафик вебинаров, мессенджеров, обновлений. В итоге заказчики говорят, что сегодня получается расшифровать 50% имеющегося объёма TLS трафика — и это хорошо.

Расшифрование TLS нужно, чтобы отдать трафик на остальные движки безопасности: URL-фильтр, IPS, антивирус, песочницу. В некоторых устройствах есть возможность отдавать расшифрованный трафик на внешние устройства, например на внешний DLP.

Нужно учитывать, что TLS-расшифрование серьёзно нагружает NGFW и снижает его производительность. Вы можете посмотреть данные поставщиков о производительности с включённым и выключенным режимом расшифрования TLS. Эти данные обычно заставляют меня улыбнуться, потому что все пишут показатели производительности с выключенными остальными движками безопасности: URL, антивирусом, песочницей и другими. А если включить?

В некоторых NGFW реализовано ещё и расшифрование протокола SSH, чтобы увидеть внутри него туннелирование других приложений.

В качестве бонуса в NGFW бывают включены различные технологии сетевого DLP. Например, блокировка файлов по типам, или поиск номеров кредитных карт и номеров телефонов, или морфологический анализ.

У некоторых производителей включена функция проверки спама и вирусов в сообщениях электронной почты в режиме mail transfer agent (MTA). Это позволяет перенаправлять электронную почту через устройство по SMTP, но эта функция катастрофически нагружает устройство, поэтому в NGFW это мало у кого сделано.

HTTP- и FTP-прокси-сервер сегодня реализован почти у всех производителей. Связано это в основном с историей развития: сделали прокси-сервер, ещё когда все межсетевые экраны были портовыми, а уже надо было анализировать приложение HTTP. Это медленная функция, которая серьёзно проигрывает в производительности прозрачной проверке URL-запросов в HTTP-трафике. Поскольку прокси-сервер работает с потоками данных «в разрыв», то он может даже что-то менять, добавлять или удалять в запросах и ответах. Если в вашей сети действительно требуется работать с трафиком через прокси-серверы, то логичнее взять его как отдельное устройство.

ПРОИЗВОДИТЕЛЬНОСТЬ

Что касается производительности, тут всё просто: нужно понять, способен ли межсетевой экран выполнить возложенные на него функции, обеспечив нужную для вашего предприятия пропускную способность с нужным включённым функционалом. Основным месседжем производителей всегда являлось использование аппаратного ускорения. Опыт показал, что производительность достигается за счёт оптимального написания кода, и тогда даже на стандартной архитектуре можно реализовать значительную скорость анализа трафика. Например, однопроходный движок анализа трафика у Palo Alto Networks в системах виртуализации достигает скорости 16 Гбит/с на одном виртуальном NGFW с функционалом контроля приложений, пользователей, IPS, антивируса и Threat Intelligence. И никаких

ускорителей там нет. Даже наоборот, там есть гипервизор, который даёт дополнительную нагрузку на серверные мощности.

В мире всего четыре иностранных производителя, кто использует ускорители:

- ♦ компания Palo Alto Networks использовала чипы Cavium и FPGA для ускорения разбора трафика приложений, TLS Decrypt, IPS и антивируса;
- ♦ компания Fortinet использует ASIC собственного производства: различные разновидности под названиями NP, CP, SOC;
- ♦ компания Cisco использовала чипы ускорения для IPsec;
- ♦ компания Juniper использовала специальную плату ускорения для SSL Decrypt.

Компания UserGate также создала платформу на основе Cavium, но санкции помешали его использованию. Остальные производители, например Check Point и Sangfor, используют обычные серверы x86.

ЗАКЛЮЧЕНИЕ

Здравая идея объединить несколько функций в одно устройство с единой системой управления вылилась в устройства класса unified threat management (UTM). Проблемой этих устройств было то, что движки внутри были написаны разными компаниями, и они плохо стыковались друг с другом. NGFW появился позже, когда выяснилось, что если запрограммировать в одной компании сразу все функции одним единым модулем, то повышаются и безопасность, и производительность.

Таким образом, NGFW — это подмножество UTM-устройств. При этом новыми функциями в NGFW стали правила по приложениям и пользователям, и это важный критерий выбора. И они должны быть вашим критерием выбора. Но также важно, чтобы у производителя были и остальные функции безопасности; проверяйте, чтобы все эти функции при включении обеспечивали нужное вам хорошее качество защиты на нужной вам скорости передачи трафика.

И ещё раз подчеркну: обязательна удобная единая система управления и журналирования.

NGFW КАК КЛЮЧЕВОЙ ЭЛЕМЕНТ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ



Владимир УЛЬЯНОВ
аналитик
по кибербезопасности

В материале приводятся характеристики и краткое описание мирового и российского рынков межсетевых экранов следующего поколения (NGFW), а также обзор новой версии Zecurion NGFW для замены продуктов, ориентированных на сегменты Enterprise и крупных государственных заказчиков.

Идея вынесения средств кибербезопасности как можно дальше на внешний край периметра не нова. Можно сказать, что рынок движется к её реализации с момента своего зарождения, когда в светлые головы создателей локального антивируса впервые пришла идея проверок по сети. В XXI веке роль форпоста информационной безопасности долгое время выполняли классические межсетевые экраны, фильтрующие пакеты на основании заголовков, проверяемых по стоп-листам или спискам доверенных ресурсов. Тактика простая и надёжная, но эффективная лишь для самых простых, массовых атак. Как фильтр первичной очистки трафика, но не более.

В основе Next Generation Firewall (NGFW) лежит логичное развитие идеи межсетевого экрана — выявить и заблокировать как можно больше вредоносного (или просто ненужного) контента ещё до того, как он попадёт в доверенный сегмент сети. Для этой цели файрвол не только смотрит заголовки, но и анализирует, разбирает рабочую нагрузку пакета. Понимание того, что конкретно содержит входящий и исходящий сетевой трафик, открывает широкие возможности для его фильтрации — от типового сигнатурного анализа до контроля данных на уровне веб-приложений.

Перспективный подход впервые предложила компания Palo Alto Networks, которая до сих пор считается од-

ним из лидеров рынка NGFW, однако за прошедшие с 2008 года 15 лет в этом сегменте стало весьма тесно — только лишь «Магический квадрант» Gartner сейчас насчитывает 17 игроков, среди которых такие гиганты, как Microsoft, Amazon, Alibaba и Huawei.

К наиболее продвинутым решениям аналитики Gartner относят следующие разработки:

- ◆ FortiGate: Next Generation Firewall (NGFW) компании Fortinet;

- ◆ Check Point Quantum компании Check Point;

- ◆ Аппаратные (PA-Series), виртуальные (VM-Series), облачные и контейнерные файрволы компании Palo Alto Networks;

- ◆ Cisco Secure Firewall компании Cisco.

Это «универсальные солдаты» рынка, комплексные решения, нацеленные на покрытие потребностей как можно более широкого числа заказчиков.

Другая сторона медали представлена нишевыми игроками, пытающимися как можно более точно заточить свой продукт под нужды определённого сектора рынка:

- ◆ Sophos, нацеленный на предприятия среднего размера, делает ставку на глубокую интеграцию с собственным EDR;

- ◆ SonicWall, предлагает встроенные в файрвол функции SD-WAN и работает по сервисной модели обслуживания (FWaaS, Firewall as a Service);

- ◆ WatchGuard, ориентируется на территориально-распределённые сети и работу с публичными облачными средами.

ОСОБЕННОСТИ РОССИЙСКОГО РЫНКА NGFW

Если же говорить о российском рынке Next Generation Firewall, то, несмотря

на популярность и где-то даже перегретость темы, можно отметить некоторые типовые проблемы, свойственные отечественным решениям этого сегмента. В первую очередь речь идёт о качестве и полноте защиты от внешних угроз. К сожалению, несмотря на громкие декларации, некоторые системы не так уж далеко ушли от классических межсетевых экранов, представляя собой не более чем гибрид последних с обыкновенным антивирусом. Между тем NGFW должен не только выполнять сигнатурный анализ, но и хорошо ловить боты, рекламу, разбираться с фишингом, выявлять неизвестные угрозы, а также обрабатывать исполняемые файлы и блокировать нежелательный контент.

Ещё одна точка роста для российских систем — недостаточная производительность. Технологии вообще играют ключевую роль в сфере NGFW, поскольку разбор и фильтрация на лету огромного массива данных — задача, безусловно, нетривиальная. Если учесть, что большая часть трафика ещё и зашифрована, то отдельные файрволы способны «положить сеть» даже при относительно небольшой нагрузке. Крупным компаниям с большим числом филиалов требуется NGFW, обладающий передовыми технологиями обработки трафика и балансировки нагрузки, без запредельных системных требований, что особенно важно в свете нынешних сложностей с поставкой аппаратных средств.

ZECURION NGFW — НОВЫЙ ИГРОК В СЕГМЕНТЕ

В 2023 году компания Zecurion выпускает NGFW Enterprise-уровня. Продукт, нацеленный на замену топовых мировых решений в крупнейших организа-



циях. Важно, что он разрабатывался на протяжении нескольких лет в рамках долгосрочной продуктовой стратегии Zecurion, а не является быстрым ответом на потребность, возникшую на российском рынке в 2022 году с уходом зарубежных ИБ-вендоров. Разберём его подробнее.

Zecurion NGFW является логическим развитием Zecurion SWG (Secure Web Gateway). Эта система появилась на рынке под названием Zproху ещё в 2014 году и была призвана заменить отживший своё Microsoft Forefront Threat Management Gateway. Помимо классических функций прокси-сервера, Zproху умел идентифицировать пользователей Active Directory, поставлял в DLP данные разбора зашифрованного трафика и имел механизм контроля доступа к интернет-ресурсам на основе правил.

Вышедший тремя годами позже Zecurion SWG проверяет трафик по базе URL, насчитывающей более полумиллиарда сайтов, разбитых на сто с лишним категорий, а также способен контролировать использование интернета сотрудниками компании, запрещая доступ к веб-ресурсам определённых тематик. Помимо этого, что уже не совсем укладывается в функции классического файрвола, Zecurion

SWG обладает базовыми возможностями систем обнаружения вторжений (IDS) и работает с внешними решениями для проверки трафика, обмениваясь с ними данными по протоколу ICAP. Продукт пользуется спросом и хорошо зарекомендовал себя при работе в крупнейших российских организациях на нагрузке в десятки тысяч рабочих мест как средство контроля доступа в интернет и защиты от ряда угроз и один из элементов эшелонированной системы безопасности предприятия.

Новый Zecurion NGFW несёт на борту все функции SWG и дополнительно предоставляет заказчику:

- ◆ полноценный межсетевой экран уровня L7;
- ◆ встроенную систему СОВ (IDS/IPS);
- ◆ технологии и архитектуру, рассчитанные на работу в крупных распределённых информационных системах;
- ◆ антивирус с возможностью выбора из нескольких доступных решений российских разработчиков;
- ◆ функции защиты почты от спама и внешних угроз;
- ◆ криптошлюз и безопасный удалённый доступ (VPN);
- ◆ базовые инструменты Web Application Firewall;

◆ механизм управления доступом, интегрированный с различными службами каталогов.

По сути, функциональные возможности системы соответствуют уровню ведущих средств защиты периметра от внешних угроз из правой верхней четверти квадранта Gartner — Check Point Quantum, Fortinet NGFW, разработки Palo Alto Networks. Безусловно, приведённым выше перечнем списком возможностей Zecurion NGFW не исчерпывается.

ИНТЕРФЕЙС И ПОЛИТИКИ ZECURION NGFW

Управление и настройка всех элементов Zecurion NGFW осуществляется из единой консоли, которую можно открыть в любом браузере. Эта консоль едина для всех продуктов вендора, что обеспечивает быстрый старт и привычное рабочее место для администратора системы. Логика отчётов и уведомлений, расположение элементов управления и другие блоки будут понятны и знакомы тем, кто уже работал с продуктами Zecurion. Однако внешним сходством дело не ограничивается, NGFW встроен в экосистему безопасности разработчика. Продукты могут обмениваться данными по ICAP, а также взаимно обогащают информацию

сведениями об угрозах, собираемыми со своих сенсоров.

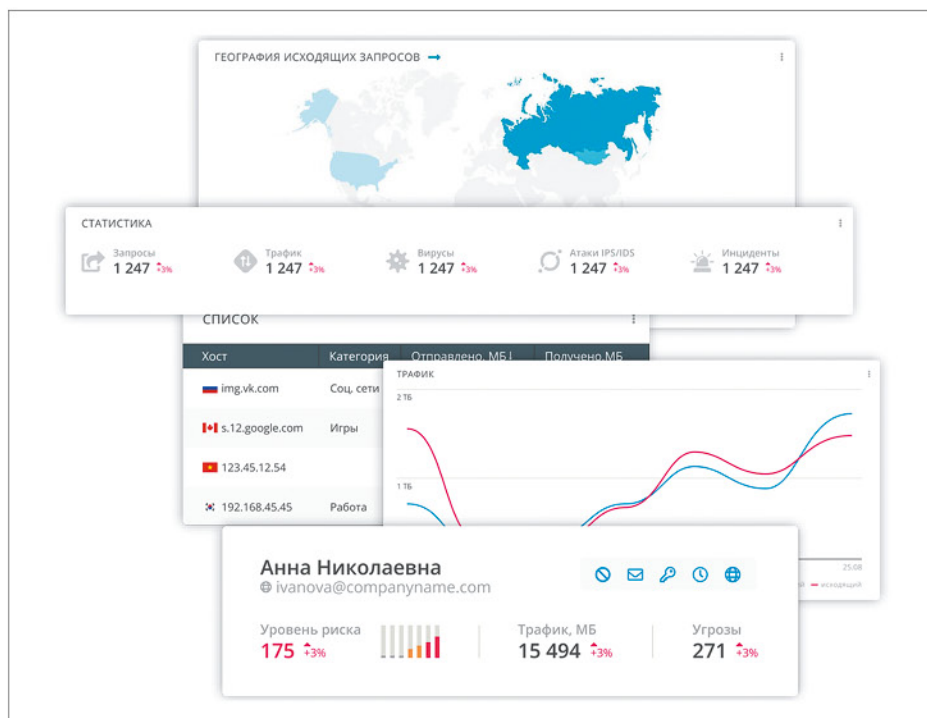
Отдельного упоминания заслуживает многослойная система политик безопасности на основе правил. В качестве условий правила могут выступать веб-ресурсы, геолокация, параметры авторизации, протоколы, сотрудники и другие объекты. Для удобства работы они упакованы в отдельные справочники. Задание параметров правил через единые сущности — справочники объектов — стандартизирует и существенно облегчает формирование политик вне зависимости от области их применения внутри системы.

Реакцию правила на выполнения условия, в свою очередь, формируют действия — по сути, список технологий, которыми обладает NGFW. Таким образом, при наступлении определённого события система может включить режим фильтрации контента, активировать антивирус или IPS, отправить уведомление, подключить WAF — администратору доступно почти два десятка различных вариантов реагирования.

Последовательность выполнения правил определяется политиками. Каждая политика содержит несколько слоёв, по сути, веток выполнения правил, что позволяет создавать весьма сложные сценарии работы системы, основанные на выполнении множества условий. Получается стройная, понятная и прозрачная модель конфигурирования даже при нескольких сотнях правил — объекты и действия являются основой правил, которые, в свою очередь, формируют политики. Такая система построения обеспечивает удобство создания и поддержания актуальности сложных политик, прозрачность их использования и будет особенно востребована службами информационной безопасности крупных организаций. Естественно, администратор может выбирать область действия политики, ограничивая её отдельным шлюзом или же распространяя её на группу и всю сеть полностью.

ТЕХНОЛОГИИ

Zecurion NGFW несёт на борту полный спектр технологий защиты от внешних угроз. В первую очередь это мощный



межсетевой экран, способный работать на седьмом уровне OSI (разбор протоколов приложений), а также обрабатывать зашифрованный трафик на уровне как глобальных (SSL/TSL), так и отечественных (ГОСТ) криптопротоколов. Всего же на вооружении системы глубокого разбора пакетов данных (DPI) Zecurion более трёх сотен протоколов — от стандартных и общеупотребимых, включая мессенджеры и VPN, до экзотических вроде DisneyPlus и Florensia.

Система обрабатывает маркеры DDoS-атак на основании обновляемых в режиме реального времени справочников с использованием настраиваемой системы квот и ограничений. Встроенный IDS/IPS распознаёт сигнатуры вредоносного трафика на базе правил, подгружаемых с онлайн-серверов или сформированных пользователем. Помимо сигнатурного анализа, используются данные об аномалиях трафика, что позволяет выявлять и блокировать ранее неизвестные вектора атаки. Ещё одним вариантом реакции NGFW может быть активация модуля блокировки рекламы, который удаляет промобаннеры со страниц сайтов, снижает вероятность взаимодействия пользователя с фишинговым объявлением и экономит трафик.

Zecurion NGFW фильтрует контент по нескольким направлениям:

- ♦ стандартный сетевой трафик проверяется на наличие объектов, подпадающих под действия отечественных и зарубежных регламентов (152-ФЗ, ПП, GDPR и другие);

- ♦ трафик на уровне приложений «из коробки» разбирается для более чем 2000 наиболее распространённых отечественных и зарубежных веб-сервисов (включая Yandex, Zoom, Office 365, Mail.ru, Telegram и другие);

- ♦ почтовый шлюз контролируется антивирусом и системой блокировки спама с возможностью реагирования как по адресным базам, так и по составу вложений.

Не каждый зарубежный продукт, успешно продвигаемый на глобальном рынке, может похвастаться таким набором технологий «под капотом». С учётом высокой планки по производительности и архитектуры решения Zecurion NGFW сможет стать ориентиром в своём классе для крупного бизнеса.

АРХИТЕКТУРА СИСТЕМЫ

Пару слов об архитектуре Zecurion NGFW. Как мы уже писали выше, она изначально заточена на работу в территориально распределённой инфраструктуре крупной организации.



Балансировка системы настраивается через уже знакомый нам механизм правил — администратор создаёт кластер, состоящий из набора узлов, и, выбирая параметры реагирования на определённые действия, описывает, как по ним будет распределяться нагрузка. При перегруженности или временной недоступности отдельных узлов кластера нагрузка может быть перераспределена на другие ноды. Администратор может в режиме реального времени получать данные о загрузке серверов и, при необходимости, самостоятельно перераспределять трафик на резервные узлы.

Вся сетевая инфраструктура, задействованная в работе файрвола, управляется централизованно, журналы могут храниться как на едином сервере, так и на разных хостах. Для ускорения настройки администратор может задавать для отдельных узлов и целых кластеров заранее предопределённые роли, такие как шлюз безопасности, лог-сервер, сервер управления и другие.

В качестве ещё одной фишки Zecurion NGFW отметим возможность построения на его основе виртуальной защищённой сети и каналов связи между офисами. Встроенный криптошлюз даёт возможность прокидывать Site-to-Site тоннель третьего уровня OSI на базе IPsec. Для шифрования используются алгоритмы AES-128/256, 3DES 168, CAST 128 и другие, в том числе и отечественные криптоключи на базе различных серий ГОСТ. Точно так же как и с обычным трафиком: зашифрованный канал может оперативно распределять нагрузку между несколькими аппаратными платформами и в случае сбоя переключаться на резервные каналы. В данный момент Zecurion NGFW использует сторонний VPN-клиент, однако ближе к концу года разработчик планирует выпустить собственное

кроссплатформенное решение для установки на конечных точках.

Zecurion NGFW поставляется как в виде программно-аппаратного комплекса (ПАК), так и в варианте Virtual Appliance с возможностью развёртывания в различных инфраструктурах, в том числе на гипервизорах VMware или Microsoft Hyper-V. Насколько нам известно, вендор активно работает в сторону портирования файрвола на отечественные ОС, а также готовит обновление аппаратной платформы с учётом максимально возможного в текущих условиях уровня импортозамещения — уже проводится расширенное тестирование на российских процессорах и доводка под перспективное отечественное железо.

ПЕРСПЕКТИВНЫЙ ПРОДУКТ С СИЛЬНЫМ БЭКГРАУНДОМ

В заключение отметим ещё раз наиболее интересные особенности Zecurion NGFW:

- ♦ архитектура системы, рассчитанная на работу в Enterprise-сегменте;
- ♦ широкие возможности кластеризации и балансировки нагрузки в сетях с сотнями тысяч рабочих мест;
- ♦ удобная и понятная система многослойных политик на основе правил, объектов и действий;
- ♦ контроль трафика на уровне приложений для более чем 1000 отечественных и зарубежных сервисов, от «ВКонтакте» до Skype;
- ♦ встроенная система обнаружения вторжений с возможностью оперативного реагирования на события;
- ♦ мониторинг почтового трафика с использованием антивируса и антиспам-модуля.

В ближайших планах Zecurion — существенное расширение наборов протоколов балансировщика нагрузки с кратным увеличением пропускной

способности системы. Возможность объединения шлюзов безопасности в собственное приватное облако для автоматизации и повышения скорости распределения нагрузки. Система маршрутизации Zecurion NGFW в ближайшем будущем, несмотря на «безопасный фокус» решения, будет расширяться.

Zecurion NGFW уже включён в реестр российского ПО Минцифры. 28 декабря 2022 года было подписано постановление Правительства № 2461, предполагающее добавление в реестр и ПАК, в связи с чем в 2023 году можно ожидать добавления туда доступных конфигураций. Продукту также предстоит сертифицироваться по перспективным требованиям ФСТЭК, что не препятствует пилотированию системы у первых клиентов.

Подытожим. Российский рынок сетевой безопасности получил перспективного и сильного игрока с продуктом, разработанным на технологическом фундаменте вендора с мировой репутацией (продукты Zecurion ранее включены аналитиками Gartner, IDC, Forrester в число ведущих мировых в своих сегментах). По своим возможностям Zecurion NGFW сможет стать достойной заменой ведущим мировым продуктам. Соответственно, основным целевым сегментом продукта будет enterprise-бизнес и крупные государственные заказчики с высокими требованиями по производительности и функциональности. Впрочем, с учётом широкой линейки и разных вариантов поставки для Zecurion будет открыт и сегмент СМБ, особенно если цена окажется ненамного выше уровня российских конкурентов.



Дмитрий СЛОБОДЕНЮК
коммерческий директор
ARinteg

ARZip от ARinteg

КАК ИНТЕГРАЦИЯ АРХИВАТОРА С DLP ПОВЫШАЕТ ВОЗМОЖНОСТИ СИСТЕМЫ И УПРОЩАЕТ ЖИЗНЬ ОФИЦЕРА ПО БЕЗОПАСНОСТИ

Современные DLP-системы уже давно вышли за рамки своего базового функционала. Для чего необходимо защищать информацию, в целом понятно. В случае с DLP это позволяет сократить убытки от утечек информации. А вот для чего связывать архиватор с DLP? Для тех же целей.

При работе с большими файлами сотрудники часто отправляют запароленные архивы через корпоративные каналы связи. При стандартной схеме работы DLP-система, не получая доступа к такому файлу, отправляет его в карантин, после чего уже офицер безопасности в ручном режиме принимает решение разрешить или запретить пересылку.

ARZip от ARinteg — единственный находящийся в реестре отечественного программного обеспечения архиватор, позволяющий офицеру по безопасности, через консоль управления, создавать и менять мастер-пароли для организации взаимодействия с DLP-системой через restAPI.

Таким образом, с помощью мастер-пароля, система контроля всегда имеет доступ к файлам, находящимся в зашифрованном архиве, и самостоятельно принимает решение запретить или разрешить отправку файлов, исходя из настроек DLP, принятых в компании.

ARZip — это архиватор для MS Windows и Astra Linux, средство создания и управления архивными файлами. Имеется версия с графическим интерфейсом пользователя.

Оболочка ARZip имеет два основных режима работы: режим управления файлами (выводится список файлов и папок в текущей папке) и режим управления архивами (выводится список файлов и папок в архиве). В режиме управления файлами производится работа с файлами и папками, находящимися в папке (в том числе добавление их в архив), а в режиме управления архивами — с файлами и папками, находящимися в архиве (в том числе извлечение их из архива).

Функциональные возможности ARZip:

- ♦ архивирование ZIP;
- ♦ разархивирование ZIP, RAR;
- ♦ просмотр содержимого файлов, в том числе заархивированных;
- ♦ запуск программ непосредственно из архива (например, установка новой программы без распаковки дистрибутива);
- ♦ другие дополнительные функции, например, добавление архивных комментариев, протоколирование ошибок.

Функционал архиватора постоянно расширяется, в том числе посредством использования поддерживаемой им модульности. Цель расширения функционала — поддержка дополнительных алгоритмов сжатия, включая модули, использующие существующие алгоритмы архивации и разархивации.

Расширение функционала осуществляется пользователем за счет добавления загруженных с веб-сайтов разработчиков упомянутых алгоритмов (или с сайта правообладателя ПО).

Хотите получить консультацию от специалиста и заказать бесплатную демоверсию ARZip? Обратитесь напрямую к производителю. ARinteg — российский разработчик собственных решений и системный интегратор, предоставляющий полный комплекс экспертно-аналитических, технических и консалтинговых услуг в сфере информационной безопасности и широкий спектр ИТ-сервисов на основе надежного программного обеспечения и оборудования.





Яков ГРОДЗЕНСКИЙ
руководитель направления
информационной безопасности СТИ

ЗАЩИТА ОТ СКРЫТЫХ АТАК

ИЛИ КАК НАЙТИ ЧЁРНУЮ КОШКУ В ТЁМНОЙ КОМНАТЕ

По оценкам аналитиков, общий объём рынка ИБ в России за 2022 год достиг 160 млрд руб. Несмотря на серьёзные цифры бюджетов, затрачиваемых на информационную безопасность, ущерб от киберпреступлений остаётся колоссальным. Статистика подсказывает, что минимальное время проникновения в компьютерную сеть составляет тридцать минут, а в среднем злоумышленникам требуется 1–2 дня для преодоления защиты. При этом хакеры могут оставаться незамеченными довольно продолжительное время, доходящее до нескольких месяцев и более. И всё это — несмотря на большое количество средств защиты информации (СЗИ), внедрённых, во всяком случае, в крупных компаниях. За счёт чего же это становится возможным и как эффективно защититься от кибератак?

НАЙТИ УЯЗВИМОСТЬ

Наш опыт проведения тестирований на проникновение показал, что боль-

шому числу компаний присущи ряд недостатков, позволяющих хакеру получить доступ уровня администратора сети. К ним относятся неисправленные уязвимости как на внешнем периметре, так и в программном обеспечении внутри сети. Отметим использование словарных и простых паролей, не установленные обновления безопасности. Всё ещё довольно редко применяется двухфакторная аутентификация в Active Directory. Зачастую бывает отключён мониторинг запрашиваемых билетов Kerberos. В качестве мер защиты мы применяем у наших заказчиков установку сканеров уязвимостей, внедряем систему управления паролями и ряд других мер. Отдельного внимания заслуживает опасность компрометации привилегированных учётных записей, для борьбы с которой рекомендуем устанавливать специализированные решения по их управлению.

Основными факторами повышенной киберуязвимости становятся значительно возросшая частота применения

методов социальной инженерии, высокая доля целенаправленных атак, в том числе использование уязвимостей нулевого дня. Не стоит сбрасывать со счетов использование такого вида атаки, как «злой двойник» (Evil Twin Attack), позволяющей создавать поддельные точки доступа и получать доступ к информации, проходящей через них. Наша практика показывает, что злоумышленника, проникшего в сеть, проще выявить, если внедрять решения по анализу трафика и сеть ловушек, позволяющих увидеть подозрительную активность. Кроме того, положительно зарекомендовала себя технология UEBA, позволяющая на основе машинного обучения увидеть аномальные активности со стороны пользователей.

ПРО СОЦИАЛЬНУЮ ИНЖЕНЕРИЮ

По опыту общения с заказчиками, применение методов социальной инженерии кратно возросло в течение 2022 года. Злоумышленники получают доступ к логинам, паролям и другой информации с помощью манипуляций и обмана, а СЗИ далеко не всегда срабатывают в этих случаях. Фишинг, смшинг, вишинг — эти слова стали неотъемлемой частью лексикона не только ИБ-специалистов, но и обычных пользователей. Статистика киберучений показывает, что при грамотно сформулированном псевдомошенническом

Статистика подсказывает, что минимальное время проникновения в компьютерную сеть составляет тридцать минут, а в среднем злоумышленникам требуется 1–2 дня для преодоления защиты

письме доля открытия вложений и ссылок достигает 50% и более. В случае получения настоящего фишингового письма это может приводить к компрометации учётных записей, и злоумышленник попадает в сеть незамеченным. Несмотря на повсеместно внедрённые решения по защите электронной почты, благодаря созданию новых доменов, использованию VPN и созданию максимально правдоподобного контента часть писем доходит до адресатов, что приводит к печальным последствиям. Для борьбы с фишингом предназначены решения класса Security Awareness, включающего обнаружение с помощью псевдофишинговых рассылок сотрудников, подверженных рискам, их обучение и дальнейшее тестирование.

НОВЫЕ МЕТОДЫ БОРЬБЫ С ЦЕЛЕНАПРАВЛЕННЫМИ АТАКАМИ

Целенаправленные атаки отличаются высоким уровнем планирования, включают разведку и сокрытие следов присутствия и наносят серьёзный финансовый ущерб. Помимо традиционных средств борьбы, таких как «песочницы», существует ряд относительно новых и весьма эффективных методов обнаружения атак и минимизации рисков компрометации информационных активов.

В первую очередь это решения класса Network Traffic Analysis, системы анализа трафика, позволяющие находить следы компьютерных атак как на периметре, так и внутри сети. Такие продукты позволяют находить различные источники атак, включая попытку эксплуатации уязвимостей, открытые порты и т.д. При этом благодаря хранению копии трафика данные решения играют важную роль в расследовании киберинцидентов.

Особое место занимают решения класса Detection, которые за счёт расстановки в сети приманок и ловушек, имитирующих реальные информационные системы, позволяют пустить злоумышленника по ложному следу и заодно обнаружить атаку. Внедрение подобных технологий удачно ложится в канву проведения тестирования на проникновение. Если пентестер в

первую очередь после проникновения в сеть зайдёт на «подложную» информационную систему, значит, ловушки расставлены правильно и с большой вероятностью на эту же информационную систему клонет и реальный хакер.

Есть и другой класс эффективных решений, позволяющих противодействовать обходу хакерами СЗИ. При запросе ядра операционной системы о наличии на хосте тех или иных решений ИБ такое решение перехватывает эти запросы и даже при отсутствии тех или иных СЗИ на вопрос об их наличии отвечает утвердительно, тем самым атака захлёбывается, едва начавшись.

Говоря о готовности сотрудников SOC и СЗИ к атакам на предприятие, нельзя не упомянуть о классе решений BAS (Breach and Attack Simulation), позволяющем в автоматизированном режиме проводить атаки на компьютерную сеть.

В последние годы стали популярны XDR-решения (Extended Detection and Response — расширенное обнаружение и реагирование). Они объединяют в себе базу индикаторов компрометации вместе с анализом всех хостов в сети, как конечных точек, так и сетевого оборудования, строят цепочки событий и позволяют анализировать, например, не восемь отдельных событий, а одно, их объединяющее. Это сильно экономит время ИБ-службы, а дополнительное преимущество заключается в возможности автоматизированного реагирования благодаря интеграции с различными СЗИ.

THREAT INTELLIGENCE

Внедряемые CTI платформы Threat Intelligence позволяют благодаря регулярно обновляемой базе индикаторов компрометации находить признаки начинающейся атаки, например подмену DLL-библиотеки, и эффективно решают задачи по обнаружению вторжения там, где традиционные IPS-системы (Intrusion Prevention Systems — системы предотвращения вторжений), основанные на сигнатурном методе, оказываются недостаточными. Что же касается Threat Hunting, то эта технология рассчитана на высокий уровень зрелости информационной безопасности организации, что

предполагает наличие аналитиков, в проактивном режиме ищущих следы компрометации, в отличие от традиционной модели работы, парадигма которых — дожидаться сигнала об атаке, после чего предпринимать действия по защите от неё. Внедрение концепции Threat Hunting может стать вишенкой на торте, но уже после внедрения всех основных ИБ-решений, включая решения по сетевой защите, мониторингу и управлению событиями безопасности и защите прикладных систем.

КОМПЛЕКСНЫЙ ПОДХОД

Для обеспечения эффективной защиты важен сервисный комплексный подход. CTI предлагает «безвендорскую» поддержку оборудования и ПО западных производителей на уровне, максимально приближённом к тому, что предлагали до 2022 года сами производители. Рынок подобных услуг сейчас во многом определяется техническими возможностями и ресурсами конкретной сервисной компании, а спрос на них можно назвать ажиотажным. Компания CTI на протяжении многих лет работала как с иностранными, так и с российскими вендорами. Накопленный экспертный опыт позволяет осуществлять проекты максимально бесшовного перехода с западных решений на отечественные с учётом глубокого понимания специфики их функционирования. Высококвалифицированные инженеры сервисного департамента оказывают как «безвендорскую» поддержку, так и услуги 1-й и 2-й линии поддержки по решениям российских вендоров.

Подводя черту, отметим, что в силу изменения ландшафта угроз базовыми, с точки зрения выявления атак, становятся такие решения, как NTA, Threat Intelligence, XDR, процессы проактивной охоты за угрозами (Threat Hunting), которые наряду с повышением осведомлённости сотрудников об угрозах ИБ и проведением киберучений способны стать опорой в борьбе с киберпреступностью.

**Екатерина СТЕПАНОВА**ведущий консультант отдела аудита
и консалтинга ДИБ АМТ-ГРУП, к.т.н.

ОЦЕНКА РИСКОВ

ИЛИ СКОЛЬКО СТОИТ КИБЕРУСТОЙЧИВОСТЬ

Статистика инцидентов за 2022 год показала увеличение количества как массовых, так и целенаправленных компьютерных атак. Из аналитики, публикуемой участниками рынка, можно проследить тренд на увеличение в несколько раз количества атак по сравнению с аналогичными периодами предшествующих лет.

И если раньше злоумышленники преимущественно двигало стремление к получению материальной выгоды, то в 2022 году добавились мотивы, связанные с идеологическими соображениями: атаки нацелены на создание общественного резонанса, привлечение внимания к социальным и политическим вопросам. Таким образом, фокус злоумышленников сместился с попытки получения доступа к банковским счетам компаний на организацию недоступности систем, перехвата управления над ними, DDoS-атаки, атаки на веб-ресурсы, утечки конфиденциальной информации.

Поэтому сейчас, как никогда раньше, актуальны задачи обеспечения киберустойчивости организаций. Базовые меры обеспечения киберустойчивости понятны, большинство организаций так или иначе их уже реализовали:

1. Выделение сегментов в сети для различных сервисов и приложений, контроль сетевых потоков между ними;
2. Использование средств антивирусной защиты и своевременное обновление баз данных признаков вредоносного программного обеспечения;

3. Создание резервных копий и тестирование возможности восстановления систем из них;

4. Своевременная установка необходимых обновлений;

5. Контроль отсутствия слабых или заданных по умолчанию паролей, скомпрометированных учетных записей;

6. Минимизация привилегий.

При этом почти каждый руководитель по информационной безопасности (ИБ) задаётся вопросом: достаточно ли уже реализованных мер и как обеспечить уровень киберустойчивости, позволяющий отвечать текущим вызовам?

ОЦЕНКА РИСКОВ

Одним из возможных вариантов ответа на данный вопрос является оценка рисков ИБ.

Во многих организациях сложилась практика формального моделирования угроз (в связи с требованиями регуляторов) и абстрактной оценки рисков информационной безопасности. Безусловно, к результатам такой оценки вопросов больше, чем ответов она способна дать.

Как показывает наша практика, для того чтобы получить действительно приносящую пользу оценку рисков ИБ, необходим инструментарий, предполагающий:

- ♦ идентификацию всех процессов и выделение критических, которые обеспечивают достижение целей организации;
- ♦ определение, какие системы поддерживают, обеспечивают управление и контроль критических процессов;

- ♦ оценка, к каким негативным последствиям могут привести действия злоумышленников в отношении систем (например, потеря денежных средств, дополнительные затраты на восстановление деятельности и устранение последствий, штрафы, наложенные исполнительными органами государственной власти, недополученные доходы от приостановления или прекращения оказания услуг и другие);

- ♦ моделирование возможных действий применительно к информационной инфраструктуре организации при реализации атак с использованием баз знаний о техниках и тактиках злоумышленников (например, ФСТЭК России, MITRE ATT&CK®), результатов расследования инцидентов ИБ;

- ♦ определение, какие меры и средства защиты уже внедрены и обеспечивают нейтрализацию действий злоумышленника, какие планируются к внедрению;

- ♦ оценка эффективности мер и средств защиты по нейтрализации действий злоумышленника.

Бесспорно, реализация данного подхода достаточно трудоёмка и может потребовать привлечения дополнительной экспертизы для проведения оценки. Однако внедрение данного подхода позволит:

- ♦ количественно оценить величину рисков ИБ и сопоставить со стоимостью внедрения мер защиты;
- ♦ оценить влияние внедрения отдельной меры на значение киберустойчивости организации в целом;

♦ идентифицировать слабые места, которыми могут воспользоваться злоумышленники.

КАКУЮ ВЫГОДУ МОЖНО ИЗВЛЕЧЬ ИЗ РЕЗУЛЬТАТОВ?

Во-первых, оценить экономическую целесообразность внедрения отдельных средств защиты или их комплекса. Такой подход позволяет обеспечивать баланс затрат на построение системы защиты информации и потенциальных потерь в результате реализации идентифицированных рисков ИБ.

Во-вторых, можно выбрать средство или меру защиты из аналогичных или взаимозаменяющих, опираясь на их влияние на киберустойчивость организации в целом. Так, определяя способ, как «закрыть» эксплуатируемую вредоносным программным обеспечением уязвимость рабочих станций, можно сравнить по прогнозируемому значению риска ИБ варианты с полномасштабным обновлением всей инфраструктуры (что само по себе несёт риски нарушения работоспособности организации) и реализацией запрета взаимодействия по используемому вредоносным программным обеспечением протоколу на межсетевых экранах.

В-третьих, обеспечение планирования выбора или замены уже реализованных средств защиты с учётом ещё одного тренда 2022 года — прекращения или существенного сокращения функциональных возможностей зарубежных решений, невозможности продления подписок в связи с уходом или приостановкой деятельности зарубежных при условии, что заменить всё и сразу, как правило, не представляется возможным, в том числе ввиду ограниченности финансовых и временных ресурсов.

Безусловно, можно учитывать критичность отдельных систем и оборудования — в первую очередь внимания требуют те, которые обеспечивают критические процессы, где потенциальное влияние инцидентов и сбоев может привести к критичным последствиям. Но, располагая сведениями о влиянии отдельной меры на киберустойчивость организации в целом, а также о том, каким действиям злоумышленника они противостоят, можно



осуществить работы по замене более эффективно.

В-четвёртых, идентифицированные слабые места можно дополнительно контролировать. Например, реализовать правила корреляции в системах класса SIEM (Security information and event management), что может помочь своевременно выявить и остановить продвижение злоумышленника по информационной инфраструктуре организации. Сформулированные таким образом ключевые индикаторы риска (КИР) можно использовать для отслеживания подозрительной активности; КИР действительно будет «работать» для обеспечения ИБ кредитной организации, а не использоваться для формального выполнения требований Положения Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» (716-П).

Кроме этого, требования 716-П и Положения Банка России от 12.01.2022 № 787-П «Об обязательных для кредитных организаций требованиях к операционной надёжности при осу-

ществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг» (787-П) предписывают проведение оценки рисков ИБ с учётом осуществляемых кредитной организацией процессов и форм (способов) контроля операционного риска.

Положение 787-П определяет требования к идентификации и учёту критичной архитектуры, в том числе технологических процессов и технологических участков в их составе, объектов информационной инфраструктуры организации, задействованных при их выполнении. Идентификация этих данных является одним из начальных этапов оценки рисков ИБ.

Таким образом, использование количественных оценок риска ИБ не только обеспечивает соответствие требованиям Банка России, но и позволяет обеспечивать управляемую киберустойчивость, так как деятельность не может быть управляема, если она не может быть измерена.

**Евгений ПОЛЯН**менеджер продукта MaxPatrol VM,
Positive Technologies**Анастасия ЗУЕВА**руководитель отдела продуктового маркетинга,
Positive Technologies

ЧЕК-ЛИСТ

КАК УПРАВЛЯТЬ УЯЗВИМОСТЯМИ И ПОДРУЖИТЬ ДЕПАРТАМЕНТЫ ИТ И ИБ В ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ

Компании финансового сектора действуют в цифровом мире, а это значит, что важность работы отделов ИТ и ИБ одинаково бесспорна. ИТ-подразделение поддерживает доступность и работоспособность сервисов, а департамент ИБ обеспечивает защищённость организации, не позволяя атакующим реализовать недопустимые для бизнеса события. К сожалению, непростые отношения между подразделениями ИТ и ИБ — частая история, и финансовый сектор не исключение. Но есть одна область, где они обязаны выступать единой сплочённой командой, — речь об управлении уязвимостями. Обеспечить слаженную работу по выявлению, приоритизации, устранению брешей в защите и по контролю за процессом невозможно без плотного взаимодействия этих команд.

Как компании прийти к гармонии между безопасностью и эффективностью работы? Отсутствие согласия в этом вопросе нередко является причиной недопонимания и многолетнего существования уязвимостей даже там, где их легко исправить. Какие подразделения должны участвовать в формировании процесса VM (vulnerability management)? Какими должны быть договорённости между отделами

ИТ, ИБ и бизнес-блоком? Мы ответим на эти и другие вопросы, опираясь на опыт развития MaxPatrol VM, нашего продукта для управления уязвимостями, и рассмотрим шаги, необходимые для выстраивания VM в финансовой организации (с учётом того, что в больших компаниях принято рассматривать инфраструктуру как набор систем или сервисов, а не как что-то гомогенное).

ЗАЧЕМ УПРАВЛЯТЬ УЯЗВИМОСТЯМИ

Согласно нашему исследованию, если рассматривать последствия атак, то финансовые организации чаще всего сталкивались с кражей конфиденциальных данных (53%) и остановкой бизнес-процессов (41%), 6% компаний понесли непосредственные денежные потери. В 6% случаев злоумышленники использовали ресурсы финансовой организации для проведения дальнейших атак на клиентов и другие предприятия.

В ходе внешних пентестов, проведённых нашими экспертами в организациях финансового сектора, в 86% случаев исследователям удавалось получить доступ в локальную сеть. А при внутренних пентестах во всех случаях специалисты смогли получить полный контроль над инфраструктурой, а также продемонстрировать возможность

получения доступа к критически важным системам: например, в одном из банков была выявлена уязвимость, позволяющая скомпрометировать банкоматы.

Высокие риски и потери от кибератак повышают необходимость в грамотно выстроенном процессе vulnerability management. Уязвимости должны вовремя выявляться, приоритизироваться и устраняться. В банковской сфере пренебрежение их управлением может привести к недопустимым событиям, например:

- ♦ выводу денежных средств свыше определённой суммы со счетов финансовой организации или её клиентов;
- ♦ приостановке операционных процессов компании из-за недоступности её информационных систем;
- ♦ утечке баз данных с персональными данными клиентов.

По этой причине важно организовать процесс VM и скоординировать специалистов из департаментов ИБ и ИТ.

ПОДКЛЮЧИТЕ СПЕЦИАЛИСТА ПО ИБ

Мы нередко сталкиваемся с ситуациями, когда системы разрабатываются и внедряются без привлечения специалистов по ИБ: их задействуют для поиска уязвимостей уже на этапе эксплуатации

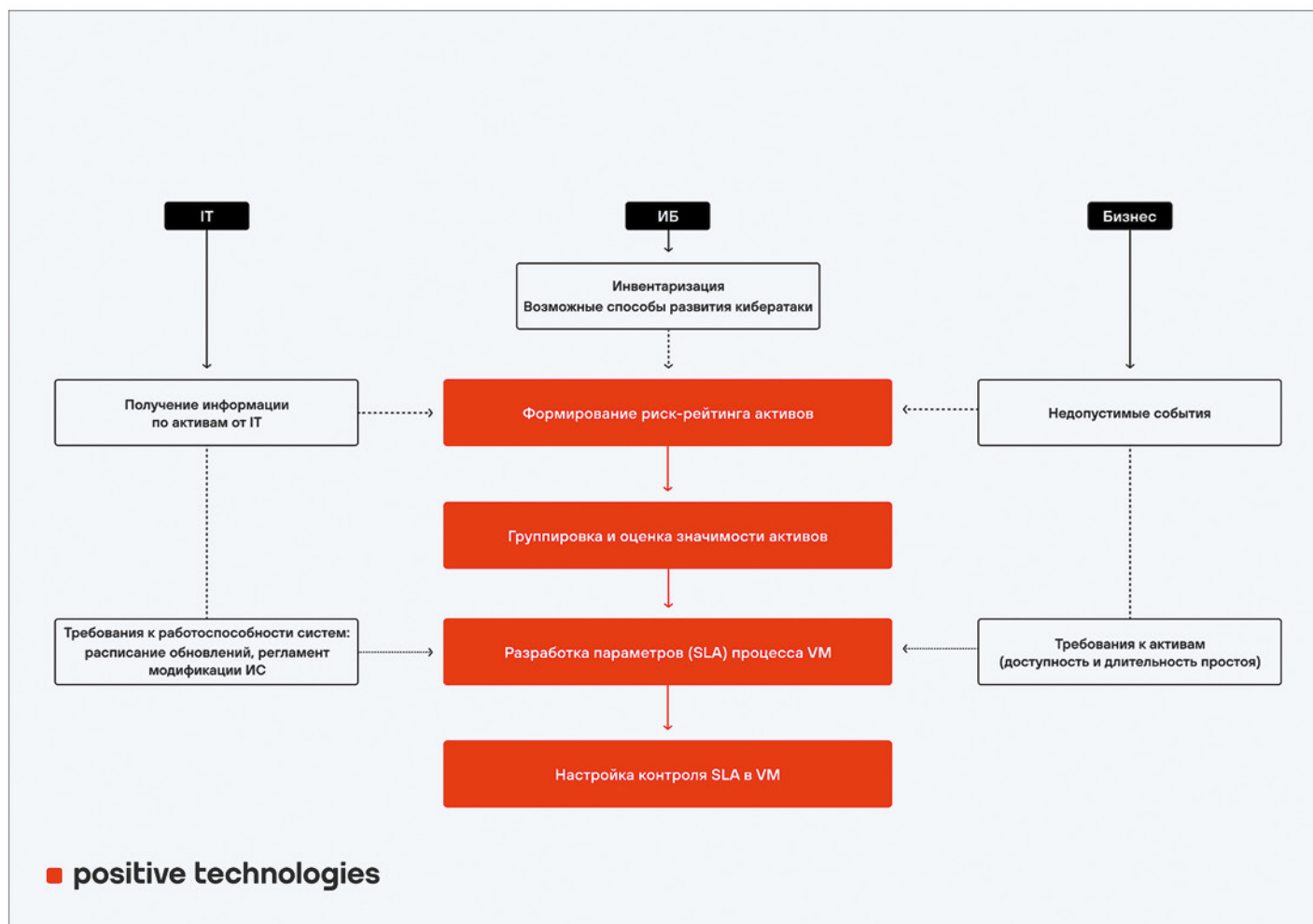


Рисунок 1. Схема взаимодействия бизнеса, отделов ИТ и ИБ в процессе управления уязвимостями

сервиса. Так делать не следует. Ещё на этапе разработки проекта специалист по ИБ должен убедиться, что в техническом задании на проектирование систем учтены:

- ♦ требования к информационной безопасности, в том числе предусмотрены технологические окна для регулярных обновлений;
- ♦ возможность сканирования, которая требует дополнительной нагрузки на сети и узлы;
- ♦ совместный для подразделений ИТ и ИБ план реагирования на появление новых опасных уязвимостей.

На стадии разработки или опытной эксплуатации специалисты по ИБ проверяют систему на уязвимости. Если результаты анализа защищённости плохие, то вводить продукт в промышленную эксплуатацию не стоит. Если всё в порядке, после его запуска рекомендуем продолжать поддерживать высокий уровень защищённости.

СДЕЛАЙТЕ ТРИ ШАГА

Итак, вы запустили систему. Теперь нужно организовать процесс управления уязвимостями, для которого, в свою очередь, требуется чётко распланированное взаимодействие отделов ИТ, ИБ и бизнеса. Выполните три шага:

Шаг 1. Определите перечень недопустимых для организации событий — обязательно вместе с бизнес-подразделением, в том числе с владельцами компании и топ-менеджментом. Таких событий не должно быть много (иначе защита сведётся к попыткам объять необъятное): их количество, как правило, не должно превышать пяти.

Шаг 2. Определите риск-рейтинг активов, отталкиваясь от списка недопустимых событий: исследуйте, какие активы могут являться целью злоумышленника и задействоваться при атаках.

Шаг 3. Составьте регламент работы и обслуживания каждого типа активов,

обсудите его с бизнесом и согласуйте с ИТ-отделом.

ЗАФИКСИРУЙТЕ РОЛИ ПОДРАЗДЕЛЕНИЙ

Руководство компании занимается обеспечением бизнес-процессов, знает, как расставить приоритеты, и формирует перечень недопустимых событий. Топ-менеджмент помогает определить, какие сервисы нужно защитить в первую очередь, простой какого масштаба компания сможет выдержать.

ИТ-подразделение, чья роль — поддержка работоспособности систем. ИТ-отдел должен обновлять ПО, чтобы устранять уязвимости, улучшать параметры систем. В обязанности ИТ-отдела входит отслеживание обновлений, чтобы они устанавливались с учётом расписания для каждого типа актива и в рамках оговорённых сроков (SLA, service level agreement, оно же соглашение об уровне сервиса).

Роль отдела ИБ — защита систем. Специалисты по ИБ знают, каким маршрутом пойдёт атакующий, представляют приоритеты в устранении уязвимостей, задают критерии эффективности процессов ИБ, а также контролируют уровень защищённости компании.

Специалисту по ИБ нужно отсортировать активы, присвоить им значимость и определить приоритетность обработки в зависимости от выбранной группы. Так, атакующий в большинстве случаев будет пытаться получить доступ к традиционным **целевым активам** (например, к серверу СУБД с персональными данными клиентов, серверам с финансовой отчётностью или планами, автоматизированной банковской системе), а путь к ним лежит, как правило, через типичные **точки проникновения** (веб-приложения на периметре сети, серверы с внешними сетевыми интерфейсами, рабочие станции с доступом в интернет, подключённые к беспроводным сетям). Для развития атаки злоумышленники используют так называемые **ключевые активы** — те, которые являются промежуточной целью: это контроллеры домена, серверы Exchange, система управления виртуализацией, рабочие станции администраторов.

ОПРЕДЕЛИТЕ СРОКИ ОБНОВЛЕНИЯ СИСТЕМ

На инфраструктуру в больших компаниях принято смотреть как на набор автоматизированных систем. Некоторые из таких сервисов будут работать на одном сервере и использовать одно сетевое оборудование. Для обеспечения защищённости бизнеса специалисты по ИБ не должны тратить ресурсы на защиту каждого актива: им стоит сосредоточиться на предотвращении неприемлемых событий. Кроме того, нужно скрупулёзно отслеживать все изменения инфраструктуры и понимать, где расположены важные с точки зрения ИБ активы, а где — менее значимые.

Поддержание всех систем в актуальном состоянии — задача нетривиальная, а в больших компаниях и нереалистичная, поэтому надо

определить **наиболее важные сервисы**. К ним мы относим те, которые помогут злоумышленнику реализовать недопустимое для бизнеса событие. Чтобы понять, какие компоненты наиболее важны для бизнес-процессов, надо сформировать **риск-рейтинг активов**. Для этого необходимо обратиться к топ-менеджменту компании.

Указать на активы, скорее всего относящиеся к ключевым (такие как контроллер домена), поможет система управления уязвимостями. Например, в MaxPatrol VM существуют специальные запросы, которые позволяют выделить важные категории активов и расставить их по уровню значимости (вручную или с помощью политик).

Далее нужно установить **регламенты**, то есть определить **технологические окна**, во время которых можно перезагрузить систему. Функциональность или производительность сервисов при этом, вероятно, будет ограничена — нужно предусмотреть дублирование систем. Если сервис не может прерываться, значит, нужно решить, как обновлять его по частям. Обычно критически важные системы редко обновляются, так как их нельзя останавливать, — именно поэтому специалисты по ИБ ещё на этапе разработки технического задания должны выдвигать отдельные требования к вариантам обновления, регулярного и экстренного, когда обнаружилась опасная уязвимость, которую нужно срочно устранить. Среди параметров, позволяющих определить SLA, — риск-рейтинг активов, технологические окна, требования к доступности активов и к версии.

Спланировать обновление Windows на рабочих станциях достаточно просто (в отличие от, допустим, встраиваемых ОС в банкоматах): Microsoft публикует патчи, как правило, раз в месяц. Двух недель на тестирование и «раскатывание» систем в большинстве случаев должно хватить. Просрочки в регламенте необходимо фиксировать, разбираться в причинах и при необходимости менять договорённости о сроках. Эффективность закреплённых регламентов можно анализировать во встроженных отчётах MaxPatrol VM.

В условиях сложившейся в 2022 году ситуации остро стоит вопрос обновления зарубежного ПО. Повышаются риски внедрения недокументированных возможностей и нежелательного контента в продукты для российских пользователей. Регуляторы рекомендуют отключить автоматическое обновление ПО, но без регулярного обновления в программах будут появляться новые уязвимости, в том числе критически опасные. Специалисты по информационной безопасности должны решить, обновлять ПО, рискуя получить недокументированные возможности, или не обновлять и получить уязвимости. Национальный координационный центр по компьютерным инцидентам (НКЦКИ) опубликовал алгоритм, который может помочь решить эту дилемму.

В тестовом режиме на сайте БДУ ФСТЭК России (Банк данных угроз безопасности информации) работает раздел с результатами тестирования обновлений ПО. В нём эксперты предоставляют рекомендации после проверки вышедших обновлений и выносят вердикт по выявлению их негативного влияния на инфраструктуру. Чтобы принять решение об установке патча, можно обратиться к этим указаниям.

Согласно нашему исследованию, 74% специалистов по ИБ в финансовой сфере изменили подход к патч-менеджменту, 31% специалистов отметили, что обновляют только критически важные узлы, 29% респондентов увеличили сроки проверки ПО в тестовой среде перед обновлением. Только 14% компаний в банковской отрасли приостановили обновления на всех узлах. Таким образом, специалисты считают риск накопления уязвимостей более серьёзным, чем риск получения обновления с недокументированными возможностями.

ДОГОВОРИТЕСЬ О РЕГУЛЯРНЫХ ОБНОВЛЕНИЯХ

Если специалист по ИБ придёт к ИТ-службе с огромным списком уязвимостей без какой-либо их приоритизации, это не даст эффекта. В списке должен быть набор узлов и программного обеспечения, которые необходимо обновить в первую очередь, а также сроки выполнения этих действий. Для

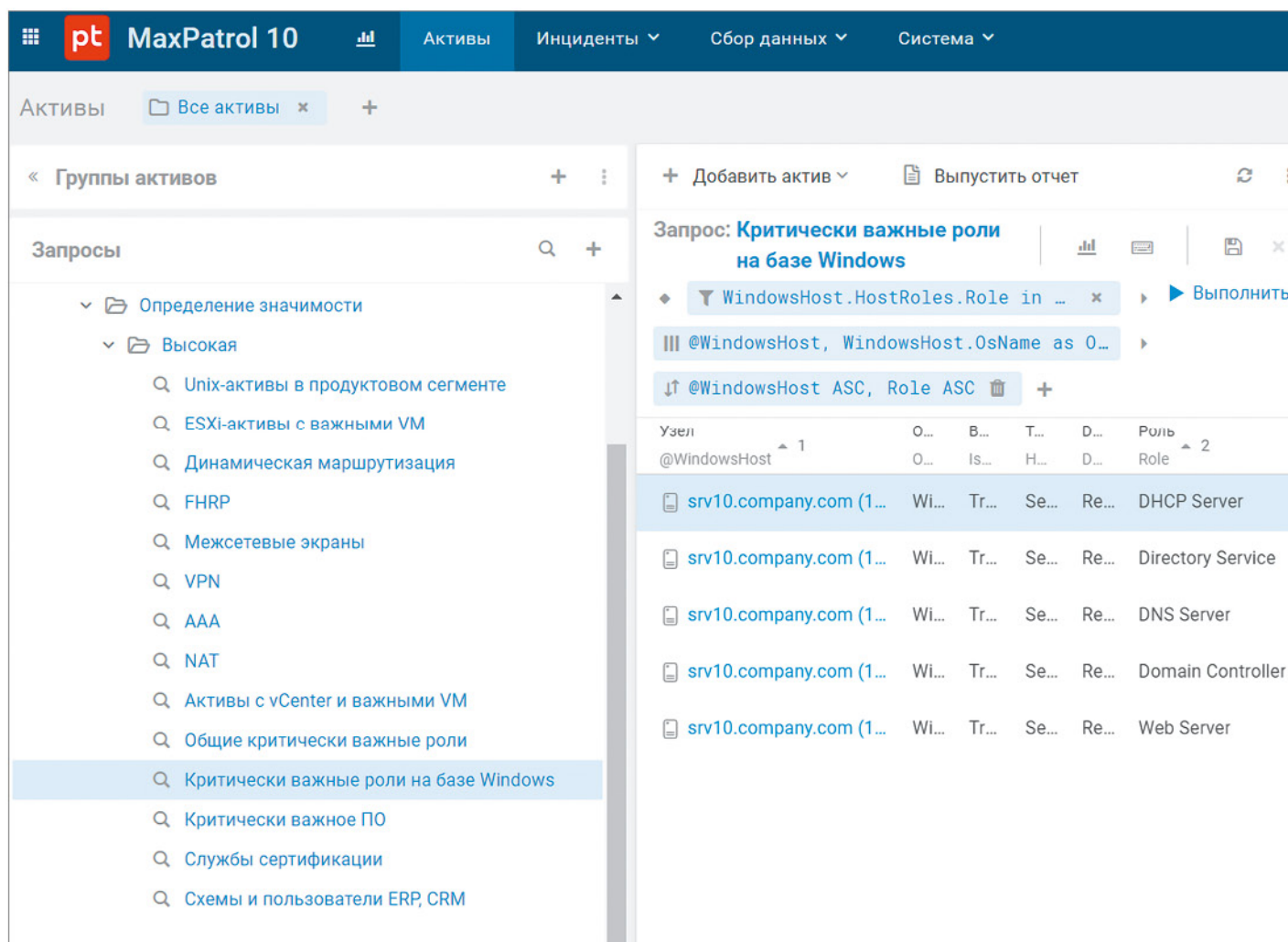


Рисунок 2. Пример запроса на присвоение уровня значимости активам

ИТ-службы есть несомненные плюсы в регулярных обновлениях: при появлении опасной уязвимости не придётся разбираться с множеством разных систем (к примеру, СУБД разных версий) и будет возможность синхронно обновлять ПО для всей инфраструктуры.

Договорившись о регламенте обновлений, следите, чтобы патчи устанавливались в оговорённые сроки, и, если они нарушаются, специалисту по ИБ надо выяснять причину. При формировании или изменении сроков необходимо помнить, что на процесс влияет и специфика отрасли компании. По этой причине не исключайте индивидуальный подход, ища наилучшее решение: у компании могут быть крайне специфические системы, относящиеся к ключевым (вспоминаем о банкоматах), и тогда регламент должен учитывать реальные трудности при обновлении ПО такого оборудования.

РЕЗЮМЕ

За устранение уязвимостей (обновление версий ПО, установку патчей) и применение компенсирующих мер (выключение сервисов, закрытие портов на межсетевых экранах) отвечает, как правило, ИТ-подразделение, поэтому для результативной работы с уязвимостями специалистам по ИБ важно грамотно выстроить взаимодействие с коллегами. Недавно мы провели опрос, чтобы выяснить, как этот процесс выстроен в разных компаниях. Результаты исследования показали, что 8% специалистов усложняют работу ИТ-отделу: отправляют в подразделение список выявленных уязвимостей без фильтрации и оставляют решение о порядке их устранения за ним же. У 14% компаний обратная ситуация: ИТ-отдел заставляет специалистов по ИБ заводить заявку на каждую обнаруженную уязвимость. При этом 32% ответивших указали, что

тратят на задачи VM до 10% рабочего времени.

Проактивный подход в устранении уязвимостей используют 27% респондентов: ИТ-подразделение регулярно устанавливает патчи или обновления ОС и ПО, не дожидаясь информации об уязвимостях от службы ИБ. А 28% специалистов применяют реактивный подход: ИТ-подразделение устанавливает обновления после того, как служба ИБ предоставит информацию об обнаруженных уязвимостях и сформирует списки активов, ОС и ПО для реагирования. Автопатчинг используют 20% ответивших. В текущих реалиях внедрять обновления без тестирования может быть вдвойне рискованнее. Мы считаем, что обоснованно доверить обновление инфраструктуры ИТ-отделу, который может протестировать ПО в защищённой среде, знает особенности поддержки текущей инфраструктуры и отслеживает загрузку сервисов.



Евгения КОЛОДИНА
первый заместитель
генерального директора ГК «ЦИБИТ»

НОВАЯ ЭРА КИБЕРБЕЗОПАСНОСТИ

ГЛАВНЫЕ ВЕКТОРЫ В РАЗВИТИИ ОТРАСЛИ СЕГОДНЯ

2022 год стал поворотным в развитии рынка информационной безопасности в России, участники которого вышли на новый уровень понимания критической важности обеспечения защиты информации. А необходимость строго соответствовать требованиям законодательства стала катализатором качественных изменений в отрасли. Прежде всего, на предприятиях страны изменился сам подход к вопросам киберустойчивости — ответственность выросла многократно.

В прошлом году российские компании столкнулись с беспрецедентными по количеству и масштабу кибератаками. Под ударом оказались банки, СМИ, субъекты КИИ — атаки были направлены на нарушение функционирования важнейших государственных компаний и их ресурсов. Постоянно меняющиеся внешние условия в очередной раз продемонстрировали, что вопросам защиты информации нужно уделять особое внимание, причём всегда, а не только в кризисные периоды.

Точкой отсчёта в трансформации подходов к обеспечению информационной безопасности можно считать Указ Президента России № 250, издание которого обострило вопросы дефицита кадров и привело к курсу на импортозамещение.

НОВЫЕ ТРЕБОВАНИЯ

1 мая 2022 года президент Владимир Путин подписал Указ № 250 «О дополнительных мерах по обеспечению

информационной безопасности РФ», а в июле вышло Постановление Правительства Российской Федерации № 1272 «Об утверждении типового положения о заместителе руководителя органа, ответственном за обеспечение информационной безопасности в органе, и типового положения о структурном подразделении в органе, обеспечивающем информационную безопасность органа», в котором были представлены разъяснения к документу, касающиеся кадрового вопроса.

Конечно, новые законодательные нормы вызвали широкую дискуссию в нашей отрасли. В первую очередь Указ президента обязал ведомства и организации создать подразделения по информационной безопасности для обнаружения, предупреждения и ликвидации кибератак и реагирования на инциденты. Также в документе было обозначено требование, согласно которому возглавлять такие подразделения должны лица в ранге заместителя руководителя компании.

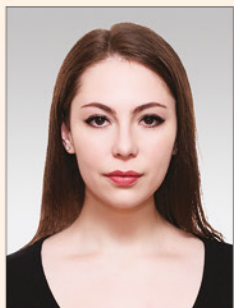


Евгений БУГАЙ
руководитель кадрового агентства «ЦИБИТ»

Чтобы исключить игнорирование вопросов защиты информации на предприятиях, Указом № 250 ответственность за кибербезопасность была возложена на топ-менеджмент компаний. Требования документа сформировали совершенно новое видение дефицита специалистов в отрасли. Например, эксперты по информационной безопасности нашего партнёра Positive Technologies после принятия Указа отмечали:

общая потребность в квалифицированных ИБ-кадрах в стране может возрасти до нескольких сотен тысяч, так как только субъектов КИИ в России насчитывается порядка 500 тысяч — и в каждой такой организации должно быть и ИБ-подразделение, и соответствующие сотрудники.

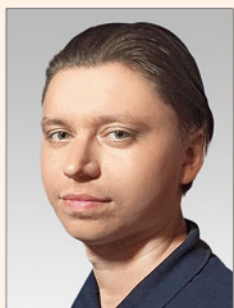
Ситуация сложная, и мы готовы прийти на помощь. Кадровое агентство «ЦИБИТ» специализируется на подборе персонала в сфере информационной безопасности уже более 8 лет. Наши рекрутеры работают с действительно ценными кадрами, в том числе с бывшими сотрудниками силовых структур и с соискателями, которые занимались обеспечением информационной безопасности на государственном уровне.



Ксения МИНАКОВА
руководитель учебного центра «ЦИБИТ»

Согласно нормам Указа № 250, у руководителя подразделения по информационной безопасности должно быть высшее профильное образование либо диплом о профессиональной переподготовке по направлению «информационная безопасность».

В учебном центре «ЦИБИТ» можно получить знания в рамках двух программ профессиональной переподготовки, которые соответствуют требованиям документа: «Технологии и средства обеспечения компьютерной безопасности» (540 часов) и «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» (504 часа).



Алексей ВЕЛЯКИН
руководитель департамента аттестационных работ
ГК «ЦИБИТ»

Мы оказываем комплексные услуги по проведению аудитов применяемых средств и систем защиты информации на предприятиях. Основными целями при оказании услуги являются обследование организации с целью оценки применяемых средств и систем защиты информации на наличие СЗИ с недействующими сертификатами и СЗИ, выпущенными в дружественных странах. Результатом нашей работы всегда является проведенная система защиты информации или предложения по её модернизации.

Ещё одним решением в части соответствия нормам Указа № 250 стало возложение обязанностей по обеспечению информационной безопасности на уже существующие ИТ-подразделения. В этом случае специалистам необходимо пройти обучение, удовлетворяющее требованиям документа. Такие курсы профессиональной переподготовки представлены в учебном центре «ЦИБИТ».

Требования к квалификации руководителей подразделений по информационной безопасности, обозначенные в Указе № 250, усилили кадровый голод, который мы фиксируем уже не первый год. Тенденция нехватки специалистов довольно значительно была выражена и в 2021 году, но 2022 оказался временем новых вызовов. Помимо рассмотренных выше законодательных норм, ощутимой проблемой стал отток кадров.

«ЦИБИТ» помогает решать даже самые сложные кадровые вопросы. Мы знаем, как работать на дефицитном рынке. Рекрутеры нашего кадрового агентства могут подобрать нужных специалистов в соответствии с требованиями регулирующих органов и пожеланиями работодателей.

ИМПОРТОЗАМЕЩЕНИЕ В ИБ

Ещё одна тенденция, которая оказала значительное влияние на трансформацию отрасли информационной безопасности, — курс на импортозамещение. Причём импортозамещение не только «вынужденное», связанное с уходом иностранных компаний с нашего рынка, но и продиктованное государственной политикой и новыми нормативными актами.

В марте 2022 года ФСТЭК России приостановила действие ряда сертификатов соответствия на программ-

но-технические средства защиты информации (СЗИ). В список таких сертификатов попали СЗИ иностранного производства, преимущественно антивирусы и межсетевые экраны. Это значит, что предприятиям необходимо было заменить указанные СЗИ на сертифицированные.

В июне Министерством цифрового развития, связи и массовых коммуникаций РФ был представлен перечень ключевых организаций, которым предстояло осуществить оценку уровня защищённости информационных систем с привлечением организаций-лицензиатов ФСБ России и ФСТЭК России. В него вошли 74 компании, включая государственные ведомства, СМИ, крупнейшие банки. Мы пришли на помощь нашим клиентам, разработав комплексную услугу по проведению оценки соответствия актуальным требованиям применяемых в организации СЗИ.

Итак, ключевые факторы изменений в сфере информационной безопасности России сегодня — усиление законодательного регулирования, кадровый голод, импортозамещение.

«ЦИБИТ» оказывает комплексные услуги в области защиты информации, помогая справиться с вызовами времени. Наши главные направления: подготовка организаций к получению лицензий ФСБ России и ФСТЭК России, аттестация объектов информатизации, аудит и приведение организаций в соответствие требованиям Банка России, подбор кадров и дополнительное профессиональное образование в сфере информационной безопасности, приведение организаций в соответствие 152-ФЗ и 187-ФЗ, поставка и внедрение СЗИ.

Мы уверены: соответствие актуальным требованиям регулирующих органов сегодня — это не просто необходимость, а прочная основа для создания не формальной, а реальной киберустойчивости в стране.

Именно в этой области работает «ЦИБИТ». Наш девиз: «Мы помогаем соответствовать требованиям!»

Группа компаний «ЦИБИТ»
+7 (495) 792-80-80
info@cibit.ru
www.cibit.ru



Инна НАГИМОВА
директор по маркетингу Xello

КАК УСТРАНИТЬ СЛЕПЫЕ ЗОНЫ В ИБ

О ЗАЩИТЕ БАНКА С ПОМОЩЬЮ ТЕХНОЛОГИИ КИБЕРОБМАНА

В современных кибератаках социальная инженерия сочетается с мастерским использованием легитимных системных инструментов. В результате даже самые продвинутые системы защиты на базе машинного обучения могут пропустить хакеров внутрь сетевого периметра. Дополнительным барьером на пути к ценным активам может стать технология киберобмана. Поговорим о том, как устроены deception-системы и как они помогают крупному банку защищать деньги и данные клиентов.

ПРОБЛЕМАТИКА

Финансовые учреждения традиционно вкладывают значительные средства в защиту сетевого периметра. Причина такого подхода в том, что наличие подробных сведений о клиентах, а также возможность похитить крупные суммы превращают банки в желанную цель для злоумышленников. Успешные атаки на инфраструктуру кредитных учреждений практически всегда имеют масштабные последствия в виде репутационных издержек, финансового ущерба, негативного влияния на экономику страны. По оценкам западных аналитиков, после инцидентов безопасности 60% малых и средних банков не в состоянии продолжать работу.

При обеспечении информационной безопасности чаще всего встречается два подхода: превентивный — предупреждение киберугроз, и детективный — выявление и нейтрализация инцидентов безопасности. В первом случае внедряются различные системы

кибербезопасности: межсетевые экраны, антивирусы, песочницы и другие. Они используют известную информацию об объекте защиты или угрозе: сигнатуры, репутационные списки, базы уязвимостей. Это отлично срабатывает с типовыми атаками, изученными разработчиками средств защиты, но не позволяет эффективно предупреждать целенаправленные атаки, где, как правило, профессиональные хакерские группировки разрабатывают различные вредоносные утилиты и ПО под конкретную организацию. Между тем, по данным Лаборатории Касперского, каждую минуту в мире создается четыре новых варианта вредоносного ПО. Таким образом, при использовании превентивного подхода вероятность пропустить «свежую» атаку очень высока.

Снизить риск помогает совмещение превентивного и детективного подходов. В этом случае детективная часть обнаруживает аномалии с применением алгоритмов машинного обучения, математической статистики и моделирования. Но и этот подход не защищен от ошибок: машинное обучение базируется на ограниченном наборе входных данных, а модель, как правило, представляет собой сильно упрощённое представление о защищаемом объекте, поэтому аномалии обнаруживаются только если идеальное и наблюдаемое состояние значительно отличаются.

Получается, что когда злоумышленник обойдёт все средства защиты и сумеет закрепиться в сети, выявить его действия на этапе горизонтально-го перемещения будет крайне сложно.

Тем более что в большинстве актуальных атак злоумышленники используют стандартные системные утилиты, установленные на компьютерах корпоративной сети.

Ликвидировать слепые зоны существующих системы ИБ и обеспечить покрытие всей инфраструктуры компании помогает технология киберобмана (deception).

ОБ ЭВОЛЮЦИИ ОБМАННЫХ ТЕХНОЛОГИЙ

Технология киберобмана представляет собой развитие концепции ловушек или ханипотов (honeypot). Так называют заведомо уязвимый ресурс, который привлекает внимание хакеров, а затем собирает данные об их действиях и различные метрики. Ханипот может имитировать сетевое оборудование (роутер, маршрутизатор), сервер в сети компании или веб-ресурс. В процессе взлома установленные на ханипоте средства слежения регистрируют действия злоумышленников.

Постепенно ловушки становились всё сложнее и функциональнее. Появились такие их разновидности, как honeyclients, honeytokens и tarpits. Но для создания даже небольшой сети из различных ложных ресурсов и уязвимых сервисов (honeynet) потребуется значительное время и услуги подготовленных специалистов. В среднем на установку и подготовку к эксплуатации одного ханипота может уйти до 20 человеко-дней в зависимости от квалификации сотрудников.

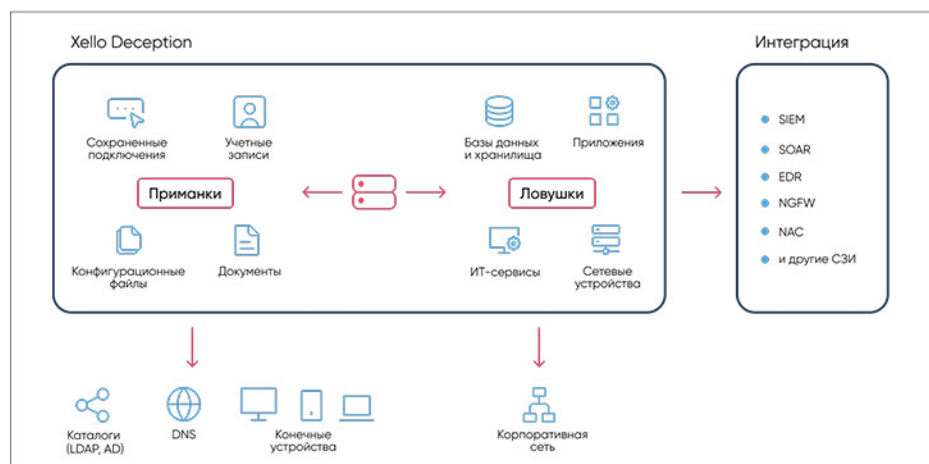
Со временем количественные изменения превратились в качественные. Ханинеты и ханипоты эволюционировали до новой технологии на рын-

ке информационной безопасности — технологии киберобмана. Новый класс решений получил название DDP (Distributed Deception Platform — распределенная платформа киберобмана). Ключевое отличие систем DDP от обычных ловушек — наличие дополнительных компонентов-приманок. Это могут быть ложные учетные записи, конфигурационные файлы, сохраненные пароли в браузерах и операционных системах, SSH-ключи, которые раскладываются на реальные хосты пользователей и сервера организации. При взаимодействии с любой приманкой deception-система оповестит специалиста кибербезопасности о киберинциденте, а злоумышленника перенаправит на ловушку, сместив фокус его внимания с ценных активов компании на фальшивую мишень. Ловушки в составе DDP представляют собой отдельные серверы со специализированной ОС или ПО. Они умеют имитировать реальные элементы ИТ-инфраструктуры — сервисы, приложения, базы данных, операционные системы или специфичные для отрасли устройства. Таким образом, злоумышленник попадает в изолированную ложную среду, которая способна имитировать реальную инфраструктуру предприятия. Современные deception-системы предоставляют централизованное управление приманками и ловушками, их адаптивную генерацию и их распространение по сети компании.

Взаимосвязанная система ложных активов по всей сети компании, которая легко масштабируется и не требует значительных ресурсов от бизнеса, позволяет эффективно выявлять сложные атаки как на ранних этапах, так и на самых поздних, когда злоумышленник атакует критические сегменты сети.

ОПЫТ ИСПОЛЬЗОВАНИЯ DECEPTION-СИСТЕМЫ В БАНКЕ

Обратимся к реальному кейсу. DDP-решение было внедрено в крупном банке. В составе сети более 100 000 хостов, используется инфраструктура виртуальных рабочих столов (VDI), средства контейнеризации и оркестрации



(Kubernetes, OpenShift), облачные службы (Yandex.Cloud, AWS, Microsoft Azure).

В банке выстроена эшелонированная защита, в составе которой имеется большинство классических решений, реализован технический контроль удаленных пользователей, произведена сегментация сети. Укомплектован и работает Центр мониторинга инцидентов безопасности и реагирования на них (SOC, Security Operation Center). ИБ-команда проводит регулярные тестирования на проникновение и проактивный поиск угроз (Threat Hunting). В организации выстроен процесс управления уязвимостями (Vulnerability management). Для противодействия угрозам, связанным с человеческим фактором, сотрудников регулярно обучают безопасному поведению и цифровой гигиене.

Несмотря на все реализованные меры, риск целенаправленных атак (Advanced Persistent Threat, APT) является критическим для банка. Потенциальные вектора для профессиональных хакерских группировок — корпоративные устройства, которые используются сотрудниками в личных целях, уязвимые open-source компоненты в составе разработанных программистами банка приложений и сервисов, и по-прежнему фишинг. Для минимизации рисков проникновения в инфраструктуру банк успешно использует решение класса DDP.

Ключевые причины внедрения deception-системы:

- ♦ отсутствие ложных срабатываний (алерт от deception-системы в боль-

шинстве случаев является инцидентом безопасности);

- ♦ демонстрация положительных результатов при тестировании на проникновение (в 90+ % случаях пентестеры «попадают» на приманку или ловушку в процессе эскалации «атаки»);

- ♦ возможность видеть последовательность действий злоумышленника при инциденте.

РЕЗУЛЬТАТЫ

Deception-платформа позволила приоритизировать события в процессе обработки киберинцидентов и автоматизировать некоторые задачи по реагированию. Например, при выявлении инцидента зараженный хост автоматически изолируется при помощи SOAR.

Собранные DDP-системой данные по инциденту направляются в SOC для агрегации и последующего анализа. Специалисты могут дополнять имеющуюся TI-платформу новыми индикаторами компрометации — названиями веток и ключей реестра, именами и хэш-суммами файлов.

Ознакомиться со всеми кейсами использования технологии киберобмана можно по ссылке:





Александр МОИСЕЕВ
ведущий консультант по ИБ
AKTIV CONSULTING

ОПЕРАЦИОННАЯ НАДЁЖНОСТЬ

УСПЕТЬ ЗА 120 МИНУТ

С 1 февраля 2023 года вводится в действие новый стандарт ГОСТ Р 57580.4–2022 «Безопасность финансовых (банковских) операций. Обеспечение операционной надёжности. Базовый состав организационных и технических мер», который детализирует ряд требований к основным процессам обеспечения операционной надёжности финансовых организаций (ФО), закреплённых в Положениях Банка России 787-П и 779-П. В новом стандарте по аналогии с ГОСТ Р 57580.1 устанавливается три уровня защиты: 3 — «минимальный», 2 — «стандартный», 1 — «усиленный».

С выходом новых стандартов по операционной надёжности, а также по управлению рисками (ГОСТ Р 57580.3–2022) система нормативной документации для финансовых организаций охватит область управления рисками (УР) реализации информационных угроз, управления защитой информации (ЗИ) и обеспечения операционной надёжности (ОН), а также затронет элементы непрерывности бизнеса и восстановление деятельности (ОНИВД).

СЛОЖНОСТИ ПРИ ВНЕДРЕНИИ

Изучив ГОСТ, я хотел бы отметить следующие ключевые особенности, которые, на мой взгляд, могут вызвать затруднения в процессе их реализации.

1. В ИТ-инфраструктурах и информационных системах (ИС) организаций финансовой отрасли большое количество элементов критичной архитектуры (КА), поэтому задача идентификации и отслеживания статусов их жизненного цикла (ЖЦ) весьма объёмна и требует привлечения большого количества ресурсов (кадровых, временных, финансовых, технологических).

2. В 787-П и 779-П регулятор установил довольно жёсткие временные параметры, направленные на обеспечение непревышения пороговых уровней допустимого времени деградации ТП. Многие ТП, обеспечивающие, к примеру, работу ДБО или ведение реестра участников торгов, необходимо будет восстановить в пределах 2 часов (120 минут).

3. Большая часть процессов обеспечения ОН в организациях традиционно не регламентирована, а для создания системы требуется разработка большого количества внутренней документации.

4. В отличие от специалистов по ИБ, сотрудники отделов ИТ, как правило, не горят желанием разрабатывать документацию, вести записи и отметки по процессам для кого-то, кроме себя, а это грозит привлечением дополнительных ресурсов (технических писателей).

ВОСЕМЬ ОСНОВНЫХ ПРОЦЕССОВ ГОСТ

Объём данной статьи позволяет привести 6 из 8 основных процессов ОН и тезисно описать их ключевые особенности, процессы «управления риском внутреннего нарушителя» и «обеспечение осведомленности об угрозах» требуют отдельного освещения.

1. «Идентификация критичной архитектуры». В рамках данного процесса прежде всего осуществляется систематическая работа по централизованному учёту и классификации всех элементов КА, а также поддержанию в актуальном состоянии перечней, реестров: БП и ТП (в том числе переданных на аутсорсинг); составляющих их технологических участков ТП; объектов информационной инфраструктуры (ОИИ), учёта их лицензионных политик и ограничений, а также инвентарного учёта; сервисов сторонних поставщиков услуг (по моделям SaaS, PaaS, IaaS).

Вторым важным направлением работ по данному процессу является документирование и техническое описание элементов КА в стандартизированных

Многие ТП, обеспечивающие, к примеру, работу ДБО или ведение реестра участников торгов, необходимо будет восстановить в пределах 2 часов (120 минут)

нотациях (BPMN, IDEF0, TOGAF и т.п.), а также поддержание данной документации в актуальном состоянии.

2. «Управление изменениями». В рамках данного процесса осуществляется комплекс организационных и технических работ следующего характера: планирование и управление изменениями конфигурации элементов КА; проведение анализа влияния на бизнес изменений, их приоритизации на «критичные» и «срочные», а также привлечение службы ИБ по согласованию, оценке и разработке минимизирующих риск мероприятий; протоколирование всех изменений и возможность их «отката»; разделение сред «разработки», «тестирования», «эксплуатации».

Большой объём работ проводится в отношении управления уязвимостями и проверки обновлений ПО: сканирования; проведения пентестов; ведения «Реестров уязвимостей»; кроме того, на этапах ЖЦ разработки прикладного ПО применяются такие виды анализа кода, как код ревью, статическое и динамическое тестирование.

3. «Обработка инцидентов и восстановление после них». Работы в рамках данного процесса являются самыми объёмными с точки зрения инженерных работ ИТ- и ИБ-специалистов. По каждому из направлений необходим расчёт и установление целевых показателей: реагирования, восстановления, анализа свидетельств и комплексный показатель эффективности реагирования и восстановления, с целевым временем восстановления (ЦВВ) и целевой точкой восстановления данных (ЦТВД).

Мониторинг и фиксация технических данных о событиях реализации информационных угроз выстраивается в соответствии с ГОСТ Р 57580.1 по принципу «эшелонированной обороны».

Реагирование на инциденты в отношении КА должно проводиться в соответствии с заблаговременно разработанными правилами и процедурами, сведёнными в playbook; в рамках снижения степени тяжести последствий инцидентов также должны быть проработаны варианты изоляции или отключения ОИИ (так называемая управляемая деградация) и установление

Можно отметить, что для принятия ключевых решений в отношении проработки альтернативных поставщиков и технологической зависимости необходимо привлекать топ-менеджмент организации

лимитов на финансовые операции при использовании каналов дистанционно-го обслуживания клиентов.

4. «Взаимодействие с поставщиками». Основной комплекс работ по данному направлению включает в себя минимизацию компьютерных атак со стороны инфраструктуры поставщиков услуг путём установления требований к обнаружению и предотвращению вторжений в их сетях; установление обязанностей поставщиков по прохождению аудита процессов обеспечения безопасности; проработка содержаний Соглашений об уровне оказания услуг (SLA), проработке основных и альтернативных поставщиков на случай возникновения у них кризисных ситуаций.

Также необходимо проработать вопросы технологической зависимости и диверсификации ИТ-технологий и услуг, систематическое выявление ОИИ, выпуск обновлений которых прекращён их поставщиками и по которым необходимо принять решение о продолжении или об отказе от эксплуатации и замене.

5. «Тестирование ОН БП и ТП». Немаловажным также является тестирование разработанных мероприятий ОН. При этом ключевые шаги — определение возможных финансовых потерь, разработка программ по сценарному анализу и тестированию готовности организации, а также вовлечение в данный процесс топ-менеджмента организации; тестирование эффективности реагирования на инцидент ОН в соответствии с ЦВВ; включение таких сценариев, как социальная инженерия, фишинг и стресс-тестирование.

6. «Защита КА от угроз при удалённой работе». Мероприятия последнего процесса хорошо знакомы

всем организациям после пандемии 2020 года и заключаются в разработке модуля Плана ОНВД в части перевода сотрудников на удалённую работу из дома; планировании пропускной способности СЗИ, реализующих удалённый доступ; обеспечении и контроле мер по «Процессу 8» ГОСТ Р 57580.1.

ЗАСЛУЖИВАЕТ ВНИМАНИЯ

Подводя итог вышесказанному, хочу отдельно выделить следующие особенности реализации требований ГОСТ:

1. Многие меры ОН пересекаются с мерами ЗИ ГОСТ Р 57580.1, а в ряде случаев имеет место прямое указание, следовательно, необходимо проверить полноту и качество их выполнения в ФО.

2. Необходимо пересмотреть стек имеющихся в организации ИТ-технологий и ИС на предмет обеспечения временных параметров пороговых уровней из 787-П и 779-П и рассчитать по ним ряд целевых показателей.

3. Также можно отметить, что для принятия ключевых решений в отношении проработки альтернативных поставщиков и технологической зависимости необходимо привлекать топ-менеджмент организации.

4. Для кредитных организаций также необходимо учесть особенности обработки инцидентов ОН в составе «Базы событий» в соответствии с требованиями 716-П, она должна быть дополнена уникальными полями.

5. Стоит отметить, что эффективно управлять ОН в режиме «бумажной» документации крайне затруднительно. Организациям требуется заранее заложить подходы, позволяющие реализовывать процессы ОН в «электронном» виде в существующих корпоративных информационных системах согласно 63-ФЗ «Об электронной подписи».

**Евгения ЛАГУТИНА**эксперт по системам мониторинга ИБ
и SOC-сервисам, «Лаборатория Касперского»

МОЩНЫЙ ОТВЕТ НА КИБЕРВЫЗОВЫ

ЧЕГО ЖДАТЬ ОТ XDR?

В статьях и выступлениях об XDR довольно часто можно услышать, что этот класс решений уже вовсе не новый, несмотря на то что на российском рынке появился относительно недавно. Что он возник как ответ на потребность рынка в объединении разных классов решений, а потому он — спаситель, Чип и Дейл и вообще серебряная пуля. Но так ли хороша эта историческая ноша и не происходит ли с XDR то, что случается с продуктом любого другого класса? Все они неизбежно обрастают всевозможными артефактами, которые впоследствии мешают поддерживать темп развития, задаваемый рынком, и приводят к разговорам про NG-что-угодно.

В какой же момент появляется на рынке идея о том, что пришло время следующего поколения класса решения? Естественно, когда существующее поколение фактически не справляется — перестаёт функционально соответствовать запросам. То есть не может помочь защититься от действий злоумышленника, которые соответствуют его актуальному профилю.

Возможно, пора задуматься, так ли мы далеки от разговоров об NG-XDR? И стоит ли в таком случае сейчас внедрять подходящий в условиях конкретной инфраструктуры XDR или лучше подождать новой концепции этого класса решений?

РАЗБИРАЕМСЯ В ТЕРМИНОЛОГИИ

Тут хочется сделать небольшое отступление и оговорить, что мы подразумеваем под XDR. Во-первых, это не просто набор разрозненных продуктов, а цельное решение с единым интерфейсом, которое в работе использует кросс-продуктовые сценарии. А во-вторых, будем рассматривать тот вариант развития XDR, в котором ключевую роль играет функциональность SIEM-системы, обогащённая возможностями, которые дают интеграции с EDR. Это важно, поскольку мышление в парадигме SIEM учит нас более комплексно воспринимать имеющиеся данные о происходящих событиях в инфраструктуре. То есть находить взаимосвязи и проследивать действия злоумышленника от момента выявления инцидента до нахождения всех элементов цепочки атаки.

ИСТОРИЧЕСКИЙ КОНТЕКСТ

Как уже было сказано, XDR стал ответом на запрос рынка. Запрос был следующим: нужен инструмент, который позволил бы объединить многие классы решений в единой платформе. То есть перейти от «туннельности» контекста восприятия защиты на разных уровнях инфраструктуры (хосты, сеть, приложения) и средств выявления и реагирования (либо продукт для выявления, либо для реагирования) к восприятию объёмному.

Итак, какие характеристики можно считать отличительными чертами XDR уже сейчас, исходя из истории появления.

- ♦ Объединение функциональных возможностей разных продуктов, отсюда — более широкий взгляд на инфраструктуру, учитывающий разноплановые факторы.

- ♦ Применение сценариев работы с одними решениями к другим. Например, классический сценарий применения фидов в SIEM предполагал только обогащение событий дополнительной информацией, которая позволяет приоритезировать инцидент и добавить контекст. А в случае с XDR появление определённого индикатора компрометации в событиях межсетевого экрана может стать стартом реагирования на EDR на основании этого индикатора. То есть для SIEM внутри XDR IoC — уже не просто дополнительная информация, а параметр реагирования, как для EDR.

- ♦ Приспособленность к работе с большими объёмами данных: архитектура предполагает использование актуальных технологий, пользовательский интерфейс учитывает разноплановость задач участников команды информационной безопасности.

- ♦ Возможность гибко менять архитектуру и функциональные возможности платформы в условиях непрерывного изменения инфраструктуры.

Те решения XDR, которые есть на рынке сейчас, стремятся развиваться

активно и динамично, чтобы успешно отвечать описанному запросу. Мы в «Лаборатории Касперского» стремимся к тому, чтобы наш XDR принёс пользу заказчикам и не стал дополнительной нагрузкой на людей и инфраструктуру. Поэтому изначально Kaspersky Symphony XDR задумывался и проектировался как гибкая, легко масштабируемая платформа, объединяющая возможности наших лучших экспертных решений — как проверенных годами, так и созданных недавно — в целостную эффективную экосистему.

ПРОГНОЗЫ И ПЕРСПЕКТИВЫ

Если посмотреть на тренды развития киберпреступности, можно заметить, что развитие происходит как по классическому пути, так и по ряду более неожиданных.



Что грозит
корпорациям
в 2023 году:
шантаж в СМИ,
фейковые утечки
и атаки через
облако

Например, тренд на унификацию и конвейеризацию атак. Этот тренд характерен сейчас для ИТ в целом, а не только для подхода злоумышленников: все стараются снижать стоимость работ, и бизнес киберпреступников тут не исключение. Многие инструменты можно взять напрокат. Действительно, зачем делать что-то специализированное и заточенное под конкретную уязвимость, если проще и быстрее воспользоваться готовым инструментом и не тратить деньги на разработку. К тому же, поскольку появляется возможность арендовать множество разноплановых инструментов, злоумышленник теперь может брать не качеством, а количеством векторов атак. Это приводит к тому, что для того, чтобы увидеть картину целиком, нужно будет получать и анализировать информацию с большого количества информационных систем и средств защиты информации.

Ещё одна «модная тенденция» — шантаж в медиа, публикация информации об успешных взломах в открытом

Kaspersky Symphony XDR задумывался и проектировался как гибкая, легко масштабируемая платформа, объединяющая возможности наших лучших экспертных решений — как проверенных годами, так и созданных недавно — в целостную эффективную экосистему

доступе и требование выкупа за неразглашение. При этом растёт и количество фейковых новостей о взломах и утечках. И становится очень важно видеть реальную картину происходящего, чтобы реагировать в соответствии с ситуацией. В контексте работы SOC это значит в том числе создание максимальной прозрачности и видимости инфраструктуры и наличие хорошо организованного и автоматизированного процесса реагирования на инцидент, который позволит быстро определить правдивость заявлений преступников и серьёзность угрозы.

И конечно, нельзя забывать о классическом тренде, существовавшем всегда: усложнение атак и разработка новых кастомных инструментов киберпреступников. Тут всё давно известно: сложную атаку легко упустить, и чем она сложнее, тем выше вероятность, что так и произойдёт.

Всё это очевидно приведёт к увеличению нагрузки на операторов и аналитиков SOC, которым придётся обрабатывать огромные объёмы инцидентов от разнообразных средств защиты, анализировать их с использованием большого количества дополнительных источников контекста и реагировать, используя разрозненные инструменты. При этом сконцентрироваться на важном будет всё сложнее. Причём если с такого рода проблемой может помочь справиться автоматизация некоторых процессов выявления и реагирования на инциденты, то с усложнением атак требуется и усиление функционала средств защиты, то есть их интенсивное технологическое развитие. Что часто ведёт к повышению требований к компетенциям персонала, а это — одна из главных проблем на современном рынке ИБ.

КАК ПРОГНОЗЫ ВЛИЯЮТ НА ТРЕБОВАНИЯ К XDR И ДОСТАТОЧНО ЛИ ТОГО, ЧТО МЫ ИМЕЕМ СЕЙЧАС

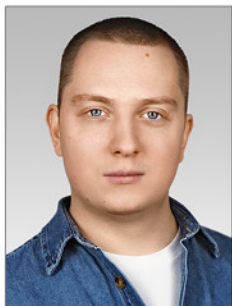
Несмотря на всплески новых трендов, запрос рынка многолетней давности остаётся актуальным: по-прежнему требуется и интеграция и тесное взаимодействие разных классов решений для увеличения прозрачности, и умение работать со значительным объёмом данных, и внутренняя архитектура решений, учитывающая динамичность конфигурации инфраструктуры и векторов атак.

Но, разумеется, меняется масштаб и скорость изменений, меняется набор инструментов, которые доступны теперь SOC и входят в набор must-have.

Получается, что XDR как классу решений до старости ещё далеко и есть место для развития и в текущем его «формфакторе»: рост экспертизы входящих в состав продуктов, непрерывный анализ и обновление стека технологий, на которых строится платформа, усиление возможностей автоматизации процессов расследования и реагирования, ну и непрерывное балансирование между обогащением пользовательского интерфейса и его упрощением.

Подробнее о Kaspersky Symphony:



**Иван РОГАЛЕВ**

руководитель отдела разработки платформенных решений BI.ZONE

**Антон СВИНЦИЦКИЙ**

директор по консалтингу АО «ДиалогНаука»

БЕЗОПАСНОСТЬ СВЕРХУ ВНИЗ

КАК ПОСТРОИТЬ ИБ-ЭКОСИСТЕМУ ДЛЯ ДОЧЕРНИХ ОБЩЕСТВ

Крупная компания защищена настолько, насколько защищены её дочерние организации — такой вывод можно сделать и по итогам атак в 2022 году, и по более ранним инцидентам. Поговорим о том, как изменить подходы к безопасности, чтобы статистика таких случаев стремилась вниз.

Владельцы экосистем и крупных холдингов прежде всего думают о безопасности головной компании. При этом взлом дочерней организации даёт злоумышленникам множество возможностей, чтобы развить атаку. Так что последствия такого взлома затронут и другие организации экосистемы или холдинга.

Например, в октябре 2022 года взломанный почтовый сервер некой организации открыл хакерам доступ к серверам Организации по атомной энергии Ирана. Скомпрометированными оказались закрытые данные о работе Бушерской АЭС, паспорта и визы иранских и российских специалистов со станции, контакты по ядерным разработкам и др.

Крупным бизнес-структурам сейчас не хватает понятных и удобных решений, которые позволили бы контролировать информационную безопасность (ИБ) во всей группе компаний. Эту проблему рынку предстоит решить в 2023 году.

ЗАЧЕМ ОБНОВЛЯТЬ ПОДХОДЫ

Большинство современных ИБ-решений направлены на защиту одной конкретной организации. В результате при взгляде на крупную экосистему картина выходит хаотичная.

1. Отсутствует стандартизация и контроль безопасности всех дочерних организаций

- ◆ Разрозненные коммуникации
- ◆ Отсутствие регулярного контроля
- ◆ Нет оперативной информации о текущем уровне защищённости дочерних обществ и о свойственных им угрозах

2. Нет отлаженной работы между организациями группы

- ◆ Каждый CISO решает задачу по-своему
- ◆ Не прописаны сценарии действий, в том числе при выходе инцидентов за пределы одной организации

3. Средства защиты в дочерних обществах внедряются хаотично

- ◆ Инструменты не связаны между собой
- ◆ Ряд инструментов работает не в полную силу
- ◆ Некорректно настроены правила
- ◆ Разрозненные и мультивендорные решения увеличивают стоимость владения и поддержки

4. Нет баланса знаний в каждой организации

- ◆ Большое количество компетенций в головной организации и малое в дочерней
- ◆ Нет опыта управления системами безопасности в дочерних обществах

В крупной инфраструктуре все компоненты взаимно интегрированы, идёт постоянное обогащение информации, чтобы компания получила больше прибыли. Такая экосистемная архитектура требует новых подходов к кибербезопасности.

Каждая дочерняя организация вносит вклад в общую защиту от современных

киберугроз. А использование единой платформы позволяет систематизировать и автоматизировать работу над повышением уровня кибербезопасности, принимать взвешенные управленческие решения, управлять задачами и отслеживать результаты такой деятельности.

КАК ЭТО МОЖЕТ ВЫГЛЯДЕТЬ

Платформа для централизованного управления масштабными ИТ-структурами может решить две проблемы. Во-первых, это интеграция сервисов безопасности во всём холдинге. Во-вторых, с возникающими проблемами можно бороться, ориентируясь сразу на всю группу компаний и выстраивая взаимодействие между дочерними обществами.

Добиться этих целей позволит набор функций, который реализован, например, в решении BI.ZONE Cyber Maturity Platform (CMP). Компания BI.ZONE развивает его в партнёрстве с интегратором «ДиалогНаука» (рис. 1).

Какие возможности нужны для управления кибербезопасностью в холдинге:

- ◆ инвентаризация ИТ-активов;
- ◆ информирование об угрозах и опросы сотрудников по итогам инцидентов;
- ◆ стандартизация требований с учётом особенностей каждой компании, входящей в экосистему (холдинг);
- ◆ аудит соответствия требованиям (с возможностью сравнения результатов организации как в определённом промежутке времени, так и с другими участниками экосистемы);
- ◆ планирование деятельности и контроль выполнения планов и мероприятий;

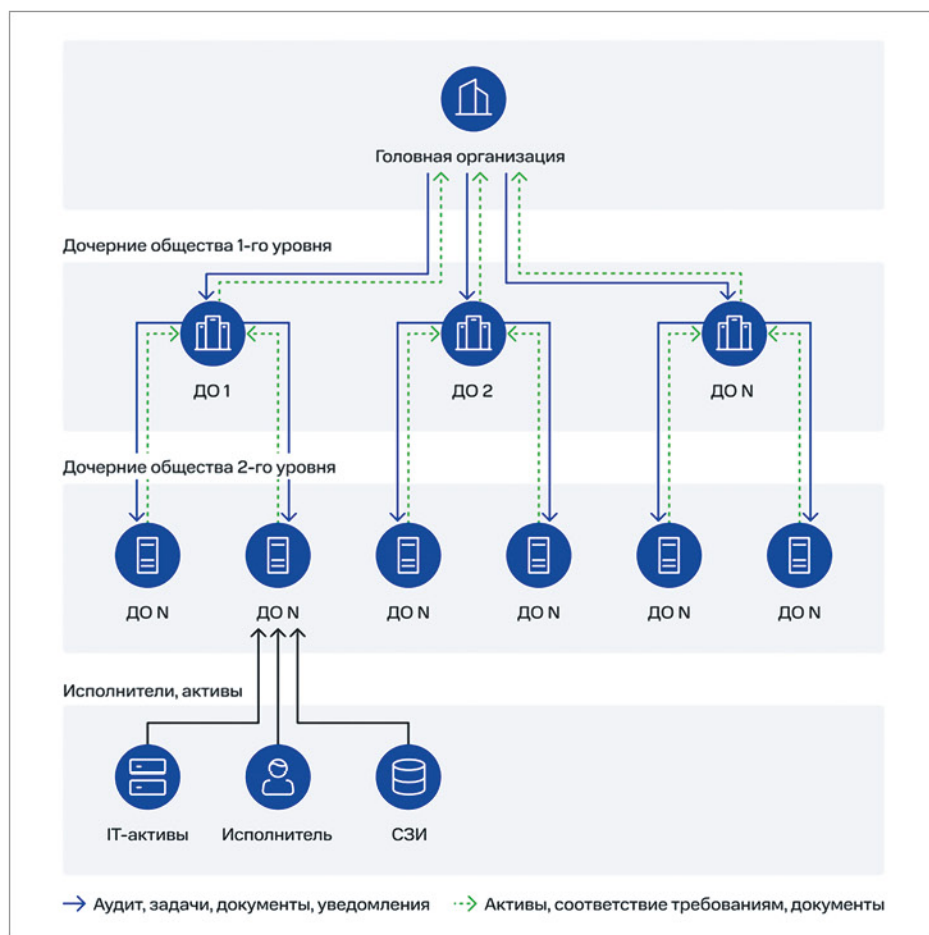


Рисунок 1. Управление информационной безопасностью в холдинге

- ♦ внедрение нормативных документов;
- ♦ управление инцидентами;
- ♦ управление знаниями;
- ♦ формирование отчётности и аналитика.

Выгоду от такого «зонтика» кибербезопасности получают все участники.

ЦЕННОСТЬ ДЛЯ ГОЛОВНОЙ ОРГАНИЗАЦИИ

Ключевое преимущество — централизованный контроль кибербезопасности во всей группе компаний. Инвентаризация активов кибербезопасности, отслеживание исполнения планов по ИБ, повышение осведомлённости сотрудников об угрозах.

Помимо этого, головной компании становится проще масштабировать опыт и технологии на всю экосистему. Инструменты аналитики позволяют специалистам выгружать отчёты по необходимым срезам данных. Автоматизация рутины по инвентаризации средств защиты разгружает сотрудников кибербезопас-

ности и сокращает ИТ-трудозатраты. Руководство группы компаний получает актуальную информацию о том, какие системы используют дочерние общества и могут получить у поставщиков скидки, учитывая общий объём используемого ПО. Помимо экономии на таких соглашениях, компания сокращает затраты на обслуживание средств защиты: на месте «зоопарка» систем появляется упорядоченная архитектура.

ЦЕННОСТЬ ДЛЯ ДОЧЕРНЕЙ ОРГАНИЗАЦИИ

Дочерние компании, в свою очередь, могут выстроить удобное операционное управление уровнем осведомлённости сотрудников и активами кибербезопасности. Совместное использование знаний на уровне группы компаний помогает соответствовать требованиям головной организации и регуляторов. В результате во всей структуре быстро формируются зрелые процессы.

Только за последний год компании столкнулись с волной эксплоитов,

которые грозили серьёзными последствиями для компаний. Уязвимости в Apache Log4j, Fortinet, Microsoft Exchange — можно вспомнить ещё много примеров. Единая платформа, охватывающая весь ландшафт группы, помогает реагировать на такие угрозы за дни или часы.

Методология BI.ZONE CMP позволяет оценивать уровень зрелости кибербезопасности в дочерних обществах и определять их вектор развития. Она включает почти 30 направлений: от архитектуры и стратегии до управления уязвимостями и тестов на проникновение.

Выбор из 900 метрик позволяет оценить по единому подходу разрозненный бизнес из множества организаций. Результаты анализа покажут, где каждый участник находится на шкале защищённости и в каком направлении ему следует развиваться с точки зрения безопасности.

Этапы применения методологии:

1. Планирование

- ♦ сбор информации, инвентаризация ИТ-активов;
- ♦ определение целевого уровня, профилирование организации.

2. Реализация

- ♦ подготовка требований по ИБ;
- ♦ создание шаблонных документов и приказов;
- ♦ стандартизация конфигураций;
- ♦ настройка внешних технических сервисов ИБ;
- ♦ внедрение типовых решений подсистем защиты.

3. Контроль

- ♦ стандартизация обеспечения ИБ в дочерних организациях;
- ♦ определение текущего уровня ИБ;

4. Совершенствование

- ♦ рекомендации по устранению несоответствий;
- ♦ планы реализации мероприятий.

2023 ГОД — ГОД ПРОАКТИВНОСТИ

Угрозы нужно устранять превентивно, а для этого компаниям следует помнить: безопасность начинается на периметре самого отдалённого дочернего общества. Если её инфраструктура защищена так же, как в головной организации, вероятность пострадать от кибератаки сильно снижается.



SOC-ФОРУМ 2022

ТРЕНД ФОРУМА — ВЗГЛЯД НА ПРОБЛЕМЫ С РАЗНЫХ СТОРОН

Сила притяжения SOC-Форума растёт год от года — на этот раз он собрал около 3 тыс. специалистов ИБ из разных сфер и регионов, не считая представителей регуляторов, заказчиков и журналистов. Плотность идей, новостей и мнений на рабочую минуту форума, казалось, превзошла возможную, и сравнить её можно, пожалуй, только с нынешней плотностью DDoS-атак на российские объекты. Корреспонденты BIS Journal побывали на мероприятиях Форума.

РАЗГОВОРЫ ОБ ОТРАСЛИ И КИБЕРВОЙНЕ

Отрасль ИБ отважно борется со штормом 2022 года, не понимая при этом,

можно ли называть происходящее в зоне её ответственности войной. В то же время, пройдя бесконечность DDoS-атак и сотни атак целевых, отразась так и не мобилизовалась должным образом. Такой вывод делает обозреватель Валерий Куликов, прослушав публичные интервью с лидерами бизнеса и представителями регуляторов отрасли ИБ.

Например, замдиректора ФСТЭК В. Лютиков заявил, что рекомендации и предписания регуляторов на местах выполняют далеко не всегда, часто применяют несертифицированные средства, пренебрегают сложными проверками. Более трети организаций «не нашли возможности в условиях обострённой ситуации

провести хотя бы сканирование периметра, чтобы понять, какие у них уязвимые места». Выразиться конкретно и предельно жёстко регулятору якобы не позволили новые реалии, которые И. Лапунов, игравший роль интервьюера, объяснил так: «Большая часть того, что происходит сейчас в киберпространстве, не публиковалась. И нельзя публиковать».

Причины неизжитости негатива обозреватель видит в излишнем оптимизме:

«...мы отбились, мы показали очень хороший результат!» (вице-президент ПАО «Ростелеком» И. Лапунов);

«...отрасль ИБ находится в ложном спокойствии, вроде бы как год пережили и ничего страшного не произошло»



(Д. Баранов, генеральный директор PositiveTechnologies).

Но если профессионалы, сказав бодрые слова, сразу же призывали коллег не терять бдительность и наращивать темпы устранения «кибердыр», то обыватели от бизнеса, похоже, сохраняют спокойствие, граничащее с апатией, о чём свидетельствует тот факт, что 40% проверенных организаций не удосужилось даже поменять пароли привилегированных пользователей.

В том числе и поэтому оценка результата, показанного отраслью ИБ в сложившемся киберпротивостоянии, на общенациональном уровне выглядит весьма обтекаемо: «Я не стал бы говорить, справились мы или не справились, я бы ограничился аккуратной фразой: в Национальный координационный центр по компьютерным инцидентам не поступала информация об инцидентах, которые привели бы к катастрофическим или необратимым последствиям» (замдиректора НКЦКИ П. Белов).

А чтобы «мы справились», считает обозреватель, необходим перелом в сознании руководства страны. И положительные сдвиги тут вроде есть, в частности, шаги по госуправлению «мобилизацией» отрасли для защиты всех предприятий. О тактических новинках в этом направлении и говорил, похоже, замдиректора НКЦКИ, рассказывая о создании оперативного штаба как новой форме сотрудничества.

А. Шойтов, заместитель министра цифрового развития, связи и массовых коммуникаций РФ, рассказал

о стратегическом намерении создать мобильные бригады для оказания помощи «местным» департаментам ИБ в устранении проблем с киберзащищённостью. Уместно вспомнить, что опыт есть: так совместными усилиями «ставился на ноги» RUTUBE.

И всё же, как оценить нынешнюю ситуацию в киберпространстве — война это или нечто иное?

Обозреватель вспомнил ПМЭФ-2022, где этот спор между Минцифрой и зампредправления Сбербанка С. Кузнецовым не был завершён. А. Шойтов счёл, что кибервойны нет, так как «нет прямого столкновения с иностранным государством», а вот С. Кузнецов придерживался иного мнения, обосновывая его численностью участников «событий» с противной стороны и перечислением стран (от США до Эстонии), с территорий которых обеспечивалась комплексная поддержка враждебных России киберопераций.

На SOC-Форуме на сторону Минцифры встала Н. Касперская, произнеся сакраментальное: «Главная недружественная страна против России кибервойну не разворачивала. Если бы она её развернула, у нас было бы всё выключено, все ключевые элементы инфраструктуры просто перестали бы работать».

Но в таком контексте логичен и довод С. Кузнецова на ПМЭФ-2022: «Если бы она её развернула, то всё было бы выключено и у «неё», потому что системы управления технологическими процессами перестают работать не только по

команде управления, но и при выключении рубильника... по той или иной причине».

С конца 40-х годов XX века войны уже не объявляются с помощью дипломатических нот. И это надо учитывать, слушая призывы о помощи профессионалов. Например, И. Ляпунова: «Мы сидим в окопе, и по нам бьют. Нам нужна система активного подавления».

Такая система была бы хорошим подспорьем к «киберпожарным командам», о которых говорил М. Шойтов.

РЕГУЛЯТОРНЫЙ ВЕКТОР

В рамках SOC-Форума состоялся регуляторный трек.

ФСБ России

Представитель НКЦКИ А. Раевский рассказал о векторах развития нормативной базы по линии ГосСОПКА. В первую очередь об изменениях в федеральный закон «О персональных данных». Так, статья 19 дополнилась пунктом про обязанность оператора ИСПДн обеспечивать взаимодействие с ГосСОПКА, включая информирование о критических инцидентах (КИ), повлёкших неправомерную передачу ПД. Приказом ФСБ России должен быть определён порядок такого взаимодействия.

Предполагаются два варианта взаимодействия. Первый — операторы будут передавать информацию о КИ в НКЦКИ в течение трёх часов. Второй — когда оператор не имеет соглашения/регламента с ФСБ или НКЦКИ. В этом

случае надо заполнять форму на сайте Роскомнадзора, и далее эта информация поступит в НКЦКИ. НКЦКИ будет иметь право направлять запросы операторам по поводу КИ и получать ответ в течение 24 часов.

Другой вектор — выполнение Указа Президента РФ «О дополнительных мерах по информационной безопасности». Согласно указу на руководителя организации возлагаются полномочия по обеспечению ИБ и созданию ИБ-подразделения. В рамках Указа от ФСБ России требуется: во-первых, определить переходный период взаимодействия с НКЦКИ на основе соглашений/регламентов; во-вторых, организовать аккредитацию центров ГосСОПКА; в-третьих, определить порядок осуществления мониторинга защищённости информационных систем.

ФСТЭК России

Начальник управления ФСТЭК России Е. Торбенко обратила внимание, что, хотя законодательство действует с 2018 года, у большинства компаний остались вопросы, причём на уровне начала реализации законодательства. Даже сейчас от тех, кто не первый год живёт в поле безопасности, раздаются вопросы о том, как провести категорирование.

Основной вопрос — нужно ли согласовывать перечень объектов, подлежащих категорированию, с регулятором? «Только в части подведомственности, — ответила Е. Торбенко. — Если вы ФГУП (казённое учреждение), то согласовываете перечень. Если вы микрофинансовая организация или, например, завод (АО), то если регулятор в вашей сфере не установил такой необходимости, то перечень объектов согласованию не подлежит».

Банк России

Заместитель директора ДИБ Банка России А. Выборнов выступил с докладом «Особенности развития нормативно-правовой базы в области обеспечения информационной безопасности объектов КИИ в кредитно-финансовой сфере».

«Исходя из требования ФЗ № 187, вся наша отрасль является субъектами КИИ независимо от их размеров,



масштабов бизнеса и т.д., — отметил он. — Банком России было издано большое число нормативных актов по ИБ и операционной надёжности. В целом, как нам кажется, мы охватили все области, и новых глобальных требований, которые нам нужно было бы издать, пока нет. Тем не менее возникают вопросы о качестве воплощения этих требований в жизнь и вовлечённости менеджмента и руководства поднадзорных организаций в реализацию этих процессов».

О ЗАЩИЩЁННОСТИ КОМПАНИЙ

Свой язвительный репортаж с Технического трека корреспондент Корней Реут начал с уже знаменитой убаюкивающей цитаты замдиректора НКЦКИ П. Белова о том, что «...в 2022 г. в НКЦКИ не поступала информация об инцидентах, которые привели бы к катастрофическим или необратимым последствиям». И тут же неистовый Корней оглушил нас высказыванием С. Кузнецова (зампред правления ПАО Сбербанк), оценившего ситуацию совсем иначе: «95% крупных российских компаний не смогли эффективно отразить кибератаки, произошедшие в этом году».

Критические танцы с бубнами корреспондента мы дословно приводить не будем — они весьма сумбуры и сводятся к тому, что пациент всё же скорее жив, чем мёртв. Но приведённые им цитаты действительно любопытны:

«И уже первые доклады трека представили фактологию о защищённости отечественных компаний, которую экзальтированные слушатели могли бы назвать шокирующей, а вот издававшие виды докладчики просто описывали такими, например, фразами: «Чуваки поставили файрвол и забыли про него» или «У чуваков в Интернете торчит эр-дипи, у которого пароль пять цифр».

Более литературные комментарии звучали так: «Плохое знание своей инфраструктуры (где какие приложения лежат, что торчит в интернет)» и «По моим личным ощущениям, 90% уязвимостей можно было легко избежать».

Уместно заметить, что последняя интуитивная оценка хорошо бьётся с объективными данными зампредправления Сбербанка, приведёнными в начале этой главы.

В целом же материалы докладов «Примеры инцидентов и тенденции 2022» (С. Голованов, «Лаборатория Касперского») и «Почему простые приёмы хакеров до сих пор работают» (А. Репин, Positive Technologies) могут, похоже, стать отличной заготовкой для доводки до ума «золотого ключика» ИБ для российских компаний.

И ВСЁ-ТАКИ... ПРО КАДРЫ

Другой неравнодушный корреспондент — Никифор Ковалёв — побывал на секции «Дебаты», продолжившей традиции легендарной Антипенарки. Разговоры-споры долго-остро-остроумно велись примерно о том, как «бабло



побеждает зло» и какое «ненадёжное болотце этот Open Source», но как-то сами собой свернули на незапланированную (причём незапланированную специально, так как всем надоела) тему проблемы кадров в ИБ.

И тут случилось давление масс — активность зала не позволила экспертам на сцене, представлявшим «ибэшные» компании, отделаться нарративами про их подвижническую деятельность на ниве образования и предложениями о необходимости дать вузам указание о том, чтобы они «выпускали тех, кто нужен, а не тех, кого выпускают».

Активисты из зала поделились живыми примерами равнодушия компаний к конкретным призывам от студенческих объединений прийти в вуз. Выведенные из зоны комфорта эксперты «Дебатов» пытались окоротить активистов репликами типа «А что ты сделал для того, чтобы в комсомоле было весело?» и призывами не беспокоить компании организованными обращениями, а спасаться поодиночке, рассылая резюме. Но эти полутотшучивания потерпели фиаско.

И на «Дебатах» было коллективно признано, что системного подхода со стороны компаний к вопросам повышения качества высшего образования нет, появление представителей компаний в вузах — это, как правило, личная инициатива исключительно самих этих представителей. И добрые намерения таких энтузиастов чаще всего падают на неподготовленную, сухую почву: программы составлены «нелогично», работать приходится со студентами, уже разочаровавшимися в профессии

(даже ещё не «понюхав пороха») и мечтающими о карьере блогера.

К этой далеко не радужной картине были добавлены мазки об отсталой лабораторной базе (инициативы, подобные работе ИнфоТеКС по оснащению вузов программно-аппаратными комплексами киберполигона Ampire, — это скорее исключение, чем правило), о низкой зарплате преподавателей и высокой забюрократизированности преподавательской работы.

Похоже, что ворота в авгиевы конюшни высшего образования со скрипом открылись под давлением общественности. Нестерпимо запахло навозом, а Геракла по-прежнему нет...

О ЗРЕЛОСТИ ЗАКАЗЧИКОВ

Завершил SOC-Форум круглый стол «Двое из ларца». Он позволил именитым экспертам ИБ обсудить существующие на российском рынке сервисы — их состояние и перспективы.

«Тенденция в области сервисов ИБ достаточно очевидная — мы уверенно движемся вперёд. С одной стороны, потому что мы серьёзно развиваемся как провайдеры услуг. Важнейшим драйвером этого развития является и рост зрелости самих заказчиков», — отметил ведущий дискуссии А. Грибков (Angara SOC).

По мнению А. Воронцова (Innostage), зрелость заказчика действительно растёт, но нельзя забывать и о репутации. «Что произойдёт, если заказчика взломают? Сервис-провайдер потеряет лицо, и кто к нему после этого обратится? Кому нужен провайдер, не сумевший защитить заказчика? А если взломают самого провайдера? Позор!

Провайдеров сегодня много, и именно поэтому вопрос репутации — важнейший драйвер их развития».

Михаил Кадер (Positive Technologies) затронул вопрос финансовой ответственности. «Мы хорошо умеем рассказывать про наши сервисы, продвигать их, и тут наш уровень зрелости весьма высок. То есть мы достаточно эффективно умеем получать деньги. Но модель финансовой ответственности за оказанные услуги у нас проработана слабо. И это очень потенциальная зона для развития».

А. Кильдюшев («Ростелеком-Солар») вернулся к теме зрелости заказчика. «Мне хочется похвалить заказчика — теперь он сам говорит, что и как ему нужно. Ещё 2–3 года назад топ-менеджеры думали, что SOC (сок) — это напиток, теперь они знают, что такое SOC, и с ними приятно работать и помогать их бизнесу».

Артём Сычёв (Positive Technologies) согласился, что зрелость и заказчиков и провайдеров растёт. Но отметил, что индустрию ИБ двигает также и регулятор. Так, благодаря именно Указу Президента РФ № 250 весь топ-менеджмент понял, насколько важна информационная безопасность. Кроме того, эксперт считает, что необходимо учитывать риски этого года. Многие сервис-провайдеры использовали решения зарубежных компаний, которых теперь нет в России. И быстро перестроить все процессы вряд ли получится.

Тем не менее завершил своё выступление любимый авторитет бодро: «Заказчики растут, провайдеры тоже. Поэтому впереди я вижу светлое будущее».



Оксана ДЯЧЕНКО
корреспондент BIS Journal

FINOPOLIS-2022

ЦИФРОВОЙ ПРЫЖОК СДЕЛАН. КАК ТЕПЕРЬ ПРЕОДОЛЕТЬ КАМЕННУЮ СТЕНУ

Проблемы конкурентоспособности цифровой финансовой инфраструктуры, создание новых бизнес-моделей и цифровых сервисов, последствия ухода иностранных компаний из России — все эти и многие другие темы прозвучали в рамках Форума инновационных финансовых технологий Finopolis-2022.

НАБИУЛЛИНА: «КАК НЕ УПЕРЕТЬСЯ В КАМЕННУЮ СТЕНУ»

Россия — один из признанных мировых лидеров по цифровизации финансовой сферы. Те из наших граждан, кто имел возможность сравнить работу сервисов отечественных и зарубежных банков, знают разницу: насколько качественно и быстро работают первые по сравнению со вторыми. По словам главы ЦБ, таких впечатляющих результатов за последние годы удалось добиться благодаря двум факторам: продвинутым западным технологиям и высокому профессионализму российских айтишников.

В 2022 году ситуация резко изменилась. Технологии дружно выстроились в ряд и покинули отечественный рынок, громко хлопнув дверью. С ИТ-кадрами тоже не всё однозначно. Как известно, это «люди с тонкой душевной организацией», многие из которых, не выдержав резкой смены ценностных ориентиров на уровне всего общества, покинули родные края.

Закономерно возникает вопрос, «как сохранить тот высокий темп развития

цифровых процессов, который был набран за последние годы, чтобы из-за санкций и внешних ограничений не упереться в каменную стену?»

Именно так сформулировала свой первый тезис Эльвира Набиуллина, открывшая в качестве модератора пленарную сессию форума.

По словам главы ЦБ, эксперты в этой связи разделились на пессимистов и оптимистов: «Оптимисты считают, что нам всё нипочём, мы справимся, мы всё умеем. Пессимисты говорят, что мы завязаны на технологиях, на стимулах международной конкуренции, поэтому мы ничего сами сделать не сможем».

Участники пленарки, среди которых были главы двух крупнейших банков страны и министр цифрового развития, как раз и должны были ответить на вопрос, каким они видят стакан — наполовину полным или наполовину пустым. И как, по их мнению, можно сохранить набранный Россией темп развития: за счёт каких ресурсов и факторов?

ГРЕФ: «ЛИБО ТЫ ОПТИМИСТ, ЛИБО ОТПРАВЛЯЕШЬСЯ НА СВАЛКУ ИСТОРИИ»

Сейчас Россия отрезана от мировых цифровых технологий и решений, поэтому нужно приложить максимум усилий для создания альтернативы, заявил президент, председатель правления Сбербанка Герман Греф.

Он сказал, что разработка российского ПО — решаемая проблема, это вопрос времени и ресурсов. Проблемы

с «железом» тоже решаемы, хотя здесь больше трудностей и всё зависит от способности государства организовать соответствующую работу, поскольку ни одна компания не справится с этой задачей в одиночку.

«Плюс в том, что нам не на кого рассчитывать, — сказал Герман Греф. — И, как всегда, это большой драйвер. Оптимистами нас заставляет быть жизнь. Либо ты оптимист, либо отправляешься на свалку истории. У любого менеджера и предпринимателя оптимизм является одним из необходимых профессиональных патронов в обойме. Если этого нет, про всё остальное говорить не следует».

Глава крупнейшего банка страны высказался также об уходе иностранных вендоров из страны. По его мнению, потеря решений, которые забрали с собой западные компании, — это не самая большая беда, поскольку под давлением обстоятельств российские предприятия будут вынуждены создавать сопоставимые по качеству решения. А вот плотность конкуренции — это настоящая проблема, последствия которой будут видны в перспективе, сказал Греф. Он признал, что никакие российские компании не сумеют поддержать тот уровень конкуренции на рынке, который был до ухода иностранных вендоров.

«Я не оцениваю уход с рынка иностранных вендоров хорошо, — сказал глава Сбера. — Никакие российские компании не сумеют поддержать тот уровень конкуренции, который был. И разовое получение каких-то активов

относительно недорого — это только разовая прибыль для кого-то, но в долгосрочной перспективе экономика потеряет, потому что конкуренция снизится».

«Главное средство развития инноваций — это жёсткая конкуренция. Там, где нет конкуренции, нет инноваций. И в этом смысле одно из самых негативных последствий для российской экономики — это уход мощных иностранных компаний с российского рынка», — подчеркнул Греф.

КОСТИН: «ОТЧЕГО НЕ ВЫЖИТЬ С ТАКИМ ЦБ? ВОТ И ВЕСЬ РЕЦЕПТ!»

Председатель Центробанка отметила, что у Сбербанка и ВТБ различные подходы к бизнес-организации, что отражается в том числе на структуре и принципах работы банковских экосистем, и обратилась к главе ВТБ Андрею Костину с просьбой «поделиться рецептом выживания организации».

Ответ главы ВТБ был следующим: «Я вам скажу (в чём секрет выживания — ред.): какой замечательный у нас всё-таки Центральный банк, коллеги! И какие у нас прекрасные лица этой мужественной команды: Эльвира Сахипзадовна, Ольга Николаевна (Скоробогатова), Ксения Валентиновна (Юдаева)... Нет такого другого Центрального банка в мире! И он, конечно, победит все Центральные банки западных стран <...> Отчего не выжить с таким ЦБ? Вот и весь рецепт!»

Безусловно, Костина можно отнести к лагерю оптимистов, которые стараются найти в сложившейся ситуации как можно больше позитивных моментов, даже если это очень трудно сделать.

Основной хорошей новостью банкир назвал тот факт, что «клиенты банка живы, несмотря на все события текущего года».

Глава ВТБ рассказал также о процессах импортозамещения в банке, которые начались ещё в 2019 году. «Мы начали процесс перехода на собственные продукты ещё с 2019 года. Если в 2019 году 90% у нас была зависимость по всем ключевым иностранным ИТ-категориям, то сегодня это уже меньше половины. А к концу 2024 года планируем на 100% по критической инфраструктуре уже это делать сами



(решения — ред.). Это даёт возможность сегодня развиваться, — считает Костин. — Уход крупнейших компаний даёт нам не только политическую защиту сегодня, но и экономию средств. Мы посчитали, что на горизонте трёх лет это экономит нам 30 млрд рублей».

ШАДАЕВ: «ЛИДЕРЫ ЦИФРОВОЙ ЭКОНОМИКИ ГОВОРЯТ, ЧТО СВАЛИЛОСЬ СЧАСТЬЕ»

Своим мнением поделился и министр цифрового развития, связи и массовых коммуникаций Максуд Шадаев.

«ИТ-отрасль переживает сейчас непростые времена, и главное в ней — это люди. Именно их самочувствие определяет основные цели развития технологий и цифровизации. Насколько они уверенно смотрят в будущее и связывают его с Россией, с её экономикой — от этого очень сильно зависит, как будет складываться ситуация», — отметил он.

«Я рад, что оптимистов больше, чем пессимистов, — подчеркнул Шадаев. — Потому что для многих испытания, с которыми мы сейчас сталкиваемся, — это новые возможности для наших компаний. Лидеры цифровой экономики говорят о том, что тяжело, но с другой стороны, «свалилось счастье», потому что раньше было тяжело конкурировать с иностранными участниками рынка. Мы пытались создавать и развивать целый комплекс мер, которые стимулировали бы спрос на российские решения и разработки. Сейчас в одночасье

эти ниши освободились, и мы их будем осваивать».

Если ситуация будет развиваться в текущих трендах, то, по мнению Шадаева, есть все возможности реализовать имеющийся потенциал. Хотя при этом он признал, что существуют ниши, где нет зрелых технологий и продуктов. Это в основном касается аппаратного обеспечения и компонентной базы.

Министр высоко оценил цифровизацию банковской сферы, причём не только по сравнению с другими направлениями экономики, но и в международном масштабе.

«Финансовый рынок, финансовая отрасль с огромным отрывом лидирует по уровню цифровой зрелости по сравнению с другими отраслями экономики. В сопоставлении с международными показателями... здесь, наверное, если и есть какая-то разница, то она минимальная. А по многим показателям финансовая отрасль по цифровизации соответствует лучшим международным практикам», — сказал Шадаев.

Он считает, что уровень цифровизации финансовой отрасли нужно сопоставлять не с другими отраслями российской экономики, а с финансовыми отраслями мира.

Радует, что на сегодняшний день ситуация обстоит именно так. Но в будущем первоначального, пусть и очень результативного «цифрового прыжка», будет мало. Много будет зависеть от способности преодолеть «каменную стену».



Марина БРОДСКАЯ
обозреватель BIS Journal

ANTIFRAUD RUSSIA 2022

ЕСЛИ ИСКОРЕНИТЬ ФРОД НЕЛЬЗЯ, ТО СТОИТ
МАКСИМАЛЬНО ОСЛОЖНИТЬ ЖИЗНЬ МОШЕННИКАМ

Мошеннические операции, нацеленные на получение прибыли с использованием банковских счетов другого человека, были, есть и будут. Побороть фрод невозможно, однако системный подход к решению проблемы поможет максимально осложнить жизнь мошенникам — к такому мнению пришли все участники дискуссий Форума AntiFraud Russia 2022.

ЗАКОНОТВОРЧЕСТВО

В чём заключается системность подхода? В объединении усилий государственных органов власти, кредитно-финансовых структур, операторов связи и платёжных систем, компаний, работающих в области информационной безопасности, и правоохранительных органов. Во многом объединению структур способствовали события февраля 2022 г. и начало СВО, введение санкций, уход западных компаний и изменение схем вывода похищенных средств.

Благодаря активному взаимодействию Минцифры, Банка России, регуляторов и операторов связи уже значительно сократилось число звонков с подменных номеров. На блокировку фишинговых сайтов уходит 2–3 дня.

Изменения в законодательстве, которые вступили или вступят в силу, обяжут операторов связи верифицировать все звонки в сети, а структурам МВД РФ позволят оперативно получать информацию от банков. В будущем планируется внести дальнейшие изменения в законы, в т.ч. в Федеральный закон «О связи» для быстрого и эффективного реагирования на звонки мошенников.

С 1 января 2023 г. вступили в силу изменения в ст. 13.2.1 КОАП РФ, которые вводят штрафы для операторов связи, не исполнивших обязанности по подключению к системе обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования. Оператор будет обязан передавать абонентам реальные номера звонящих.

По инициативе Банка России рассматриваются изменения в ФЗ «О банках и банковской деятельности», которые дадут банкам право блокировать перевод денежных средств на счета мошенников, несмотря на согласие отправителя. Этот проект закона уже получил положительное заключение правительства, ведутся работы по проработке формулировок статей для исключения двойственного толкования.

Согласно изменениям в Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» в обязанности оператора связи войдёт необходимость передавать Минцифры всю цепочку связи для установки нарушителя. Планируется также введение уголовной ответственности за нарушения данного закона, аннулирование лицензий. Среди прочих мер рассматривается возможность прекращения обслуживания номеров иностранных граждан при окончании сроков на право пребывания в стране — с номеров, зарегистрированных на таких абонентов, также поступает много поддельных звонков.

Ожидается и увеличение штрафов за утечку персональных данных. Сегодня за утечку данных предусмотрен максимальный штраф в размере 75 тыс. руб. согласно ст. 13.11 КоАП РФ. Минцифры подготовило законопроект об оборотных штрафах для компаний за утечку персональных данных — до 3% от оборота. Эти меры должны мотивировать компании вкладывать средства в инфраструктуру ИБ до киберинцидента.

Операторы платёжных систем обязаны реализовывать мероприятия по противодействию осуществлению переводов денежных средств без согласия клиента в порядке, установленном

Создание УБК МВД РФ, а также внесение изменений в Федеральный закон «О банках и банковской деятельности», которые в полной мере заработают с 21.10.2023, позволят банкам и правоохранительным органам оперативно реагировать на преступления в финансовой сфере. До октября 2023 г. есть время на заключение межведомственных соглашений и отладку механизмов взаимодействия структур.



Банком России и федеральным законодательством. Соответствующие нормы внесены в ст. 27 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платёжной системе» (вступили в силу 01.10.2022) и ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности», они начнут действовать с 21.10.2023.

ОПЕРАТИВНОЕ ВЗАИМОДЕЙСТВИЕ

В рамках реализации Указа Президента России от 30 сентября 2022 г. № 688 «О внесении изменений в некоторые акты Президента Российской Федерации» в структуре МВД России создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК МВД России).

Среди основных задач Управления — вопросы организации взаимодействия подразделений органов внутренних дел РФ с госорганами всех уровней, учреждениями финансово-кредитной системы, телекоммуникационными компаниями и другими участниками информационного обмена, включая агрегаторов больших данных.

Создание УБК МВД РФ, а также внесение изменений в Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности», которые

в полной мере заработают с 21.10.2023, позволят банкам и правоохранительным органам оперативно реагировать на преступления в финансовой сфере. До октября 2023 г. есть время на заключение межведомственных соглашений и отладку механизмов взаимодействия структур.

В рамках изменений в законодательстве ведётся заключение межведомственных соглашений о сотрудничестве между Центральным банком, МВД, Минцифры, Генеральной прокуратурой РФ, Роскомнадзором. Все эти меры направлены на прямое взаимодействие ведомств для оперативно-го пресечения деятельности преступных сообществ.

ПЕРВЫЕ УСПЕХИ

К чему привели слаженные действия всех сторон по антифроду?

По статистике Банка России, которую привёл директор ДИБ БР Вадим Уваров, за три года объём похищенных средств вырос на 39%, число преступлений увеличилось на 34%. За три квартала текущего года украдено порядка 10 млрд рублей, число операций без согласия клиентов приближается к 700 тыс. случаев. На фоне роста ущерба на одного пострадавшего число мошеннических операций не растёт. За 9 месяцев 2022 г. «средний чек» похищенных

с помощью методов социальной инженерии средств составил почти 14,5 тыс. руб. Растёт и доля кредитных средств, выданных без согласия клиента под давлением или при участии мошенников, это показал опрос банков, проведённый Банком России.

Банк России направил операторам связи почти 488 тыс. номеров, с которых происходили звонки, эта цифра почти в 35 раз больше по сравнению с 2019 г. и в 7 раз превышает показатели 2022 г. Для блокирования таких номеров БР активно взаимодействует с Минцифры, сообщил Алексей Голенищев, директор Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (ФинЦЕРТ). Итогом такого сотрудничества стало резкое сокращение подменных номеров с префиксами +7495 и +7499, о чём также сообщил Владимир Бенгин, директор Департамента обеспечения кибербезопасности Минцифры России и представители операторов мобильной связи.

После блокировки возможности подмены номеров мошенники перешли на активное использование мессенджеров, отметили все спикеры Форума. Мессенджеры популярны, охватывают большую аудиторию. Учитывая высокий уровень доверия граждан к



правоохранительным органам, звонки и сообщения от «следователей» и «сотрудников Центробанка» продолжают приносить прибыль мошенникам. К сожалению, звонки через мессенджеры не видны операторам связи и пока нет возможностей их заблокировать.

СМАТЫВАЕМ УДОЧКИ

Фишинг занимает второе место по схемам развода граждан на деньги, в 2022 г. отмечен рост таких преступлений. Платформой «Антифишинг» выявлено 60 тысяч фишинговых ресурсов, из них 30 тысяч оперативно заблокировано. Здесь регуляторы, органы прокуратуры, регистраторы, кредитные организации и Минцифры также добились значительных успехов и координации действий. На блокировку ресурсов уходит 2–3 дня, при оперативном взаимодействии — 1,5 дня. Однако основную прибыль фишинговый ресурс забирает в первые 12–16 часов, и говорить о достижениях в 2–3 дня преждевременно, считает Владимир Бенгин. Это системная проблема: банки и компании, работающие в области ИБ, научились оперативно отслеживать фишинговые ресурсы, но по-прежнему нужны механизмы для их оперативной блокировки. Минцифры России подготовил законопроект о системе отслеживания фишинговых сайтов, он проходит согласование. В случае принятия закона на блокировку фишинговых ресурсов будет отводиться 8 часов.

Мошенники уходят в мессенджеры, подтвердил Сергей Хренов, директор департамента фрод-анализа ПАО «МегаФон». Если в конце 2021 г. случаи использования мессенджеров были единичными, сегодня такие звонки — частое явление. Мобильные операторы только в 18% могут подтвердить звонок кибермошенников. При этом огромное количество жалоб абонентов касается звонков и СМС от банков, госорганизаций, МЧС. Рост недоверия к неизвестным звонкам как глобальную проблему отметил и директор по управлению фродом и гарантированию доходов ПАО «ВымпелКом» Пётр Алфёров. 75% абонентов мобильных сетей негативно относятся к звонкам с незнакомых номеров, показывают исследования операторов и компаний, работающих в сфере ИБ.

Из новых схем фрода мобильные операторы отмечают не только переход на мобильные номера и мессенджеры, но и использование международного трафика. После блокировки возможностей подмены номеров пострадавшим звонят с номеров +495, +499, +967. Многие не обращают внимания на отсутствие заветной «7» в начале номера. В сводках происшествий иностранные номера проходят по документам правоохранительных органов как набор символов, что не только говорит о низком уровне компетенции специалистов, но и создаёт дополнительные трудности при идентификации мошенников для

операторов. Блокировать иностранный фишинговый трафик отечественные операторы не могут.

Объединение усилий по борьбе с фродом всех мобильных операторов, выстраивание тесного взаимоотношения со всеми заинтересованными сторонами, привлечение к этой работе компаний, работающих в области ИБ, повышение уровня технической грамотности должны принести плоды, считает Пётр Алфёров. Принятые изменения в законодательстве, направленные на верификацию номеров, и введение ответственности операторов связи за бездействие при подмене номеров — важный шаг на пути борьбы с фродом.

БАНДУ ДРОППЕРОВ — ПОД СУДИ

О проблемах профилактики борьбы с мошенничеством и выводе средств говорили представители правоохранительных органов.

95% преступлений с использованием методов социальной инженерии идёт через кол-центры, расположенные за пределами РФ. Однако вывод средств в настоящее время проводится в России. Банковское сообщество наделено правом на отключение счетов, через которые проходят похищенные средства, согласно «Методическим рекомендациям о повышении внимания кредитных организаций к отдельным операциям клиентов — физических лиц», подготовленным ЦБ России. Эти деньги и их движение по счетам видны банкам. Правоохранительные органы могут вменить владельцу счёта участие в преступлении, отметил Филипп Немов, врио начальника УБК МВД России, но для привлечения дроппа к ответственности за оказанные им «услуги» по выводу средств нужны доказательства. Если нельзя окончательно победить методы социальной инженерии, то максимально усложнить их, ограничить доступ дроппов к ДБО — реально.

Об ответственности граждан, передавших свои банковские карты или счета преступникам, говорят и представители банковского сообщества. С одной стороны, появление новых клиентов и открытие ими счетов — это бизнес банка. С другой — бесконтрольное

массовое открытие гражданином счетов в разных финансовых организациях и передача доступа к ним сторонним лицам или самостоятельное использование для вывода или перевода средств, полученных преступным путём, создаёт проблемы самим банкам, считает Николай Пятиизбянцев, начальник Управления противодействия мошенничеству в сфере информационной безопасности Газпромбанка. Кибермошенничество как криминальный бизнес выгодно и безопасно. Все уголовные дела заводятся на дроппов, а не на заказчиков преступлений. И существует два направления борьбы с явлением — разрушение схем вывода денежных средств и усиление ответственности за противоправную деятельность. Это работа правоохранительных органов.

СБОР ДОКАЗАТЕЛЬСТВ

О возможностях технико-криминалистического управления Следственного комитета РФ в части раскрытия преступлений подробно рассказал заместитель руководителя Главного управления криминалистики, руководитель управления, генерал-майор юстиции Иван Стрельцов. Под его началом работают 25 человек, имеющих юридическое и техническое образование, способных провести экспертизу носителей информации, баз данных, видео- и аудиоинформации и т.д. Благодаря сотрудникам управления и их коллегам в регионах уже раскрыты многие преступления и доказана вина подозреваемых.

О защите прав граждан, их персональных данных в рамках борьбы с фродом много говорили старший прокурор Генеральной прокуратуры России Аркадий Гриненко и начальник отдела центрального аппарата Прокуратуры г. Москвы Вадим Нидзельский. Отметив технические проблемы выявления и предотвращения фрода, они отметили необходимость уголовно-правовой защиты граждан. Криминальный бизнес распределяет обязанности внутри своих схем: есть дропперы, кол-центры, кто-то пишет вредоносное ПО, кто-то передаёт персональные данные в кол-центры. Необходима защита персональных данных не только средствами Кодекса об административных



правонарушениях РФ, но и путём внесения изменений в Уголовный кодекс РФ. Злоумышленники улавливают тенденции и развивают свои схемы. Всё чаще они используют доверие граждан к правоохранительным органам, поэтому последствия общения мошенников от имени правоохранителей значительны, о чём говорит статистика Банка России.

Ещё одна сторона вопроса — предотвращение вывода и легализации денежных средств. Такая работа ведётся, она не афишируется, поскольку носит закрытый характер. В работе принимают участие ФНС России, ФСБ, Росфинмониторинг, органы прокуратуры и финансовые организации, они видят выведенные средства и их масштаб. Средства, полученные от фрода, можно выявить, но часто они падают на счета и смешиваются с другими доходами, полученными преступным путём. Их легализация — другая сфера криминального бизнеса, и ей противостоят другими методами.

ПРАВИЛА АНТИФРОДА

Рост числа киберинцидентов в 2022 г. во многом связан с массовыми обращениями пострадавших к регуляторам и компаниям, работающим в сфере ИБ. В 2021 г. о таких вещах старались забыть и не говорить, считает Сергей Голованов, главный эксперт «Лаборатории Касперского». В 2023 г. он прогнозирует рост числа DDoS и

целевых хакерских атак, увеличение числа вирусов в сети Интернет до уровня 10–15-летней давности.

Алексей Сизов, руководитель Департамента по противодействию мошенничеству компании «Инфосистемы Джет», также отметил среди тенденций 2022 г. рост числа мошеннических операций с использованием методов социальной инженерии и переход мошенников на работу с системой быстрых платежей. Он отметил и массовый переход мошенников в мессенджеры, хотя ещё в конце 2021 г. работа в них была редка и каждый случай рассматривался аналитиками отдельно. Эксперт прогнозирует дальнейший рост фрода, но отмечает, что при правильном подходе компаний к вопросам ИБ смена вектора в деятельности хакеров не становится проблемой. В 80% случаев стандартные правила антифрода эффективны и работают, но требуют корректировки и отладки. Сложные кейсы требуют детального разбора специалистами.

По мнению А. Сизова, мероприятия по повышению уровня осведомлённости клиентов банков не отражаются на снижении уровня фрода. Нужны иные механизмы, которые принудительно подтолкнут граждан к правильным действиям. Также необходимы новые альтернативные способы подтверждения действий клиента, которые затруднят жизнь мошенникам и усложнят процесс вывода денежных средств со счетов жертв социальной инженерии.

«ИТ-СЕРВИС СЕГОДНЯ: ОТ ВЫЗОВОВ ДО РЕШЕНИЙ»

НИЧТО НАС В ЖИЗНИ НЕ ВЫШИБЕТ ИЗ СЕДЛА!

В конце года в Москве состоялась конференция «ИТ-сервис сегодня: от вызовов до решений», посвящённая вопросам сохранения работоспособности корпоративных цифровых инфраструктур после ухода с российского рынка ключевых поставщиков ПО и оборудования.

BANI — ЭТО ВАМ НЕ VUCA

Теоретические основы конференции были заданы на круглом столе «BANI-мир: выживать или развиваться?».

Кстати, лингвистический крой этой шапки заставил вспомнить BIS Summit 2019 — тогда тема форума звучала похоже: «Как выжить в VUCA-мире». Та аббревиатура обозначала Volatility Uncertainty Complexity Ambiguity — непостоянство, неопределённость, сложность, неоднозначность. А отсутствие знака вопроса в теме указывало, что тогда, три года назад, рецепт выживания предлагался.

BANI — это уже не VUCA. Хрупкий, беспокойный, нелинейный, непостижимый. О выборе модели поведения в таком мире и дискутировали. Забегая вперёд, скажу, что рецепты нашлись и в этих обстоятельствах.

О ЧЁМ ГОВОРИЛИ, К ЧЕМУ ПРИШЛИ?

Основными темами круглого стола стали:

♦ Как изменились приоритеты вашей компании после 24 февраля?

♦ Какие цели и задачи ставит бизнес перед ИТ в текущих условиях?

♦ Как эти задачи решает современный CIO и на какие критерии опирается компания при выборе подрядчиков с уходом вендоров?

В качестве спикеров выступали Н. Шуткин, вице-президент ВТБ; М. Григорьева, управляющий директор компании AXENIX (ранее Accenture); А. Тамбовский, директор по технологиям «ФОРС дистрибуция»; А. Тригуба, директор по развитию «AST», М. Сизов, управляющий партнёр «Мобиус Технологии».

Сценарный замысел круглого стола очевиден — два владельца цифровых инфраструктур для поддержки крупномасштабного бизнеса и две ИТ-компании с многолетним опытом цифровой поддержки такого рода бизнеса. И все они попали «под каток» разборки глобального масштаба.

О чём говорили, к чему пришли? Если вкратце, то в планах бизнеса — по-прежнему развивать цифровую поддержку своих деловых процессов, а в планах ИТ-компаний — продолжать помогать в этом бизнесу, сохранив свои коллективы и развивая свою «цифровую» компетентность.

Часть этих планов уже решена: коллективы сохранены, пути развития

намечены, как минимум на период работ по импортозамещению.

ОНИ УШЛИ, А ОПЫТ ОСТАЛСЯ

То, что планы ИТ-компаний не декларативны, было доказано в ходе докладов «Независимая сервисная компания. Миф или реальность?», «Гарантии надёжности ПО: развеём опасения», предложенных участникам конференции после круглого стола.

На примере мирового опыта технической поддержки продуктов компании Oracle директор по технологиям компании «ФОРС дистрибуция» рассказал о возможностях и принципах работы независимых сервисных компаний и об опыте перенесения этой практики на отечественную почву. Другой представитель «ФОРС дистрибуции» поведал о реализованных возможностях контроля безопасности прикладного и системного ПО, используемого в ИТ-инфраструктурах на основе продуктов Oracle.

Доклад «Цифровая устойчивость и независимость в условиях тотальной неопределённости» (от компании «Мобиус Технологии») обобщил опыт по оказанию базовой техподдержки в части комплексного управления ИТ-инфраструктурой (включая её развитие) на основе той части продуктов и технологий Open Source, которые приняты на вооружение и адаптированы к работе в цифровых инфраструктурах мировых ИТ-лидеров.

В дискуссиях на мероприятии были подняты вопросы эксплуатации уже развёрнутых ИТ-систем на основе оборудования иностранных компаний, ушедших с российского рынка, оценены риски этого для бизнеса. А в ходе неформального фуршета участники получили возможность обсудить конкретику организации техподдержки в новых условиях.

BANI — это уже не VUCA. Хрупкий, беспокойный, нелинейный, непостижимый. О выборе модели поведения в таком мире и дискутировали. Забегая вперёд, скажу, что рецепты нашлись и в этих обстоятельствах

ТРЕНД 2023 ГОДА — АТАКИ НА ИИ

ЭКСПЕРТЫ «ЛАБОРАТОРИИ КАСПЕРСКОГО» ПОДВЕЛИ ИТОГИ ГОДА И СДЕЛАЛИ ПРОГНОЗ НА 2023 ГОД

Эксперты «Лаборатории Касперского» пригласили журналистов и блогеров, собравшихся декабрьским утром в центре Москвы, погрузиться в мир цифровой природы. И хотя за окном бушевала метель, в небольшом зале была создана атмосфера тропиков Мадагаскара. Правда, в отличие от обитателей тропического леса речь шла о другом ландшафте.

Основные события года были связаны с концом февраля. Именно в этот момент изменился ландшафт угроз, исчезли телефонные мошенники и наступило кратковременное затишье, отметил Сергей Голованов, главный эксперт «Лаборатории Касперского» (ЛК). Впрочем, уже в мае эксперты отметили шквал мошеннических звонков, кибератак и взломов.

ПРО ТЕЛЕФОННЫХ МОШЕННИКОВ

По предварительным данным, в третьем квартале 2022 г. почти 52% пользователей поступили вызовы с неизвестных номеров с подозрением на мошенничество. По оценкам специалистов ЛК, нежелательные спам-звонки в июле-сентябре 2022 г. получили практически все пользователи.

Принятые регуляторами и операторами мобильной связи меры к концу августа остановили шквал звонков с подменных номеров. К концу года ситуация с мошенническими звонками вернулась в состояние, аналогичное 2021 г. Однако изменилась технология: мошенники перешли на звонки с мобильных номеров, а позже — на звонки через мессенджеры или с иностранных номеров, которые не могут отследить отечественные операторы. На текущий момент ситуация стабилизировалась и вернулась на уровень показателей начала февраля.

ПРО УТЕЧКИ

Ещё один тренд 2022 года — кража ПД. Суммарный объём персональных данных россиян, попавших в доступ с марта текущего года, составляет более 1,5 млрд не уникальных записей.

Эксперты ЛК отметили не только увеличение числа утечек, но и рост числа непрофессиональных хакеров и хакерских группировок. Они рекламируют свою деятельность в соцсетях, создают фальшивые новости с целью навредить репутации той или иной компании, дестабилизировать, обвалить котировку акций на бирже.

Был отмечен всплеск шифровальщиков и загрузчиков. Количество программ-вымогателей выросло на 181%, а загрузчиков — на 142%. Около 85% вредоносных файлов нацелено на ОС Microsoft. На 20% выросло число новых вредоносных под Linux, на 10% — под Android.

Растёт число атак на бизнес. Количество сложных атак на крупные предприятия выросло в 4–5 раз, растёт число утечек ПД. Если компанию не взломали сейчас, то взломают в будущем, полагает эксперт ЛК.

ПРО ДАРКНЕТ

Особый аспект, на который обратили внимание в ЛК, — состояние рынка найма работников из ИТ-сферы в даркнете. Специалисты изучили 155 форумов в даркнете и отобрали 800 объявлений на тему поиска и предложений работы. Ожидание соискателей — финансовая выгода. Доля резюме, по данным исследования, составила 17%, возможно, соискатели предпочитают откликаться на вакансии (83% объявлений).

Чаще всего в даркнете ищут разработчиков (61% объявлений). Среди программистов популярны веб-разработчики (60%) и вирусописатели. Востребованы специалисты по проведению атак (17% предложений). Порядка

10% вакансий ориентированы на дизайнеров, реже требуются администраторы (6%) и реверс-инженеры (4%). Гарантий, что «работодатель» выполнит обещания, никто не даёт. Одновременно действия такого «сотрудника» подпадают под статьи УК РФ, отмечают специалисты ЛК. Несмотря на сложности работы в этой сфере, первые приговоры хакерам в российских судах уже прозвучали.

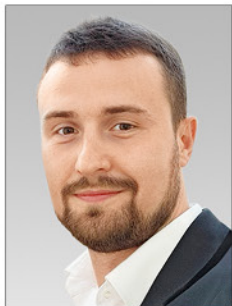
ПРОГНОЗЫ

Санкции, уход операторов Visa и MasterCard свели на нет такое явление, как кардинг. Полностью нарушены схемы вывода средств. Поэтому опасаться, что деньги с банковской карты в Москве будут списаны в Аргентине, сегодня не стоит. И это всё о положительных трендах.

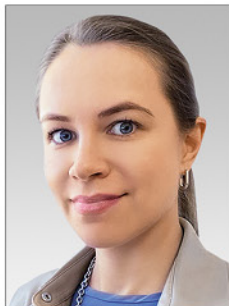
В 2023 г. вероятность встретить вирус в Интернете составит 75%. Также наблюдается рост вредоносного ПО (45–54%). В ЛК считают, что число хакерских атак вырастет в два раза, одновременно сократится время реагирования на них. Во многом это сокращение произойдёт благодаря усилению регуляторной политики ЦБ и Минцифры.

Компаниям необходимо задуматься о своей информационной безопасности, считает в ЛК. Чем меньше времени пройдёт между обнаружением киберинцидента и началом работы специалистов, тем активнее пойдёт расследование и тем меньше ущерба, в том числе репутационного.

Отмечая необходимость системного подхода к кибербезопасности, в ЛК прогнозируют продолжение DDoS-атак, шифровальщиков, утечки данных, в том числе через цепочки поставок. Количество хакерских группировок растёт, в их прицел попадают технологические компании. Ожидаются дальнейшие атаки на искусственный интеллект, начало которым положено в этом году. Это тренд 2023-го и последующих годов.



Алексей РОМАНЕНКО
ведущий научный сотрудник,
группа компаний ЦРТ



Олеся КУЛИКОВА
менеджер продукта ASR,
группа компаний ЦРТ



Ольга РУДНИЦКАЯ
ведущий системный аналитик,
группа компаний ЦРТ

ЗОЛОТЫЕ РЕБЯТА

РОССИЙСКАЯ КОМАНДА В ОЧЕРЕДНОЙ РАЗ ОДЕРЖАЛА ПОБЕДУ НА МЕЖДУНАРОДНЫХ СОРЕВНОВАНИЯХ ПО РАСПОЗНАВАНИЮ РЕЧИ!

В 2022 году группа компаний ЦРТ победила в международном конкурсе GRAM VAANI ASR Challenge¹, который был посвящён распознаванию спонтанной — естественной — речи в телефонном канале на языке хинди. Теперь распознавание речи от группы ЦРТ доступно на 14 языках: русском, английском, казахском, испанском, арабском, немецком, французском, турецком, бенгальском, филиппинском, фарси, урду, португальском, хинди.

ОБ ОРГАНИЗАТОРАХ КОНКУРСА

Цель конкурса GRAM VAANI ASR Challenge 2022 — распознавание спон-

танной речи на языке хинди в телефонном канале.

Gram Vaani управляет несколькими платформами голосовых средств массовой информации в Индии. Эти платформы работают на основе IVR: люди звонят по уникальному номеру телефона, объявленному Gram Vaani, после чего сервер IVR прерывает звонок и автоматически перезванивает человеку, делая звонок бесплатным для пользователя. Во время этого звонка пользователи могут записать голосовое сообщение, которым они хотят поделиться, или прослушать голосовые сообщения, оставленные другими пользователями. Эти голосовые сообщения охватывают различные области: новости, вопросы о сельском хозяйстве или здравоохранении, а также народные песни и стихи.

После получения голосового сообщения модераторы Gram Vaani рассматривают его, и, если сообщение признаётся приемлемым, оно публикуется на платформе и может быть услышано другими пользователями. Пользователи могут добавлять комментарии, ответы или создавать собственные сообщения. Эти записи голосов тысяч пользователей Gram Vaani, соответствующие транскрипции, составили набор данных, на основе которого решалась задача конкурса.

О ПРОИСХОЖДЕНИИ ДАННЫХ

Набор данных включал в себя данные телефонного качества речи на хинди. Записи были собраны с помощью платформы Mobile Vaani, работающей с пользователями со всей Индии, и,

Участие в международном конкурсе по распознаванию речи на языке хинди — новый уровень для российских разработчиков: язык экзотичный, сложный, непривычный, а среди конкурентов были и команды, для которых этот язык родной. Именно поэтому победа во всех треках этого конкурса была особо значимой — она демонстрирует не просто распознавание ещё одного языка, а широкий спектр возможностей российских разработчиков в области распознавания речи. Качество распознавания речи и многообразие языков и диалектов укрепляют позиции ЦРТ в области речевых

технологий, позволяют переводить сервисы из разряда инновационных в повседневные, позволяют совершенствовать речевую аналитику — автоматизировать работу контактных центров: распознавать естественную речь, делать выводы об удовлетворённости клиента и качестве диалога — существенно оптимизировать работу современных контакт-центров ретейла, e-commerce, телеком, а также создавать диалоговых ассистентов — интеллектуальных текстовых и голосовых роботов для крупного бизнеса и государственного сектора, с которыми легко и приятно взаимодействовать.

¹ <https://sites.google.com/view/gramvaaniasrchallenge/home?authuser=0>

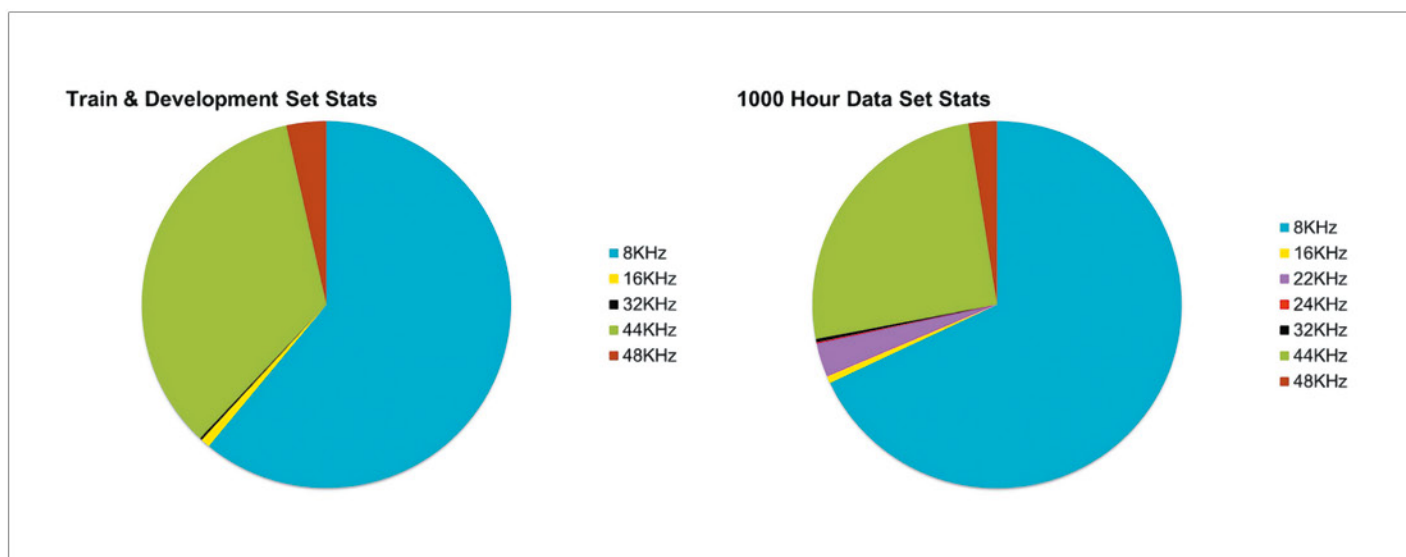


Рисунок 1. Данные были предоставлены в виде mp3-файлов, среди которых присутствовали записи с разнообразной частотой дискретизации (8, 16, 32, 44 и 48 кГц)

следовательно, включают региональные и диалектные вариации хинди. Записи сопровождаются эталонными расшифровками — транскрипциями, сделанными сотрудниками, которые были набраны через крауд-платформу Uliza.

В конкурсе было представлено четыре набора данных.

- ♦ **Отекстованные данные для обучения** — 100 часов телефонных переговоров. По заявлению организаторов, эталонные расшифровки записей могли быть не очень точными.

- ♦ **Неотекстованные данные для обучения** — 1000 часов записей преимущественно из телефонного канала. Для этих данных расшифровки и детальные характеристики не были предоставлены.

- ♦ **Отекстованный отладочный набор данных (dev set)** — 5 часов телефонных переговоров, для которых организаторы предоставили точные эталонные расшифровки.

- ♦ **Отекстованный тестовый набор данных (eval set)** — 5 часов телефонных переговоров, на которых организаторы проводили финальное сравнение систем распознавания. Эталонных расшифровок для этого набора организаторы не предоставили, чтобы исключить возможность подстройки систем под конкретный тестовый набор.

Данные были предоставлены в виде mp3-файлов, среди которых присут-

ствовали записи с разнообразной частотой дискретизации (8, 16, 32, 44 и 48 кГц). Статистика по данным на рис. 1 и по ссылке <https://sites.google.com/view/gramvaaniasrchallenge/dataset?authuser=0>

ТРИ ТРЕКА

В конкурсе было заявлено три трека:

- 1. Closed Challenge** — для подготовки любых моделей можно было использовать только 100 часов отекстованных данных для обучения и 5 часов данных отладочного набора. Использование различных предобученных моделей в этом треке было запрещено. Необходимо было готовить систему распознавания с нуля, имея лишь данные обучающего и отладочного наборов.

- 2. Self Supervised Closed Challenge** — для подготовки любых моделей, дополнительно к изложенному выше, можно было использовать 1000 неотекстованных данных, предоставленных организаторами.

- 3. Open Challenge** — для подготовки моделей можно было использовать любые доступные данные (в том числе наборы с открытой лицензией, наборы, собранные самостоятельно из открытых источников, и т.д.), а также предобученные нейросетевые модели (экстракторы эмбедингов, готовые системы распознавания, и т.д.)

Команда ASR группы компаний ЦРТ участвовала во всех трёх треках.

КЛЮЧЕВЫЕ УЧАСТНИКИ

В конкурсе участвовали ведущие мировые и индийские исследовательские команды, в том числе:

- ♦ **LEAP LAB IISC & SRI** — совместная команда Индийского института наук LEAP LAB IISc и Американского некоммерческого научно-исследовательского института SRI (бывший Stanford Research Institute);

- ♦ **Speech@SRI-B** — команда исследовательского института Samsung R&D в Индии;

- ♦ **CDAC_M** — Индийский центр разработки перспективных вычислительных технологий CDAC_M;

- ♦ **TU Delft** — команда Делфтского технического университета в Делфте, Нидерланды TU Delft (старейший и крупнейший технический университет в Нидерландах);

- ♦ крупные индийские R&D-компании: **Uniphore Software Systems** — компания, специализирующаяся на ИИ в сфере речевого взаимодействия, в частности в кол-центрах, **Cogknit** и другие.

Полный список участников можно найти по ссылке <https://sites.google.com/view/gramvaaniasrchallenge/leaderboard?authuser=0>. География участников на рис. 2.

НАУЧНЫЕ ПОДХОДЫ

В ходе конкурса нашей команде удалось применить разнообразные технологии, в том числе:



Рисунок 2. География участников

1. Unsupervised и Semi-supervised-обучение экстракторов признаков. В рамках первого и второго конкурсных треков команда обучала с нуля модели, архитектурно аналогичные wav2vec 2.0. Такие модели для обучения требуют значительных объемов данных, поэтому в первом треке мы использовали множество разнообразных техник аугментации обучающего набора данных. В том числе были использованы: аугментация кодеками (звук перекодируется различными кодеками со сжатием, а затем восстанавливается в формат, пригодный для использования в подготовке моделей), аугментация изменением скорости и громкости (speed and volume perturbation), аугментация в процессе обучения, заключающаяся в деформации спектрального представления звука — применение временных и частотных искажений для маскирования блоков последовательных временных шагов или мел-частотных каналов. Во втором треке обучение таких моделей проводилось с добавлением неотекстованного набора данных в 1000 часов, с последующей адаптацией на 100-часовом отекстованном обучающем множестве. В рамках работ по третьему треку конкурса команда использовала предобученную модель wav2vec 2.0

(CLSRIL-23) в качестве экстрактора высокоуровневых признаков для дальнейшего обучения акустических моделей. Базовая CLSRIL-23 модель была дообучена в различных режимах на данных конкурса. Адаптированные модели позволили подготовить итоговые системы распознавания, которые на вход получают высокоуровневые эмбеддинги, и демонстрируют высокую точность распознавания.

2. End-to-end модели. В ходе конкурса мы, наряду с классическим гибридным подходом, применили современный подход к построению систем распознавания речи, основанный на E2E-моделях. Был обучен ряд моделей на архитектуре Conformer. Как правило, такие модели весьма требовательны к объему обучающих данных. Однако нам удалось подготовить E2E-модель с высоким уровнем точности распознавания даже для первого трека, в котором доступны лишь 100 часов обучающих данных. Во втором и третьем треках мы смогли в полной мере воспользоваться 1000-часовым набором для обучения E2E-моделей. На первом этапе мы подготовили текстовки для всех 1000 часов с помощью распознавания имеющимися у нас на тот момент классическими гибридными моделями. Для повышения

точности подготавливаемых текстовок в распознавании мы использовали комбинацию таких моделей с последовательным применением нескольких постобработок (рескорингов результатов распознавания). Такая стратегия позволила нам получить максимально точные текстовки, которые мы затем использовали в качестве эталонных расшифровок при обучении E2E Conformer моделей для второго и третьего треков. В каждом из треков конкурса результаты распознавания E2E-моделями были использованы в комбинации с классическими гибридными моделями для получения финальных результатов распознавания.

3. Различные виды постобработки (рескоринга) для улучшения итогового результата распознавания. Для получения итоговых результатов распознавания мы использовали несколько моделей для постобработки (рескоринга) результатов. Для первоначальной постобработки результатов мы применили нейросетевую языковую модель AWD-LSTM, которая перевешивала языковые веса в результатах распознавания, представленных в виде сеток. Затем, модифицированные сетки подавались на две более продвинутые нейросетевые языковые модели — GPT2-Hindi и Transformer.

TYPE	WER		CER	
Closed Challenge Winners	Speech @ SRI-B #2	23.3251	STC #2	12.1874
	STC #2	23.7579	STC #1	12.3882
	STC #1	24.7938	LEAP LAB IISc & SRI	14.1155
Self Supervised Closed Challenge	STC #2	22.1856	STC #2	11.23
	LEAP LAB IISc & SRI #2	26.0442	STC #1	13.1838
	STC #1	26.1441	TU Delft #1	13.4227
Open Challenge	STC #2	18.2161	STC #3	8.92973
	STC #3	18.2568	STC #2	8.93449
	STC #1	19.0855	STC #1	9.4826

Рисунок 3. Результаты конкурса. Наша команда (STC) заняла первые места во всех трёх треках

При помощи этих моделей гипотезы в сетках распознавания вновь перевзвешивались. В итоге результатом применения всего пайплайна постобработки являлись два комплекта сеток распознавания, каждый из которых был получен с применением разной последовательности моделей (AWD-LSTM GPT2-Hindi и AWD-LSTM Transformer). Стоит отметить, что ввиду ограничений в правилах конкурса для первого и второго трека использовалась только AWD-LSTM модель, так как доступный объём текстовых данных позволял обучить только подобного рода архитектуру.

4. Для получения итоговых результатов распознавания в каждом из треков использовалась комбинация

наилучших соответствующих комплектов сеток (результатов распознавания от различных систем с применением подходящих стратегий постобработки). Параметры комбинации моделей определялись на отекстованном отладочном множестве данных и затем применялись в ходе формирования финальных сабмитов с результатами для тестового множества.

РЕЗУЛЬТАТЫ КОНКУРСА

Наша команда (STC) заняла первые места во всех трёх треках (рис. 3).

Полная версия результатов всех участников доступна по ссылке <https://sites.google.com/view/gramvaaniasrchallenge/leaderboard?authuser=0>

Комментарии:

♦ В **closed challenge** мы немного уступили по **WER** (на 0,4%), однако значительно оторвались по **CER** (на 1,9%) от ближайших соперников. Стоит отметить, что результат команды Samsung (Speech@SRI-B #2), показавший лучшее значение **WER**, по **CER** уступил нашему на более чем 2%.

♦ В треках **self-supervised** и **open challenge** мы продемонстрировали результаты, значительно превосходящие результаты соперников как по **WER**, так и по **CER**.

♦ Рядом с названиями команд #1 #2 #3 обозначают номера сабмитов (каждая команда могла отправить три результата распознавания по каждому из треков).

Для оценки качества распознавания речи традиционно используются метрики пословная ошибка распознавания (word error rate, WER) и посимвольная ошибка распознавания (character error rate, CER). Чем меньше значение этих метрик, тем лучше качество распознавания речи.

Для получения оценки WER сравнивают последовательность распознанных слов (результата распознавания) с последовательностью сказанных слов (эталонной текстовкой). Производится сопоставление (выравнивание) этих двух последовательностей, которое обеспечивает минимальное количество вставок, удалений и замен слов, позволяющих преобразовать идеальную текстовку в результат распознавания. Такое количество называют «редакционным расстоянием» (расстоянием Левенштейна) между двумя последовательностями слов. WER измеряется в процентах:

$$WER = \frac{I + D + S}{N} \cdot 100\%$$

где I — вставки (Insertions), количество добавленных в исходную строку слов,

D — удаления (Deletions), количество удалённых из исходной строки слов,

S — замены (Substitutions), количество заменённых слов, N — количество слов в исходной строке.

Метрика CER рассчитывается таким же образом, но учитывается количество добавленных, удалённых и заменённых символов без учёта пробелов.

Для хинди обе эти метрики крайне важны, так как язык является символьным, текст на нём выглядит примерно так: नादया और राम की बलि्ली.



**Сергей
РОМАНОВСКИЙ**
начальник отдела
рисков ИБ ВК



ШАГ ЗА ШАГОМ ПОСТЕПЕННО

КАК ВЫСТРОИТЬ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ НА ОСНОВЕ СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ

За последние годы зависимость уровня корпоративных рисков от принятой в компании культуры кибербезопасности устойчиво растёт. По результатам опроса McKinsey Global Survey¹, топ-менеджеры большинства компаний признают управление информационными рисками важной частью своей операционной деятельности.

В условиях быстрого развития цифровых систем рациональное использование бюджетов на инвестиции в ИБ становится для компании стратегическим приоритетом. Всё чаще при обсуждении планов по развитию ИБ

звучат аргументы в пользу перехода от реактивного стиля управления информационными рисками, продиктованного горящими запросами операционных процессов, к методам, основанным на анализе рискообразующих компонентов цифровых продуктов, потребностей клиентов, рисков третьих сторон, динамики развития нормативной базы.

Решения о том, как наилучшим образом управлять информационным риском, достигаются при участии как минимум трёх заинтересованных сторон — бизнес-подразделения или «владельца риска», ИТ- и ИБ-отделов. И парадокс ситуации в том, что каждая сторона будет отстаивать собственный интерес. ИТ будет сфокусировано на

наборе конкретных мероприятий и проектных инициатив, которые гарантированно снизят риски до приемлемого уровня. ИБ будет максимально интересоваться качеством, управляемостью и прозрачностью этих мероприятий. Бизнес-руководители и владельцы цифровых продуктов будут принимать решение о затратах на реализацию инициатив, оценивая стоимость решений и приоритетность их реализации в терминах оптимизации затраченного времени, денег и операционных усилий.

КЛАССИЧЕСКИЙ ПОДХОД

В настоящее время подходы к управлению информационными рисками, основанные на оценке моделей зрелости, по-прежнему являются самыми

¹ <https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/a-time-for-boards-to-act>

распространёнными, «золотым стандартом качества». Эти подходы направлены на достижение зрелости путём создания определённых функций обеспечения защиты. Например, для достижения одного из уровней зрелости организация может создать центр управления безопасностью (SOC), чтобы улучшить оценку, мониторинг и реагирование на потенциальные угрозы для корпоративных информационных систем и приложений. Или внедрить многофакторную аутентификацию (MFA) по всему перечню активов, чтобы повысить уровень зрелости контроля доступа.

Подход к управлению рисками, основанный на оценке зрелости, может быть полезен в ситуациях, когда требуется запустить программу обеспечения ИБ «с нуля», но для организаций, которые продвинулись дальше «нулевого уровня», этот подход уже неприменим.

В данном случае проявляется классическая проблема «органического роста» практически любой компании: по мере усложнения бизнеса в какой-то момент происходит неуправляемое увеличение контрольных и надзорных процедур. Особенно это показательно в мониторинге процессов ИБ, когда у компании возникает желание максимально реализовать принцип «контролировать всё». Результат чаще всего плачевный: когда количество приложений в мониторинге превысит возможности аналитиков и технических инструментов, автоматизация контрольных средств затормозит операционные процессы компании. Но в реальности только некоторые приложения содержат в себе серьёзные уязвимости с высоким потенциалом риска. Поэтому для снижения риска необходимо перейти от позиции «контроля всего» к выборочному мониторингу наиболее критичных приложений или функций.

Объём способов контроля растёт из года в год, поскольку планирование программ кибербезопасности по-прежнему требует увеличения расходов на дополнительные средства. К тому же такие программы часто создают парализующий эффект, когда вынуждают и без того перегруженные практическими мероприятиями команды параллельно внедрять и совершенствовать большое количество процессов обеспечения ИБ.

В результате ни один проект никогда не реализуется полностью, а на информационных панелях программ постоянно отображается «жёлтый» статус для всего набора инициатив.

УПРАВЛЕНИЕ НА ОСНОВЕ АНАЛИЗА РИСКОВ

На фоне внешнего роста киберугроз всё больше компаний начинают анализировать возможности по снижению информационных рисков и оценивать свой «аппетит к риску» (уровень риска, который организация готова принять, не принимая дополнительных действий для его снижения).

Максимально нивелировать киберриск — это непростая задача для любой компании. Для достижения наибольшей отдачи от инвестиций нужно привлекать значительный объём ресурсов и применять этот подход ко всем компонентам программы обеспечения ИБ. Но проблема в том, что многие организации зачастую не могут точно определить, как и насколько необходимо снизить риск.

Например, инвестиции в снижение корпоративных рисков лучше окупаются благодаря информированию и обучению сотрудников. Модель, основанная на оценке зрелости, в данном случае не потребует от организации анализа соотношения «величина риска / издержки на снижение риска» и оценки объёма необходимого финансирования для организации дополнительных систем мониторинга. И это в результате приведёт к тому, что расходы пойдут на оба направления — и мониторинг, и развитие сотрудников (осведомлённость и обучение), хотя одно из них может иметь несоразмерное влияние на снижение корпоративных рисков по сравнению с другим.

Утвердив снижение риска в качестве основной цели, компании могут точнее и эффективнее расставлять приоритеты при выделении бюджетов на ИБ (особенно это применимо к задачам, связанным с внедрением контролей, включая средства защиты информации (СЗИ). В идеальной картине мира это помогает руководству добиться чётких, прагматичных проектов, согласованных на первой, второй и третьей линиях защиты. Такой подход помогает

осуществлять как стратегические, так и тактические действия по снижению рисков, позволяя компании больше не внедрять механизмы «тотального контроля и мониторинга», а направлять своё внимание на наиболее уязвимые места в текущем моменте.

ТРАНСФОРМАЦИЯ ВНУТРИ КОМПАНИИ: С ЧЕГО НАЧАТЬ?

Организации, применяющие подход, основанный на оценке зрелости, в какой-то момент неизбежно сталкиваются с проблемой перехода к модели управления, основанной на оценке рисков. Для этого необходимо реализовать набор инициатив в определённой последовательности:

1. Встроить систему управления рисками ИБ в структуру управления корпоративными рисками организации.

2. Создать в организации условия для формирования принципов риск-культуры, чтобы повысить уровень профессиональных компетенций сотрудников в вопросах обеспечения ИБ.

3. Классифицировать уязвимости организации в терминах бизнеса в отношении людей, процессов, технологий и продуктов в масштабах организации, включая интересы третьих сторон.

4. Создать модель «субъектов угрозы», определить их возможности и мотивацию.

5. Разработать модель гибкого управления проектами в привязке к структуре уязвимостей, которые они устраняют. Определить, какие усилия необходимы для реализации и совершенствования модели.

6. Сравнить корпоративные риски с системой управления рисками ИБ, учитывая субъектов угрозы и их возможности, а также уязвимости, которые они стремятся использовать, и средства контроля ИБ.

7. Сопоставить риски ИБ с «аппетитом к риску», чтобы понять, как усилия в области ИБ снижают риски организации.

8. Обеспечить мониторинг рисков ИБ и мероприятий по их снижению через реализацию ключевых показателей риска (KRI) и ключевых показателей эффективности (KPI) внедряемых процедур по обеспечению ИБ.

**Юрий КАРДЮКОВ**руководитель направления Identity Platform
и Open API, eKassir

ЗАЩИЩАЯ API

НУЖНО СОКРАТИТЬ РАСХОДЫ НА ИБ

Когда некая компания открывает API, возникают информационные потоки, вовлекающие клиентов и партнёров. Это ставит перед службой информационной безопасности и программными архитекторами задачу обеспечить защищённый обмен данными и предоставить контролируемый доступ к API.

Им нужно разработать меры противодействия внешним угрозам, опасностям утраты или кражи токенов доступа у партнёров и/или клиентов, а также обеспечить безопасность внутреннего контура. Они должны помнить, что существует также риск непреднамеренно раскрыть через токен доступа важную информацию — о местонахождении партнёров, уровне доверия к ним и т.д.

Безопасная работа с API — объёмная тема, требующая вдумчивого изучения и подробного обозрения. В этой статье мы остановимся в основном на безопасности при выпуске токена доступа, рассмотрим методы его защиты и хранения.

Мы покажем, как можно защитить доступ к API, заметно сократив расходы на информационную безопасность. Продемонстрированная вам практика реализации этой задачи основывается на опыте разработки и внедрения ПО eKassir Identity Platform.

API ДЛЯ ПАРТНЁРОВ И API ДЛЯ КЛИЕНТОВ

Открывая API в своей ИТ-инфраструктуре, компания может выделить два сценария:

- ♦ API для клиентов;
- ♦ API для партнёров.

Общие принципы безопасности для обоих сценариев схожи, но существуют принципиальные отличия, которые надо учитывать при проектировании ИБ-системы.

Когда компания предоставляет API для пользователей (клиентов), обычно подразумевается взаимодействие с человеком посредством UI. Клиент скачивает мобильное приложение либо открывает веб-сайт и работает в интерфейсе. В ответ приложение или браузер отправляют запрос к API компании.

API для партнёра предполагает тип взаимодействия «система к системе» (system 2 system), при котором UI не используется. Одна информационная система подключается к API другой, передаёт входные параметры и обрабатывает полученные данные напрямую.

Партнёры, как правило, обладают высокой квалификацией в области информационных технологий и безопасности и содержат собственную

ИТ-инфраструктуру. Им не составит проблемы использовать инфраструктуру публичных ключей (PKI), чтобы идентифицировать друг друга и организовать взаимную аутентификацию mutual TLS (mTLS). Клиенты же, являющиеся конечными потребителями продукта, не только не обладают, но и не должны обладать компетенциями в ИТ-области.

Взгляните на таблицу, которая демонстрирует принципиальную разницу между клиентами и партнёрами (рис. 1).

ЧТО ТАКОЕ ТОКЕН ДОСТУПА?

Сервис, который предоставляет API, должен авторизовать запрос, то есть убедиться, что запрашивающий субъект обладает привилегиями на его выполнение. Современные стандарты авторизации и аутентификации OAuth 2.0 и OpenID Connect используют токен доступа (access token) в

Клиенты	Партнёры
Всегда есть пользователь	Пользователь может отсутствовать
Взаимодействие через UI	Взаимодействие через сервисы (system 2 system)
Компетенции в ИТ отсутствуют	Высокая компетенция в ИТ. Есть собственная инфраструктура
Сложность при работе с сертификатами	Возможность работы с сертификатами

Рисунок 1. Таблица демонстрирует принципиальную разницу между клиентами и партнёрами

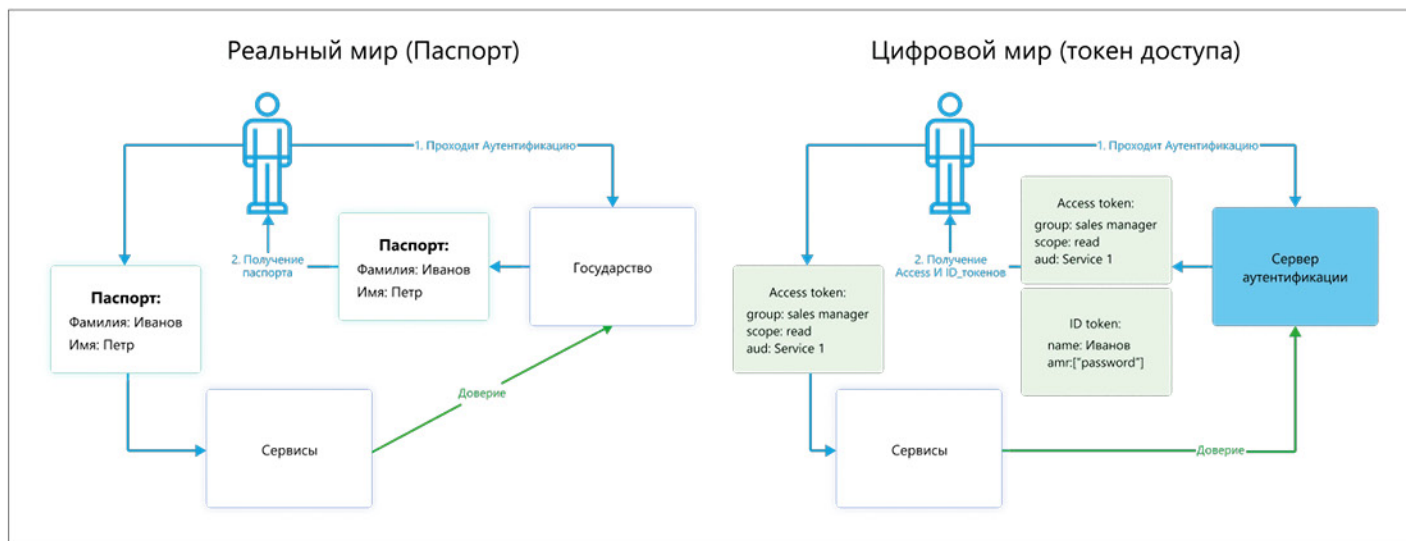


Рисунок 2. Пользователь (или система) аутентифицируется на сервере, после чего тот выпускает токен доступа, содержащий в виде утверждений информацию о пользователе (системе) и его привилегиях: каким сервисом он может пользоваться и какие действия на сервере ему разрешены

качестве источника авторизационной информации.

Наиболее полно понять, что такое токен доступа, поможет аналогия между цифровым и реальным миром.

Молодой житель Российской Федерации обращается в территориальный орган МВД, чтобы получить выпущенный и заверенный государством паспорт гражданина. Все структуры и службы России безоговорочно доверяют государству, и когда гражданин предъявляет паспорт, например, в банк или в МФЦ, их сотрудники уверены, что данные о Ф. И. О., прописке и дате рождения гражданина полностью достоверны.

В цифровом мире в роли государства выступает **сервер аутентификации** — единый центр администрирования проверок подлинности всех сервисов и ресурсов. Пользователь (или система) аутентифицируется на сервере, после чего тот выпускает токен доступа, содержащий в виде утверждений информацию о пользователе (системе) и его привилегиях: каким сервисом он может пользоваться и какие действия на сервере ему разрешены (рис. 2).

Мы в eKassir разработали программный комплекс **Identity Platform**, позволяющий создать единый центр аутентификации, управления доступом и защиты API. Один из его компонентов (**Access Manager**) как раз является таким сервером. После публикации

токена Access Manager заверяет данные цифровой подписью, благодаря чему их невозможно модифицировать.

При каждом обращении к API сервиса пользователь предъявляет токен доступа. Поскольку сервис доверяет Access Manager, то и в релеванности токена не сомневается. Сервис проверяет подпись, и если всё в порядке, то, удостоверившись, что токен доступа не был модифицирован, считывает утверждения и на их основании авторизует пользователя. В противном случае запрос отклоняется. Например, если для запрашиваемой операции нужна административная роль, а сервис не находит значение **privileged** в утверждении **role**, он отклоняет запрос.

ПОЧЕМУ ВАЖНО ЗАЩИЩАТЬ ТОКЕН ДОСТУПА?

Как сказано выше, токен доступа определяет привилегии пользователя. Большинство токенов имеют формат bearer («предъявитель»), то есть их предъявители получают и могут пользоваться установленными привилегиями.

Токен доступа — этакая «шкатулка» с драгоценностями в виде клиентской информации, которая представляет первостепенный интерес для злоумышленников. Наличие токенов доступа на устройстве создаёт предпосылку для возникновения вектора хакерской атаки на него, а потому их максимальная защита так важна.

К сожалению, защитой токена нередко пренебрегают. Некоторые компании просто выпускают токены доступа, передают их клиентам или партнёрам и более не думают о мерах безопасности. Последствия подобной беспечности хорошо известны: кража данных, финансовые махинации, слитые клиентские базы и прочее.

На примере решения Identity Platform рассмотрим, с помощью каких методов можно обеспечить высокую степень защиты токенов доступа и реализовать механизм их безопасного хранения.

ЗАЩИТА API ПАРТНЁРА

Как правило, партнёры eKassir обладают собственной ИТ-инфраструктурой и способны обеспечить безопасность токенов доступа. Однако перекрыть все уязвимости или полностью обезопасить себя от кражи токена они не могут.

Мы передаём им токены доступа и при помощи Identity Platform принимаем дополнительные меры безопасности. Например, можем привязать токен к системам партнёра на принудительной основе — и даже если он будет украден, то злоумышленники никак не смогут им воспользоваться.

Защита от внешних угроз. На первой линии защиты необходимо ограничить использование API, предоставив эту возможность только доверенным партнёрам. Для этого понадобится его безопасная аутентификация.

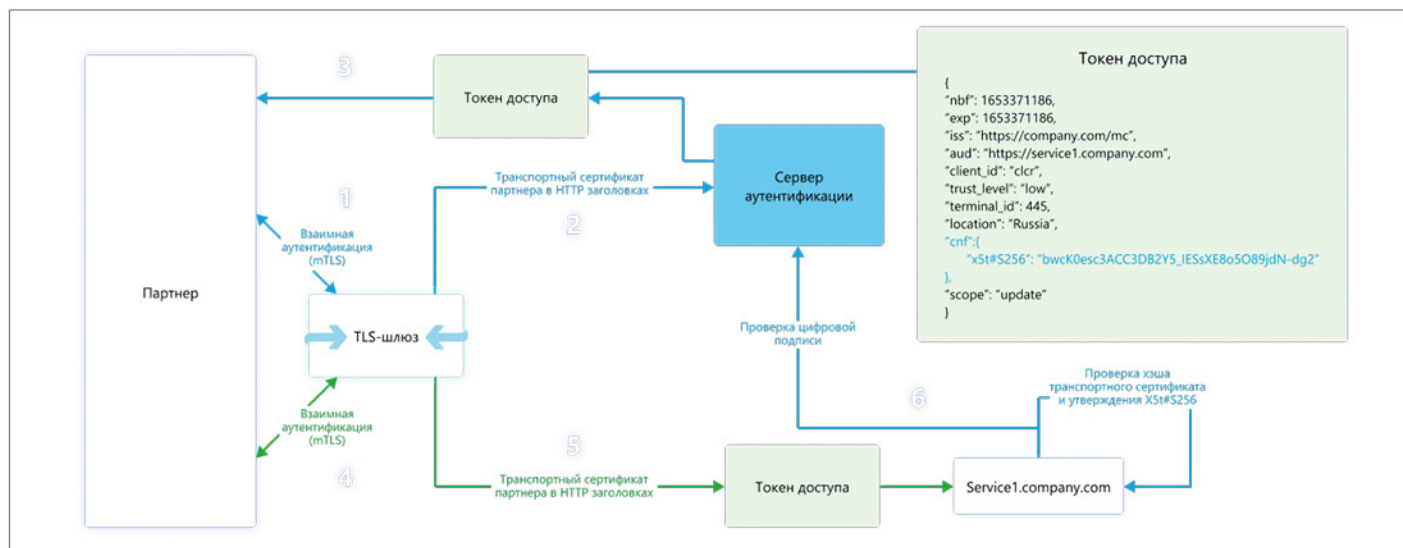


Рисунок 3. Реализация такого мероприятия помогает защитить партнёров и предотвратить неправомерное использование токенов доступа, которые были похищены

```
POST /v1/open-banking/statements/100200 HTTP/1.1
Host: service1.company.com
x-jws-signature:
eyJhbGciOiJSUzI1NiIsImtpZCI6IjY2NjVCRDA0QUQ0M0JENzY1RDczNDhCNkM3QTdEODI0MTFBMEQ0RTkiLCJ4NXQiOiJabVc5QksxRHZYWmRjMGkyeDZmWUUpRC2cx2TsiLCJ0eXAiOiKV1QifQ.SODIo-q192OUUPY9IbPIVSIthpujYlWGe-
RZkORL7l0iXmWQ0l7nRJVsXiMcy4jZldc_ZLVjN9xfNqyXeoY7Elm3xP8e4WeaJRcD4sEyC9fpUsSM5Q3mLw_gJfO47Hxq
Authorization: Bearer 359f3ba0175ebf0094e9110b25d8ee81d8eee0e24aae48c19bf9655e3bf5c5d2
Content-Type: application/json
Content-Length: 153

{"Data":{"Statement":{"accountId":"100200","fromBookingDateTime":"2020-01-03T00:00:00+00:00","toBookingDateTime":"2020-02-03T00:00:00+00:00","amount":"100.00","currency":"RUB"},"Risk":{"}}
```

Рисунок 4. Если внутри контура нагрузка была модифицирована, сервис обнаружит фрод и откажется выполнять запрос

Согласно Стандарту Банка России **СТО БР ФАПИ.ПАОК-1.0-2021** считаются безопасными те методы аутентификации, которые одновременно:

- ◆ не передают секрет в открытом виде;
- ◆ используют инфраструктуру публичных ключей (PKI).

К сожалению, распространённые методы аутентификации при помощи пароля, API Key или с применением симметричного хеширования HMAC не обеспечивают должный уровень защиты. Так, пароль и API Key передают секрет в открытом виде, а HMAC не использует PKI.

Но можно обойти эту проблему, сделав обязательной взаимную аутентификацию между сервером API и партнёром на транспортном уровне mTLS с проверкой сертификата. Подключиться к API в этом случае могут лишь партнёры, получившие от доверенного удостоверяющего центра сертификат X.509.

Уже эта мера отсекает существенную часть внешних угроз.

Защита от кражи токенов доступа.

На второй линии выполняется привязка токена доступа к партнёру. Тип токена доступа как бы замещается другим, с более высоким статусом: токен bearer («предъявитель») становится токеном PoP (Proof of Possession — «доказательство обладания») или, по-другому, HoK (Holder of the Key — «держатель ключа»).

При таком подходе в утверждении токена доступа записывается информация об отпечатке транспортного сертификата партнёра. Получив такой токен, сервисы проводят дополнительную валидацию: они сравнивают отпечаток сертификата во входящем запросе с утверждением, находящимся в самом токене. Если они отличаются, значит, имел место фрод: некто завладел токеном и неправомерно его использует.

Реализация такого мероприятия помогает защитить партнёров и предотвратить неправомерное использование токенов доступа, которые были похищены (рис. 3).

Защита от внутренних угроз. Ключевые меры обеспечения безопасности — настроенная взаимная mTLS-аутентификация и привязка токена доступа к партнёру — надёжно защищают API «снаружи». Но что делать с внутренними угрозами?

После терминации TLS-соединения, но до того как сервис получит запрос и обработает его, полезная нагрузка остаётся без защиты и возникают векторы атаки, которыми поспешит воспользоваться злоумышленник.

Решить проблему партнёр может при помощи цифровой подписи полезной нагрузки. Перед отправлением запроса нагрузка подписывается, и подпись размещается в HTTP-заголовке. Получив

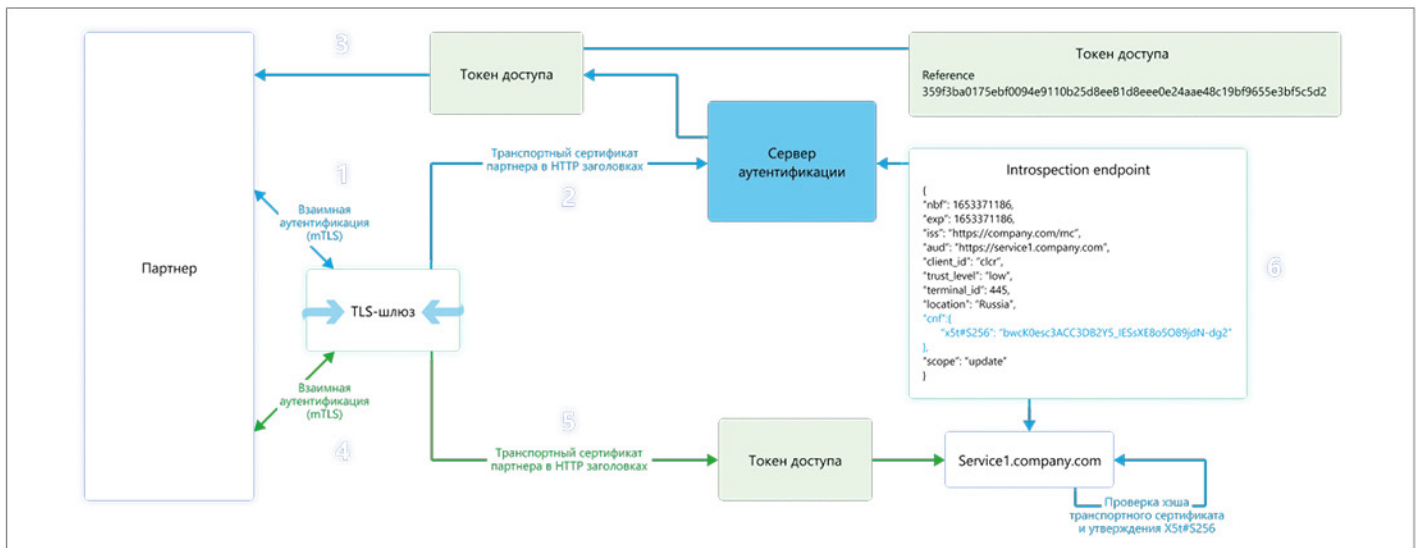


Рисунок 5. Identity Platform предлагает решить проблемы другим, лишённым перечисленных недостатков, способом

запрос, сервер API вычисляет подпись и сравнивает с содержимым заголовка, тем самым проверяя аутентичность полезной нагрузки. Если внутри контура нагрузка была модифицирована, сервис обнаружит фрод и откажется выполнять запрос (рис. 4).

Защита от нераспространения информации. Партнёрам доступно содержимое токена доступа, и они видят его утверждения — это создаёт риск непреднамеренного раскрытия информации. Утверждения токена могут содержать информацию о местоположении партнёра или критически важные бизнес-данные. В состав утверждений также может входить определение уровня доверия (**trust_level**) компании, открывающей API, к партнёру. Может выйти конфуз, если партнёр вдруг увидит в этом поле значение **low**.

Как скрыть информацию в этом случае? Очевидное решение зашифровать содержимое токена доступа может сработать, однако несёт в себе немало минусов:

- ◆ шифрование и дешифрование — затратный процесс, значительно увеличивающий потребление ресурсов;
- ◆ размер зашифрованного токена в два с лишним раза превышает размер незашифрованного; более того, предъявлять токен нужно при каждом запросе API, чтократно увеличивает объём сетевого трафика;
- ◆ шифрование должно выполняться ключом сервиса, получающего запрос,

но стандарта обмена подобными ключами не существует;

◆ сервер авторизации не сможет расшифровать токен доступа, выпущенный для сервиса. Поэтому механизмы отзыва токена (**revocation endpoint**) и проверки содержимого и актуальности токена доступа (**introspection endpoint**) затруднены или невозможны.

Иными словами, шифрование токена превращает меры информационной безопасности в трудоёмкое и дорогостоящее для бизнеса предприятие. eKassir Identity Platform предлагает решить проблемы другим, лишённым перечисленных недостатков, способом (рис. 5).

В этом случае токен доступа возвращается партнёру в формате **reference** — уникального набора символов, не несущего смысловой нагрузки. Партнёр не получит от него авторизационной информации.

Здесь в дело вступает второй компонент Identity Platform — **Identity Gateway**, сервисное приложение для организации единой точки входа. Оно поддерживает функцию реверсивного установления соединений, при которой один Identity Gateway установлен в DMZ, а второй — во внутреннем сегменте сети, и установление соединения инициируется из внутреннего сегмента в DMZ.

Identity Gateway перехватит запрос от партнёра к API и заменит **reference**-токен доступа на полноценный, содержащий утверждения и цифровую

JWT-подпись (**JSON Web Token**). Получив полноценный токен, сервис успешно выполнит авторизацию.

Результат защиты API партнёра. В описанной выше ситуации API оказывается защищён от внутренних и внешних угроз, а также устранена опасность, связанная с возможной кражей токена доступа.

Поскольку токен доступа хранится только в Access Manager (сервер авторизации), не нужно думать о его безопасном хранении. Identity Gateway перехватывает **reference**-токен, обращается к Access Manager и получает токен доступа в формате JWT. Далее он обогащает запрос и отправляет этот токен на сервис.

Такая архитектура решения не позволяет токенам доступа JWT покидать инфраструктуру компании: партнёр получает набор символов, которые не раскрывают никакой информации.

Благодаря применению **reference**-токена не только устраняется проблема с непреднамеренным раскрытием информации, но и сетевой трафик к API заметно сокращается.

API ДЛЯ ПОЛЬЗОВАТЕЛЕЙ

В отличие от партнёров, никакими ИТ-компетенциями пользователи не обладают и потому не способны обеспечить безопасное хранение токенов доступа. Многие фреймворки предлагают свести риски, связанные с хранением токенов на пользовательских устройствах, к минимуму. Это не слишком

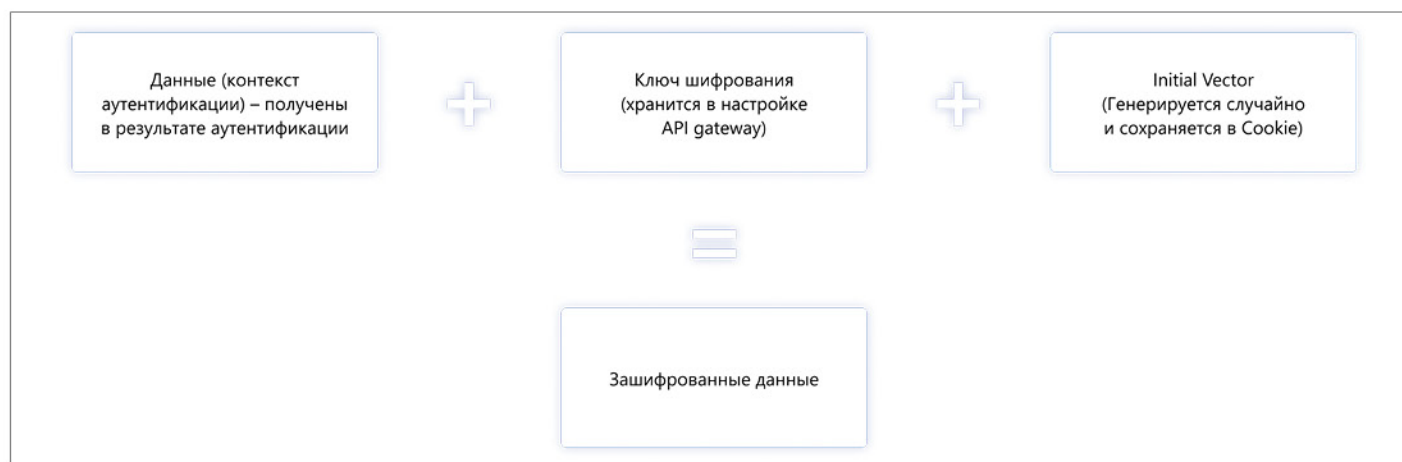


Рисунок 6. Чтобы успешно дешифровать токен, требуется два ключа, один из которых находится у Identity Platform, другой (Initial Vector) — в сессионной cookie

безопасно, ведь токены будут передаваться на фронтальные устройства, которые могут работать в недоверенной среде исполнения.

Мы предлагаем решить эту проблему иначе: вообще не передавать токены доступа на устройства пользователей. Вместо этого хранение токенов будет обеспечивать сервисный компонент комплекса Identity Platform — Identity Gateway.

Выглядит это так. Identity Gateway открыто перехватывает неавторизованный запрос пользователя и направляет его в Access Manager, где пользователь проходит аутентификацию. Далее Identity Gateway самостоятельно, без участия браузера или мобильного приложения пользователя, получает токен доступа и сохраняет его в базе данных NoSQL. Вместо токена на пользовательское устройство отправляется безопасная сессионная cookie.

Всякий раз, когда с устройства передается запрос, к нему добавляется сессионная cookie. Identity Gateway её получает, извлекает токен доступа из хранилища и добавляет к запросу. Таким образом, Identity Platform не отдаёт сам токен из защищённого контура, а замещает и отправляет вместо него на устройство пользователя «артефакт» — сессионную cookie.

Таким образом, сервисы и API не получают информацию о логине и пароле пользователя — он вводит их только на стороне Identity Platform. Сервис не владеет, не знает и не хранит credentials пользователя, что существенно снижает риск компрометации учётных

данных. С другой стороны, токен доступа не покидает ИТ-инфраструктуру и пользователь его никогда не получает.

БЕЗОПАСНОЕ ХРАНЕНИЕ ТОКЕНА ДОСТУПА

Токен доступа относится к чувствительной информации — критически важно обеспечить его безопасность. В Identity Platform перед записью токена в базу данных применяется шифрование по алгоритмам с обязательным использованием Initial Vector. Чтобы успешно дешифровать токен, требуется два ключа, один из которых находится у Identity Platform, другой (Initial Vector) — в сессионной cookie. Можно сравнить это с доступом в хранилище банковского депозитария, дверь в который открывается двумя ключами — работника депозитария и сотрудника охраны банка (рис. 6).

При таком подходе зашифрованные данные бесполезны для злоумышленника, даже если он получит в распоряжение диски с базой данных, ведь для расшифровки нужен Initial Vector — а тот есть лишь в сессионной cookie у пользователя.

ЗАКЛЮЧЕНИЕ

На первый взгляд может показаться, что построение системы защиты для безопасной и эффективной работы API — крайне трудоёмкая задача, целесообразность реализации которой зависит от ресурсов и компетенций компании. В самом деле, пошаговая работа над конфигурированием аутентификационного сервера, допустимое

шифрование токенов доступа и обеспечение безопасности инфраструктуры PKI выглядит длительным монструозным процессом, на каждом этапе которого разработчики обязательно столкнутся с проблемами.

Их эффективным решением может быть использование программного решения «коробочного» формата, который не нужно дорабатывать. В практике нашей компании таким решением стал комплекс eKassir Identity Platform. Выполняющий роль сервера авторизации Access Manager аутентифицирует клиентов и партнёров, выпускает токены доступа, а Identity Gateway обеспечивает защиту API. Интеграция «фронта» не требует ни единой строчки кода, а «бэк» внедряется минимальными усилиями, о чём мы подробно рассказали выше.

Предложенный нами способ решения задачи не является единственным, однако на практике мы убедились, что он вполне реализуем и надёжен. В частности, Identity Platform был использован при внедрении системы аутентификации для организации безопасного доступа клиентов к финансовым услугам «Открытия Инвестиции».

На первом этапе мы реализовали безопасное обращение сторонних маркетплейсов к сервисам компании по API. На втором этапе планируется подключить конечных пользователей к созданной системе, что обеспечит им бесшовную регистрацию в сервисах «Открытия Инвестиции» и подключение финансовых услуг по защищённым каналам.



Денис БАТРАНКОВ
член редколлегии BIS Journal

ЧТО МЕНЯЕТСЯ ВО ФРЕЙМАХ ETHERNET

ПРИ ПЕРЕДАЧЕ ИНФОРМАЦИИ ОТ КЛИЕНТА СЕРВЕРУ?

Вопрос из заголовка порой вводит в тупик даже коллег, имеющих сертификаты уровня CCNA. Давайте рассмотрим, как выглядят фреймы (кадры) на каждом этапе передачи от клиента коммутатору, роутеру, межсетевому экрану и серверу и какие поля при этом в них меняются.

Буду исходить из того, что читатель знаком с базовым курсом TCP/IP, и касаться только нужных для статьи моментов.

ПРОВЕДЁМ ЭКСПЕРИМЕНТ

Давайте подключимся от клиента к серверу и посмотрим на IP- и MAC-адреса источника и получателя во всех фреймах в каждом канале (рис. 1). Самый простой способ увидеть это самим — подключить в каждый канал сниффер.

Клиент с IP-адресом 10.1.1.11/24 и MAC-адресом 0000.0001.1111 подключается к серверу с IP-адресом 10.1.3.33/24 и MAC-адресом 0000.0008.8888. Маска /24 (255.255.255.0) выбрана для примера.

СТРУКТУРА ФРЕЙМОВ ETHERNET ПРИ ПЕРЕДАЧЕ ПО СЕТИ

Напомню, как выглядит структура фрейма (кадра) Ethernet при передаче в сеть: все заголовки и данные вышестоящих протоколов стека TCP/IP объединяются в единый блок данных для передачи. Ваши файлы, голос

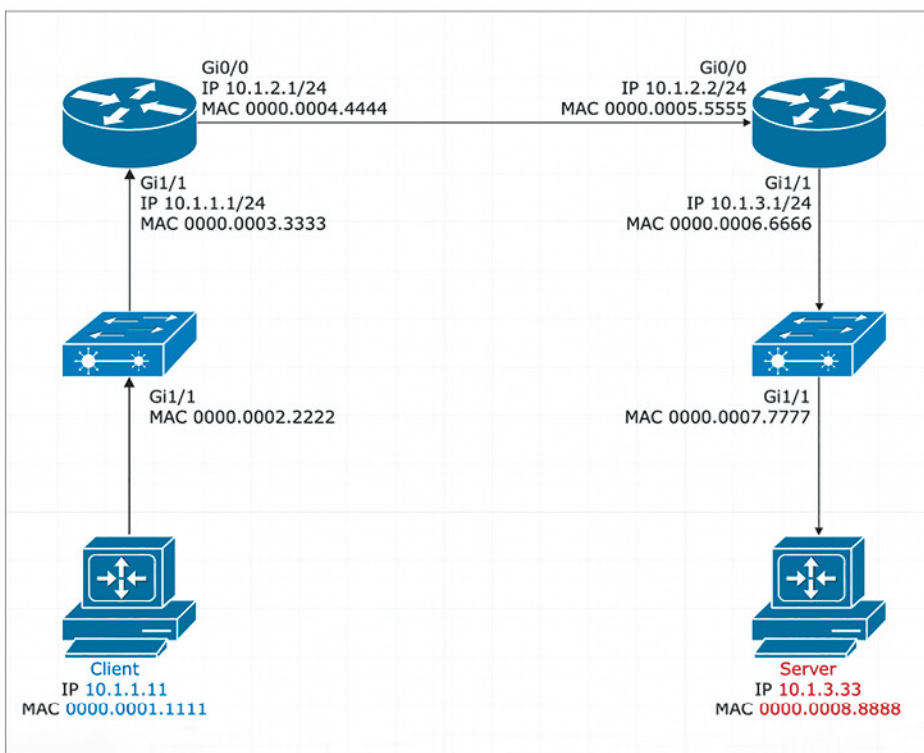


Рисунок 1. Схема подключения клиента к серверу через промежуточное оборудование

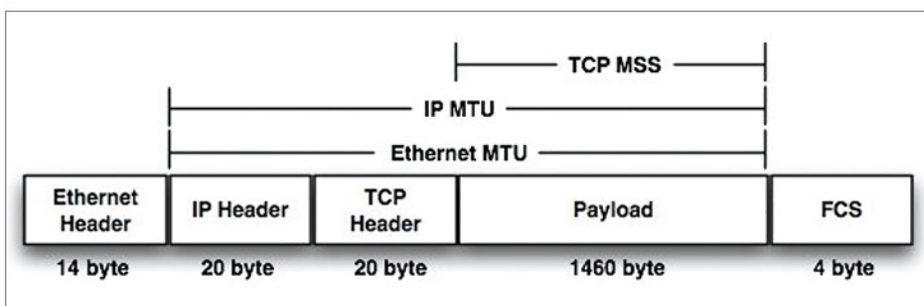


Рисунок 2. Пример фрейма (кадра) Ethernet. MTU — максимальный размер фрейма для данной среды передачи. Обычно 1500 байт. TCP MSS — максимальный размер сегмента данных TCP. Обычно MSS = MTU - 40 = 1460 В сумме длина фрейма 1518 байт.



Рисунок 3. Демонстрация, как производится пересылка фрейма через коммутатор

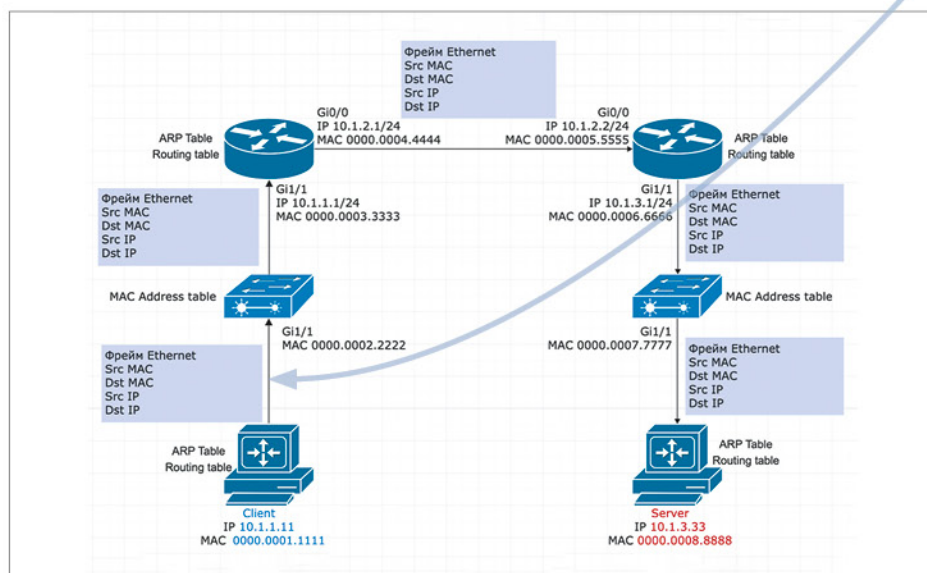


Рисунок 4. Итак, какими будут Source IP и Source MAC, Destination IP и Destination MAC в первом кадре от клиентского компьютера?

и видео в виде нарезанных кусочков перемещаются в поле Payload. Внутри Ethernet-заголовка находятся MAC-адреса источника и получателя, и внутри IP-заголовка находятся IP-адреса источника и получателя. Эта структура данных в наших сетях используется коммутаторами и маршрутизаторами для передачи фреймов друг другу. Например, на рис. 2 внутри фрейма отображены заголовки IP-протокола 4-й версии и TCP-протокола (могут

быть помещены и другие протоколы, например ICMP или UDP)

Изучим первый фрейм между клиентом и коммутатором. Итак, какими будут Source IP и Source MAC, Destination IP и Destination MAC в первом кадре от клиентского компьютера (рис. 4)? Попробуйте написать эти адреса во фреймах сами: просмотрите названия полей заголовков на рисунке 4, запишите ваши ответы и только затем читайте дальше. Проверьте себя.

Будем исходить из того, что клиент и сервер уже передавали друг другу данные и поэтому все нужные ARP-таблицы и таблицы маршрутизации настроены на всём пути от клиента к серверу. У клиента маршрутизатором по умолчанию является 10.1.1.1/24. Соответственно, MAC-адрес у этого IP-адреса уже был запрошен в одном из ранее отправленных ARP-запросов и в ARP-таблице клиента есть информация о MAC-адресе для IP-адреса 10.1.1.1.

Заполняем первый фрейм данными IP- и MAC-адресов (рис. 5):

Фрейм Ethernet

Src MAC

Dst MAC

Src IP 10.1.1.11

Dst IP 10.1.3.33

Рисунок 5. Фрейм от клиента: Src MAC — MAC-адрес отправителя; Dst MAC — MAC-адрес получателя; Src IP — IP-адрес отправителя; Dst IP — IP-адрес получателя

Полагаю, что вы понимаете, какие во фрейме от клиента будут IP-адреса источника и получателя, ведь они даны в условии задачи: мы хотим отправить данные с IP-адреса 10.1.1.11 на IP-адрес 10.1.3.33. Поэтому эти адреса вписываем в IP-заголовок.

Я встречал студентов, которые вписывали в поле с IP-адресом получателя IP-адрес следующего маршрутизатора (в примере — 10.1.1.1): это ошибка. Всегда во фреймах при движении по сетям в поле IP-заголовка будут только IP-адреса источника и получателя. Если вы отправите другой адрес, то маршрутизатору будет недоступен настоящий адрес получателя и в таблице маршрутизации не будет информации о том, куда направлять пакеты. Если вы напишете другой IP-адрес источника, то маршрутизатор не определит, куда возвращать ошибки доставки пакетов. При этом IP-адреса во фреймах могут меняться, если по пути движения кадров появится устройство с включённым Source NAT или Destination NAT. Но в нашей задаче такое устройство, выполняющее трансляцию адресов, не указано.

Кроме того, легко понять, каким будет MAC-адрес отправителя: это MAC-адрес клиента — 0000.0001.1111.

КАКОЙ MAC-АДРЕС ПОЛУЧАТЕЛЯ НАПИСАТЬ

Поскольку это самая важная часть текста, я выделил её в отдельную главу.

Какой MAC-адрес получателя написать во фрейме, исходящем с интерфейса Client? Иногда люди думают, что им будет MAC-адрес сервера, а именно 0000.00008.8888. Если вы создадите такой фрейм и отправите его с интерфейса компьютера клиента в сторону свитча, то кадр реально попадёт в широковещательный домен, доступный через коммутатор (в левой части рис. 6). Коммутатор получит этот фрейм, проверит по своей таблице MAC-адресов, что такого адреса в ней нет, и отправит кадр сразу на все свои порты. В итоге он дойдёт до роутера (в левой части картинки сверху), на котором MAC-адрес другой (0000.0003.3333), и роутер просто отбросит этот фрейм, потому что он пришёл не по адресу. Такой кадр просто не достигнет сервера.

MAC-адресом получателя также не может быть MAC-адрес свитча. Когда свитч получит фрейм, то определит, что кадр отправлен именно ему, и, скорее всего, просто «убьёт» его (зависит от производителя устройства), ведь фрейм уже дошёл и непонятно, что с ним делать. И ещё мне интересно: как вы на компьютере Client узнаете MAC-адрес коммутатора? Ведь устройство никаким образом не сообщает его подключённым клиентам.

ПРАВИЛЬНЫЙ ОТВЕТ

Нужно указывать MAC-адрес роутера, который является вашим маршрутизатором по умолчанию. IP-адрес маршрутизатора задаётся в таблице маршрутизации при настройке компьютера или может быть получен от DHCP-сервера. С компьютера Client заранее сделан ARP-запрос, благодаря которому мы узнаем MAC-адрес, соответствующий IP-адресу роутера. Именно его и надо подставлять в поле Destination MAC address.

Фрейм Ethernet
Src MAC 0000.0001.1111
Dst MAC 0000.0003.3333
Src IP 10.1.1.11
Dst IP 10.1.3.33

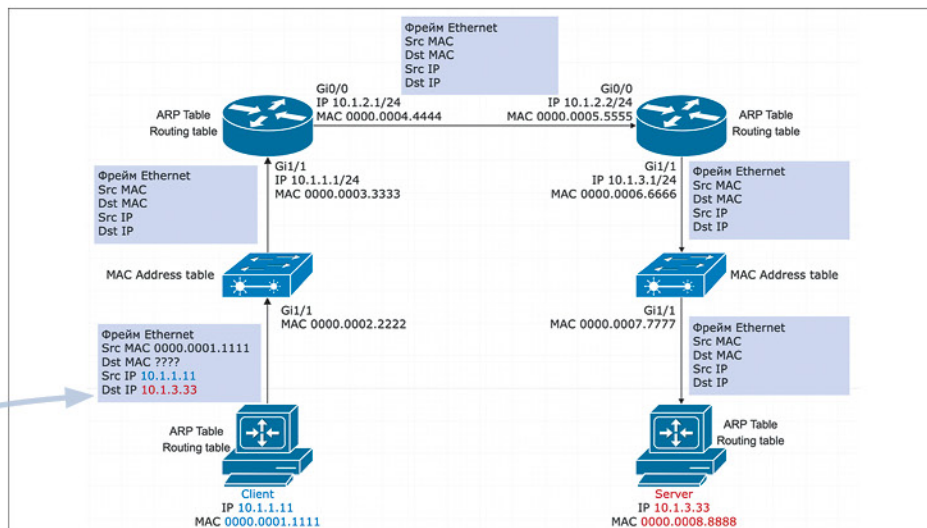


Рисунок 6

В результате этот фрейм от клиента попадает на свитч. Ключевым здесь является то, что коммутатор не меняет ни MAC-адреса, ни IP-адреса. При этом свитч хранит таблицу с описанием того, на каком интерфейсе какие MAC-адреса подключены, и определяет интерфейс, на котором находится нужный нам следующий маршрутизатор 0000.0003.3333. От коммутатора фрейм отправляется на маршрутизатор (неизменённым), где благополучно принимается, ведь получатель указал правильный MAC-адрес.

Я специально нарисовал на схеме коммутатор, потому что хотел сообщить читателям важную информацию: ни MAC-адреса, ни IP-адреса в заголовках фреймов на свитчах не меняются. Кроме того, важно заметить, что адрес коммутатора не надо указывать в поле Destination MAC address.

Иногда студенты спрашивают: почему на картинке не указан MAC-адрес интерфейса верхнего коммутатора слева? И вы уже знаете ответ: потому что это неважно. В поле Source MAC address будет указан MAC-адрес интерфейса клиентского компьютера, а не интерфейса коммутатора: коммутатор не меняет ни Destination MAC address, ни Source MAC address в заголовках фреймов. Три раза повторил, да?:)

РЕШЕНИЕ ЗАДАЧИ

Окончательная картинка будет выглядеть следующим образом: IP-адреса в заголовке внутри фрейма всегда

одинаковые, а вот MAC-адреса меняются на MAC-адреса всех интерфейсов, имеющих IP-адрес. Именно так работает сеть на основе Ethernet. По пути между маршрутизаторами могут быть и другие порты: серийные, frame relay, АТМ. Нужно понимать, что MAC-адрес применим только к протоколу Ethernet. Протоколы канального уровня используют разные схемы адресации: например, frame relay использует номер DLCI, а протокол АТМ — VPI или VCI. Сегодня мы говорим только про Ethernet.

В настоящей сети вы можете посмотреть все фреймы сниффером, подключившись к SPAN-порту любого из устройств, или воспользоваться TAP-устройствами или даже сетевыми брокерами (рис. 7). Если это виртуализация, то используйте vTAP или vBroker.

ЧТО БУДЕТ, ЕСЛИ Я ДОБАВЛЮ В ЭТУ СЕТЬ NGFW?

Давайте поместим в схему NGFW, который защищает подключения от клиентов к серверу. Нужно понимать, что NGFW будет являться маршрутизатором для сети. На его интерфейсах есть IP-адреса и MAC-адреса, и тогда схема прохождения фреймов аналогична схеме с роутером (рис. 8).

Меня озадачивают запросы на проверку MAC-адресов с помощью NGFW. Внимательно посмотрите на картинку: на NGFW видны только MAC-адреса ближайших роутеров. Вы никогда не сможете получить фрейм с настоящим MAC-адресом клиента или

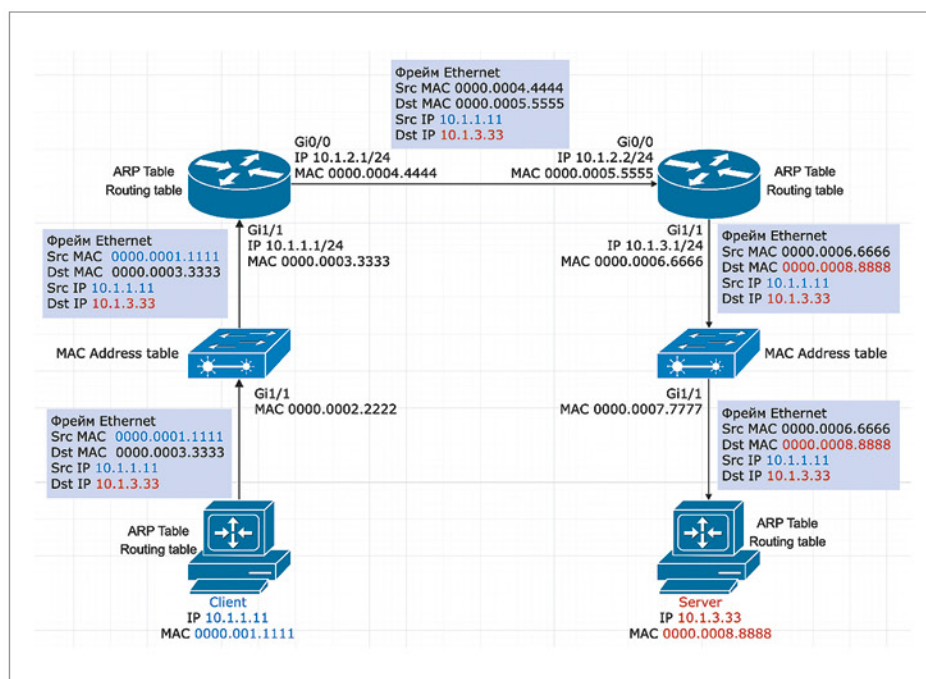


Рисунок 7. Схема передачи фреймов по сети от клиента серверу. Синим помечены адреса клиента, красным — адреса сервера

Рисунок 8. Схема передачи фреймов в сети с NGFW с включённой маршрутизацией

Рисунок 9. Схема передачи фреймов в сети с межсетевым экраном L2 (прозрачным для L3)

сервера. Проверки по MAC-адресам сделать можно, но в поле будет либо ану, либо MAC-адрес вашего роутера или роутера провайдера.

А ЧТО, ЕСЛИ Я ХОЧУ ФИЛЬТРУЮЩИЙ МОСТ?

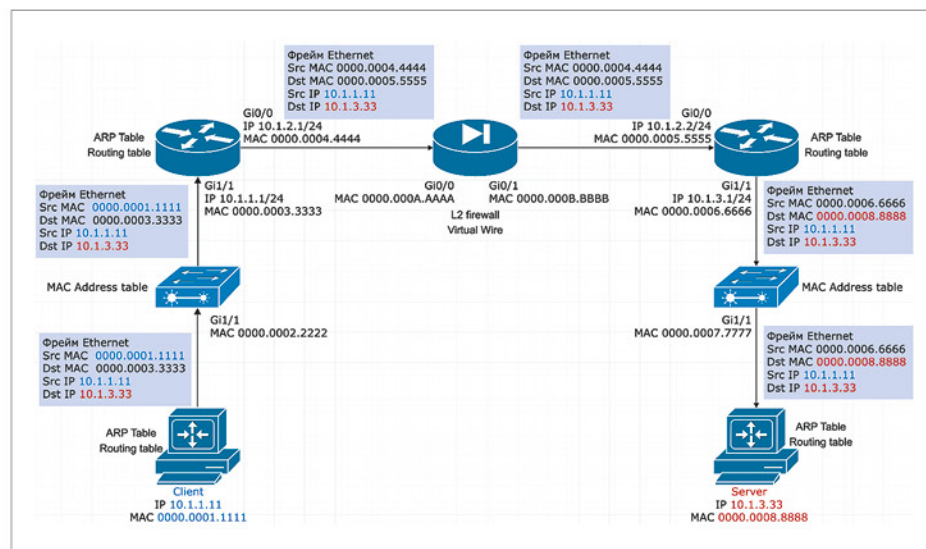
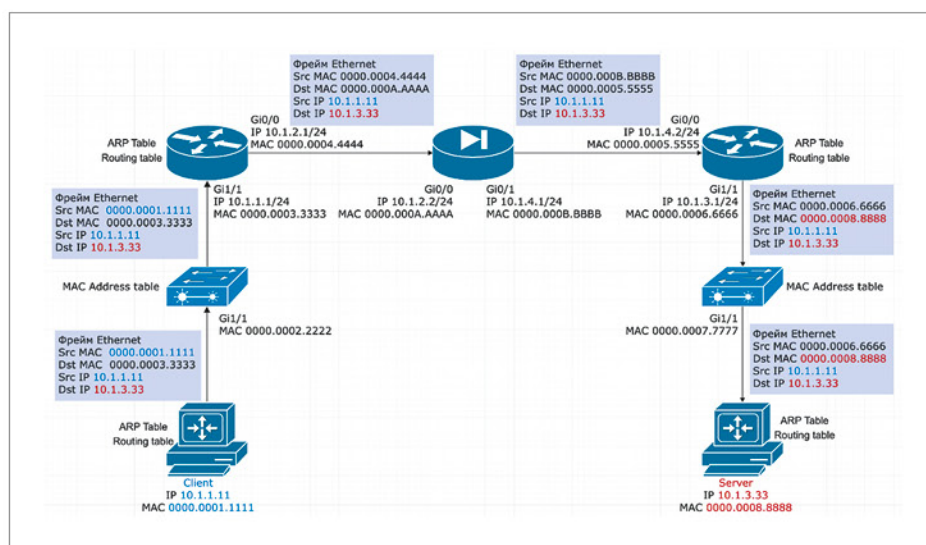
Если изменить картинку выше и подключить NGFW не как роутер (устройство layer 3), а как коммутатор (устройство layer 2) или как виртуальную линию (устройство layer 1), то NGFW на самом деле будет фильтрующим мостом согласно типовой классификации межсетевых экранов. И мы всё равно понимаем, что фильтровать можно будет только устройства, которые подключены к NGFW или напрямую, или через коммутатор. Такое, в принципе, бывает в SCADA-сетях, но в интернете все устройства L3, и по MAC-адресам их фильтровать не получится. В сети SCADA логичнее сделать VLAN insertion, разделить один broadcast domain на несколько разных VLAN и заменить теги VLAN на самом NGFW (рис. 9).

ЗАКЛЮЧЕНИЕ. ВЫВОДЫ

Мне бы хотелось, чтобы теперь все знали, что:

- ◆ при перемещении IP-пакетов по сети MAC-адреса коммутаторов не подставляются во фреймы Ethernet;
- ◆ при перемещении IP-пакетов по сети каждый маршрутизатор подставляет свои MAC-адреса, и наши снифферы или анализаторы трафика (например, системы NTA) определяют MAC-адрес ближайшего маршрутизатора, а не реального узла;
- ◆ нет смысла в фильтрации по MAC-адресам. Она нужна только для одной локальной сети или одного широковещательного домена.

Ещё будут меняться поле TTL и контрольные суммы, но это нужно обсуждать отдельно.





Ideco UTM

Комплексное решение
для защиты вашей сети.

- ✓ Межсетевой экран
- ✓ Центральная консоль
- ✓ Контентная фильтрация
- ✓ Контроль приложений
- ✓ Почтовый сервер

Заказать:

8 800 555 33 40 | sales@ideco.ru

АНАТОМИЯ НЕВОЗМОЖНОГО

ПОЧЕМУ ИИ НЕ СМОЖЕТ ЗАЩИТИТЬ ОТ АТАК НА ЛЮДЕЙ



Андрей ЖАРКЕВИЧ
эксперт
ООО «Антифишинг»

ИИ становятся всё более человечными. Они с лёгкостью проходят тест Тьюринга, пишут музыку и статьи, рисуют картины и создают программы, которые компилируются и работают, выполняя сформулированное на обычном языке ТЗ. На этом фоне вполне логичным кажется вывод, что совсем скоро могучий искусственный разум доберётся до ИБ и полностью решит проблему человеческого фактора.

Это может выглядеть, например, как объединение мировых нейросетей и непрерывного обучения на озёрах данных об атаках, которые собирают антивирусные компании. Получившийся суперИИ будет знать всё возможное и невозможное о любых действиях киберпреступников, поэтому обнаружит и заблокирует любые попытки фишинга и других видов атак на людей. Сотрудники компаний и обычные граждане смогут вести безмятежное существование под непробиваемой защитой заботливого и всеведущего наставника.

К сожалению, все эти мечты разбиваются о суровую реальность. ИИ не сможет защитить людей от цифровых атак (фишинг, вишинг, ВЕС, вредоносное ПО и другие), пока человек может выполнять потенциально опасные действия. Разберёмся, почему так происходит.

ЗАЩИТА ОТ ФИШИНГА

Сочетание низкой стоимости реализации атак с высокой эффективностью делает фишинг идеальным инструментом для киберпреступников. По данным отчёта Proofpoint, в 2021 году 83% организаций подверглись успешной фишинговой атаке, 78% столкнулись с атаками вымогателей, которые начались с фишингового письма, 86% стали жертвами массовых фишинговых рассылок, а 77% подверглись атакам с компрометацией деловой переписки. Поэтому создание надёжной защиты от фишинга — приоритетное направление для всех разработчиков систем информационной безопасности.

На что надеются

Люди научились распознавать примитивные фишинговые атаки в виде электронных писем,

текстов и QR-кодов. Грамматические ошибки, опечатки, подозрительные ссылки, поддельные логотипы и адреса электронной почты, не соответствующие отправителю, позволяют легко вычислить фальшивку.

Но мошенники тоже развиваются, поэтому они изменили тактику. Фишинговые письма нового поколения написаны и оформлены без явных ошибок, их отправители обращаются к жертвам по имени-отчеству и могут даже включать для достоверности один из реальных паролей, полученный из утечек. Всё это значительно усложняет распознавание вредоносных писем человеком.

И тут в дело вступает ИИ в составе защитных решений. Обученные на базе огромного массива фишинговых посланий нейросети успешно распознают мошеннические письма, обманувшие людей. Лучшие из них выделяют в потоке внешне легитимных и совершенно безвредных писем опаснейшие ВЕС-сообщения. Казалось бы, вот он, философский камень. Но не стоит забывать, что ИИ и нейросети могут использовать не только защитники.

Почему это не работает

Отличную демонстрацию возможностей современных нейросетей провела команда Сингапурского ИБ-агентства на конференции Black Hat и Defcon в 2021 году. Они разослали своим коллегам целевые фишинговые письма, часть которых написали сами, а часть сгенерировали с помощью платформы ИИ-как-услуга. Оба сообщения содержали ссылки, которые уведомляли исследователей о количестве переходов. Они с удивлением обнаружили, что по ссылкам в сообщениях, сгенерированных ИИ, переходило больше людей, чем в сообщениях, написанных человеком, причём со значительным отрывом.

Для генерации посланий исследователи воспользовались платформой OpenAI GPT-3 и ещё несколькими ИИ-сервисами, ориентированными на анализ личности (OSINT). Это позволило им создавать фишинговые письма с учётом биографии и особенностей характера адресатов. Пропустив полученные данные через



несколько сервисов, исследователи смогли разработать конвейер, который подготавливал и совершенствовал электронные письма перед рассылкой. По их словам, результаты звучали «странно по-человечески», а ИИ вносили в письма неожиданные уточнения, например, упоминание Сингапурского закона при создании текста для жителей Сингапура.

А теперь давайте представим, что нейросеть для генерации фишинговых писем обучили не просто делать качественные послания, на которые реагируют люди, а ещё и писать их так, что ИИ защитных решений тоже будут признавать их безвредными. Звучит невероятно, особенно если к этому добавить «фишинг под ключ» — создание набора скриптов, которые будут размещать фишинговые сайты на уязвимых хранилищах AWS, настраивать файрвол,

регистрировать домены, рассылать сгенерированные письма и в конце выдавать отчёт.

Но всё это — результат реального эксперимента с нейросетью ChatGPT, описанный в запрещённой на территории РФ соцсети Илона Маска. Оказалось, что достаточно всего лишь обратиться к ChatGPT с просьбой типа «create a python script to deploy evilgenx phishing tool to AWS» или «create a python script to register domain twitter-security-update.com with godaddy», чтобы получить на выходе полностью работоспособные python-программы.

Получается, что нападающие уже располагают инструментарием для организации и проведения масштабных фишинговых кампаний, причём благодаря тщательно обученным нейросетям они могут создавать более «человечные» письма, чем реальные люди. И самое

Секрет эффективности фишинга состоит в том, что не имеет значения, сколько тысяч фишинговых сообщений успешно распознала жертва или заблокировал ИИ-защитник. Для взлома сети достаточно пропустить всего одно

важное — эти письма будут признаваться безопасными даже лучшими системами защиты.

Налицо классическая проблема противостояния брони и снаряда. Только сейчас мы наблюдаем разбаланс: атакующие комплексы ушли далеко вперёд и вероятность того, что отставание защиты удастся быстро ликвидировать, не слишком велика.

Секрет эффективности фишинга состоит в том, что не имеет значения, сколько тысяч фишинговых сообщений успешно распознала жертва или заблокировал ИИ-защитник. Для взлома сети достаточно пропустить всего одно. И неважно, кто ошибётся, человек или ИИ.

ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО

Эвристический и поведенческий анализ присутствует в антивирусах и их более продвинутых наследниках (EDR, XDR) уже много лет. Разумеется, производители антивирусных программ рассматривают машинное обучение в качестве инструмента для улучшения методов обнаружения вредоносного ПО благодаря его способности выявлять новые типы вредоносного ПО, не встречавшиеся ранее.

На что надеются

Сегодня команды безопасности завалены данными о потенциально подозрительной активности в сетях и на периметре. Это приводит к тому, что для поиска реальной угрозы приходится буквально искать маковые зёрна на пшеничном элеваторе. ИИ помогает защитникам находить реальные угрозы, распознавая модели сетевого трафика, индикаторы вредоносного ПО и тенденции поведения пользователей.

ИИ используется для более точного обнаружения атак и последующего определения приоритетности ответных мер на основе реального риска. Он позволяет автоматически реагировать на атаки и обеспечивает более точное моделирование для прогнозирования будущих инцидентов. Всё это не обязательно устраняет аналитиков из цикла, но делает их работу более гибкой и точной. При столкновении с киберугрозами они могут сосредоточиться на важном, а не фильтровать тонны шума.

Почему это не работает

На конференции по безопасности Black Hat USA в 2017 году исследователи представили AVPASS — инструмент, который распознаёт цепочки правил обнаружения любого антивирусного механизма. Затем это умозаключение используется для маскировки вредоносного ПО под доброкачественное Android-приложение. AVPASS показал нулевой уровень обнаружения на онлайн-сервисе анализа вредоносного ПО VirusTotal с более чем 5 тыс. образцов вредоносного ПО для Android. Другими словами, AVPASS создал оперативно необнаруживаемое вредоносное ПО.

Было доказано, что системы обнаружения на основе машинного обучения могут быть обмануты агентом ИИ, предназначенным для поиска слабых мест. Исследователи, например, смогли создать вредоносное ПО, которое не обнаруживают даже антивирусные системы на основе машинного обучения. Такие вредоносы используют обучение с подкреплением, соревнуясь с антивирусным детектором. Они выбирают функции, сохраняющие вредоносность исполняемого файла Windows, и добавляют варианты, которые повышают шансы на то, что образец вредоносного ПО пройдёт незамеченным.

Вот какие способы используют злоумышленники, чтобы обойти ИИ систем защиты.

Проверка эффективности своих вредоносных программ против инструментов на основе ИИ с помощью машинного обучения. Для этого они создают собственные среды, где моделируют вредоносные программы и методы атак для определения типов событий и поведения, которые ищут защитники.

Например, сложная часть вредоносного ПО может изменять локальные системные библиотеки и компоненты, запускать процессы в памяти и взаимодействовать с одним или несколькими доменами, принадлежащими инфраструктуре управления злоумышленника. Все эти действия в совокупности создают профиль, известный как тактика, техника и процедуры (ТТП). Модели машинного обучения могут наблюдать за ТТП и использовать их для создания возможностей обнаружения.

Наблюдая и прогнозируя, как ТТП обнаруживаются командами безопасности, атакующие могут тонко и часто изменять индикаторы и поведение, чтобы опередить защитников, которые полагаются на инструменты ИИ для обнаружения атак.

Отравление ИИ неточными данными. Злоумышленники используют машинное обучение и ИИ для компрометации защиты пу-

тём отравления моделей неточными данными. Модели машинного обучения и ИИ полагаются на правильно маркированные образцы данных для построения точных и воспроизводимых профилей обнаружения. Внедряя доброкачественные файлы, похожие на вредоносное ПО, или создавая модели поведения, которые оказываются ложноположительными, злоумышленники могут обмануть модели ИИ, заставив их поверить, что поведение при атаке не является вредоносным. Злоумышленники также могут отравить модели ИИ, внедряя вредоносные файлы, которые в ходе обучения ИИ были признаны безопасными.

Сопоставление существующих моделей ИИ. Злоумышленники составляют карту существующих и разрабатываемых моделей ИИ, которые используют поставщики услуг кибербезопасности и операционные команды. Выяснив, как функционируют модели ИИ и что они делают, злоумышленники могут активно нарушать работу систем машинного обучения и моделей во время их циклов. Это может позволить хакерам влиять на модель, обманывая систему в пользу злоумышленников и их тактик. Это также может позволить хакерам полностью обойти известные модели, тонко изменяя данные, чтобы избежать обнаружения на основе распознанных закономерностей.

Таким образом, в арсенале киберпреступников имеются все инструменты, чтобы обойти защитные системы и добиться, чтобы они позволили сотрудникам компаний выполнить целевое действие — перейти по фишинговой ссылке, открыть вредоносное вложение, установить поддельное «обновление». Защитные решения снова оказываются не у дел, создавая ложное чувство защищённости.

ЗАЩИТА ОТ ТЕЛЕФОННЫХ МОШЕННИКОВ

Телефонные мошенники стали угрозой номер один для клиентов банка. Множественные утечки из различных сервисов объединяются в один большой массив, сопоставляются с данными социальных сетей, а затем с помощью ИИ производится профилирование жертв и их сортировка по различным критериям.

На что надеются

Банки обучают свои антифрод-системы на базе ИИ выявлять и блокировать переводы денег мошенникам. Но пока серьёзных успехов в этой области незаметно. Различные меры, предлагаемые ЦБ и другими ведомствами, показывают лишь частичную эффективность. Например, блокировка телефонных номеров привела к

тому, что мошенники стали подставлять номера реальных людей или вообще звонить через WhatsApp и другие мессенджеры.

Почему это не работает

Мошенники уже используют ИИ для автоматизации и быстрого обнаружения того, как жертвы поддаются на аферу или отказываются от участия. Это позволит ему сосредоточиться только на тех потенциальных жертвах, которых легко обмануть. Какой бы ложный предлог ни выбрал мошенник, чтобы убедить жертву принять участие, нейросеть сможет предугадать наиболее распространённые ответы жертвы.

В ходе автоматизированных диалогов преступники могут отслеживать, какие аргументы и логика наиболее убедительны для потенциальных жертв. Изменяя эти параметры, они могут усовершенствовать аферу, чтобы со временем добиться лучших результатов. Собрав достаточное количество данных, злоумышленники могут использовать их как характеристики для обучения всё более совершенных моделей, которые сделают атаки более эффективными.

ВЫВОДЫ

ИИ по своей сути является технологией двойного назначения. Помимо прочего, это означает, что с помощью ИИ можно как защищать людей от цифровых атак, так и проводить мошеннические кампании с использованием социальной инженерии.

По состоянию на сегодняшний день возможности ИИ для организации цифровых атак значительно выше, чем у доступных на рынке систем защиты на базе ИИ. Нейросети помогают преступникам увеличить масштабы применения социальной инженерии, автоматизируя первые шаги атаки за счёт автоматической генерации контента с помощью нейросетей GPT-3, улучшая сбор бизнес-аналитики, ускоряя обнаружение потенциальных жертв и проведение атак на нарушение бизнес-процессов.

Поскольку системы защиты всё чаще используют подходы на основе ИИ, ожидается, что преступники будут либо напрямую атаковать эти системы, либо использовать ИИ для имитации поведения пользователей. Растущая автоматизация многочисленных аспектов повседневной жизни с помощью систем на базе ИИ также неизбежно влечёт за собой возможную потерю контроля над этими аспектами. Это не только расширит поверхность для киберударов, но и создаст новые типы атак на людей и компьютерные системы.

Мы постоянно слышим со всех сторон, что сложность задач в информационной безопасности растёт, квалифицированных специалистов катастрофически не хватает, профессиональная подготовка отстаёт от требований и т.д. и т.п. Можно много анализировать причины, ссылаться на стандарты образования, жаловаться на что-то весьма непреодолимое.

А можно вот так.

Не помышляя о чуде, просто создать сервис, который позволяет получать актуальные профессиональные знания, практические навыки на основе непосредственной работы на самых современных средствах защиты информации в условиях практически неотличимых от реальных инцидентов информационной безопасности. Причём

практический навык можно тренировать до мышечного автоматизма, чтобы оставлять время и возможности работать головой.

Равная возможность для всех получать профессиональные, постоянно актуализируемые знания и практические навыки в любое удобное время и из любой точки страны, лишь бы был интернет.

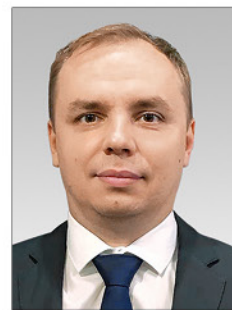
Я сам попробовал, я думал, что меня трудно удивить чем-то из области информационной безопасности, но, похоже, я не всё видел и не всё знаю, я не смог сдать тесты после обучения с первого раза.

Что зря говорить — читайте сами.

Василий Окулесский, член редколлегии BIS Journal

ДЕЛО ЗА МАЛЫМ: НАЙТИ СИСТЕМУ ВИРТУАЛИЗАЦИИ

ЭФФЕКТЫ ПАНДЕМИИ, ИЛИ КАК МЫ ПЕРЕШЛИ НА ДИСТАНЦИОННОЕ ОБУЧЕНИЕ



Андрей ЗАРУБИН
вице-президент
по науке
и образованию,
сооснователь
Академии ИнфоВотч

Тема дистанционного обучения набирает обороты уже последние лет семь, но в годы пандемии её актуальность оказалась настолько высокой, что откладывать переход на новый формат работы было нельзя.

КАК БЫЛО

В «допандемийный» период дистанционное обучение специалистов заказчиков и партнёров в «ИнфоВотч» проводилось в так называемом синхронном

формате. Одновременно для всех участников запускался вебинар, где тренер вещал подготовленный материал, проводил демонстрации и завершал занятия аттестационными мероприятиями. Такой формат, безусловно, имеет право на существование, но, как показала практика, он не очень удобен для региональных заказчиков из-за серьёзной разницы во времени. Кроме того, телеметрия вебинаров показывала, что аудитория уже спустя час занятия теряла интерес к происходящему на

экране, а некоторые слушатели и вовсе не были активны, запуская вебинар как фон во время работы. Говорить об эффективности такого обучения не приходилось. А между тем качество освоения этих программ слушателями напрямую влияет на количество обращений в техническую поддержку.

Кроме того, часть программ обучения у нас реализовывалась в очном формате, так как был сделан большой упор именно на практическую составляющую.

ПЕРЕСТРОЙКА

Пандемия перевернула всё с ног на голову, и процесс обучения пришлось перестраивать полностью. И это не преувеличение. Смена формата «доставки» материала требовала его полной переработки: изменения программ обучения, сценариев работы, административных процедур и т.д. Для перестройки

Телеметрия вебинаров показывала, что аудитория уже спустя час занятий теряла интерес к происходящему на экране, а некоторые слушатели и вовсе не были активны, запуская вебинар как фон во время работы

учебного процесса были сформулированы следующие задачи:

1. Сохранить качество материалов (а лучше повысить его и приблизить к «очке») для дистанта.
2. Сделать процесс обучения более удобным.
3. Сохранить практическую составляющую.

ПЕРВАЯ ЗАДАЧА

Первая задача потребовала переучить команду обучения из «говорящих голов» в производителей контента для онлайн-обучения. Теперь мы умеем творить чудеса в видеоредакторах, системах производства контента для СДО (Storiline, Adobe Captivate, iSpring Suite). Мы научились работать с картинкой, работать с голосом за кадром, писать сценарии для роликов, монтировать ролики, вычищать шум в картинке и звуковой дорожке, использовать различные эффекты внутри видео для фокусировки и удержания внимания, формировать траекторию обучения и много чему ещё продолжаем учиться.

ВТОРАЯ ЗАДАЧА. СДО

Для решения второй задачи было принято решение полностью отказаться от синхронного формата дистанционного обучения (вебинаров) и перенести все материалы в систему дистанционного обучения (далее СДО). Очевидными плюсами СДО были:

- ♦ возможность изучения материала с любого устройства в любой точке земного шара, где есть интернет;
- ♦ относительная свобода в выборе темпа, отсутствие привязки к строгому расписанию занятий.

Безусловно, для обеспечения эффективности мы ввели некоторые ограничения. Например, доступ к СДО мы предоставляем слушателям на определённое время (от 2 до 4 недель в зависимости от курса), и они сами решают, когда учиться и сколько времени в день этому посвящать.

Каждый курс построен по определённой логике и обязательно завершается контрольными мероприятиями: тесты, экзамен, контрольный практикум. Такой подход гораздо удобнее и позволяет совмещать производственную деятельность наших заказчиков с обучением.

Мы пришли к необходимости создания учебных стендов с продуктами в облаке, но это перспектива, пока же ведётся тестирование систем виртуализации в условиях санкционных ограничений

Нашим слушателям больше нет необходимости делать выбор в пользу работы или учёбы. Учиться можно и в перерывах, и дома, и даже в дороге (в метро или автобусе). Материалы удобно структурированы, что позволяет в любое время вернуться к нужному разделу курса.

Новый формат работы потребовал изменений в организации процесса записи на обучение, учёта результатов в CRM, документообороте. Однако выбора у нас не было, и мы с настойчивостью катка проехали по всем граблям, заботливо разложенным для нас новой реальностью.

ТРЕТЬЯ ЗАДАЧА. ВИРТУАЛИЗАЦИЯ

Третья задача оказалась самой трудной, так как продукты компании сложны и тяжеловесны. У нас появилась дилемма: либо разворачивать дорогостоящие облачные тестовые стенды и предоставлять слушателям к ним доступ, либо использовать текущую инфраструктуру класса и предоставлять доступ к уже имеющимся в отделе ресурсам. Но как эти ресурсы эффективно использовать при асинхронном дистанционном обучении? Поскольку все стенды в классе, по сути, являются десктопами с набором виртуалок, вопросы администрирования и отказоустойчивости при новом сценарии использования делали такой подход контрпродуктивным.

Поиском решения этой задачи мы занимались всем отделом, несколько недель тестируя разные подходы. Забегая вперёд, скажу, что мы всё-таки пришли к необходимости создания учебных стендов с продуктами в облаке, но это перспектива (хоть и близкая), пока же ведётся тестирование систем виртуализации в условиях санкционных ограничений.

ПРО ОБЛАЧНЫЕ СТЕНДЫ

До готовности облачных стендов пришлось импровизировать и перестроить

подход к организации практических занятий по ряду программ. Мы отказались от коллективных практических занятий в силу невозможности качественно организовать процесс на текущей инфраструктуре и ввели индивидуальные занятия с тренером над стендом, встроив их в программу обучения некоторых курсов. Подход оказался достаточно эффективным и хорошо себя зарекомендовал. Скорее всего, мы продолжим применять в обучении именно этот подход, заменив только технологическую часть: перенесём стенды в облако.

Кроме прочего, в работе с облачными стендами после их запуска мы планируем применить технологии и методические наработки, которые готовили совместно с экспертным сообществом компетенции WorldSkills «Корпоративная защита от внутренних угроз ИБ». За годы работы с этой организацией мы создали целый ряд инструментов для среднего профессионального и высшего образования: это и генератор событий с заранее запрограммированными наборами инцидентов для DLP-системы, и система автоматической проверки качества настройки DLP, которая на основе загруженного в неё эталона подключается к DLP для фиксации результатов работы. После запуска генератора событий она выводит результат в удобной для восприятия табличной форме. Кроме того, был собран внушительный набор инцидентов DLP, которые обновлялись не реже четырёх раз в год на протяжении пяти лет.

В этом смысле задел на будущее у нас уже более чем внушительный. Дело за малым — найти качественную отечественную систему виртуализации, которая подошла бы нам по всем параметрам.



Ксения ТРОХИМЕЦ
заместитель CSO hh.ru

ОСТРЫЙ ДЕФИЦИТ ИБ-СПЕЦИАЛИСТОВ СОХРАНЯЕТСЯ

РЫНОК ТРУДА В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ:
ИТОГИ 2022 ГОДА

54% российских компаний испытывают дефицит кадров на рынке информационной безопасности. Из них 17% отмечают, что

в 2022 году он усилился по сравнению с 2020–2021 гг. Это показали результаты совместного опроса «СёрчИнформ» и hh.ru, проведенного осенью.

За 2022 год компании-работодатели опубликовали на hh.ru 27,2 тыс. вакансий для ИБ-специалистов, что на 22% ниже показателя 2021 года. При этом, по среднемесячным значениям в течение года спрос на ИБ-специалистов замедлился незначительно: в 2021 году ежемесячно было открыто 2,9 тыс. вакансий, в 2022–2,3 тыс. Есть и положительные тенденции по спросу, которые позволяют прогнозировать дальнейший рост числа вакансий в 2023 году. Треть опрошенных hh.ru и СёрчИнформ сообщили, что в их компаниях в этом году ИБ-подразделение появилось или находится в процессе создания. Столько же отметили, что в компании появился или в ближайшее время появится ответственный за информационную безопасность руководитель.

Один из главных позитивных моментов — рост роли и значения функции ИБ в бизнесе, независимо от того, является ли он частным, государственным, крупным, средним, малым. Мы видим понимание, что буквально любой бизнес, любая компания так или иначе задействует информационные технологии в своих процессах и их применение просто невозможно без обеспечения киберзащиты силами

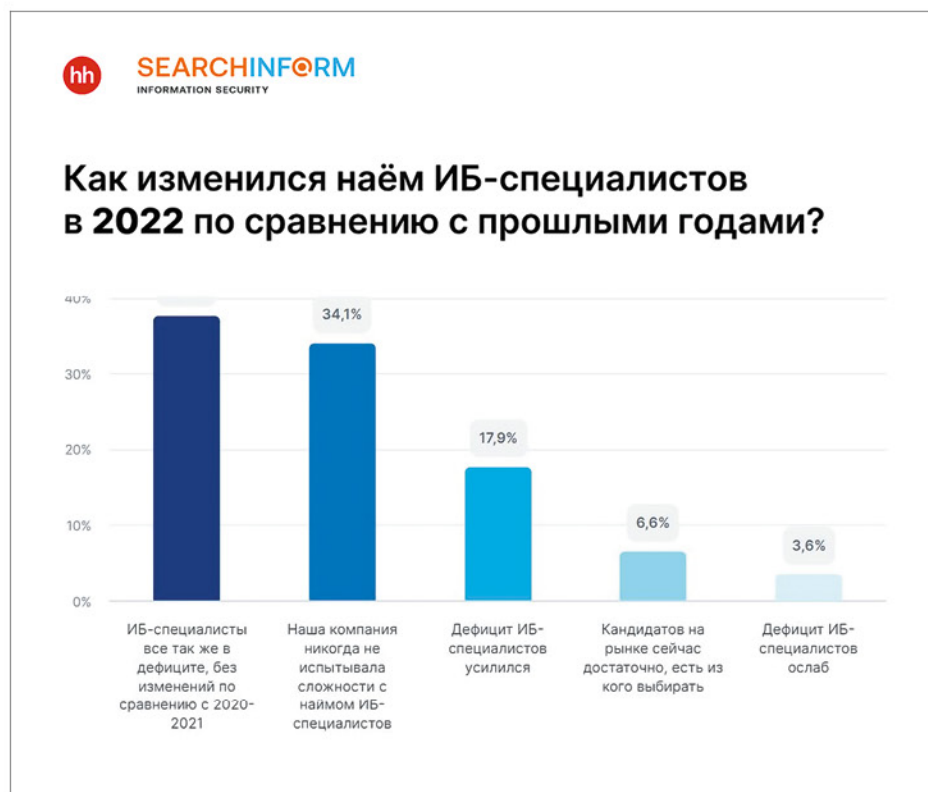


Рисунок 1. Как изменился наём ИБ-специалистов в 2022 году по сравнению с предыдущими годами



Востребованные навыки ИБ-специалистов и зарплаты

Топ-10 навыков, требуемых в ИБ-вакансиях

	2021		2022
Информационная безопасность	18%	Информационная безопасность	31%
Linux	15%	Информационные технологии	14%
Информационные технологии	14%	Linux	13%
SQL	9%	Английский язык	9%
Английский язык	9%	Технические средства информационной защиты	8%
Работа в команде	6%	Средства криптографической защиты информации	7%
TCP/IP	6%	Работа в команде	6%
Cisco	6%	Внедрение систем информационной безопасности	6%
Python	5%	Пользователь ПК	6%
Технические средства информационной защиты	5%	SQL	6%
Зарплата, медиана по РФ			
Предлагаемая	59 500	2022	63 100 (+6%)
Ожидаемая	78 300	2022	75 100 (-4%)

Рисунок 2. Востребованные навыки ИБ-специалистов и зарплаты в 2021–2022 гг.

квалифицированных специалистов на должном уровне. Сохранение высокого спроса гарантирует привлекательность данного направления в ИТ-сфере для талантливой молодежи на годы вперед, что может в дальнейшем облегчить для работодателей ситуацию с дефицитом ИБ-кадров.

Резюме ИБ-специалистов на платформе hh.ru имеет тенденцию к росту (+60% год к году), а их количество достигло 22,8 тыс. Несмотря на такую разнонаправленную динамику спроса и предложения дефицит в данном сегменте сохраняется: вакансий по-прежнему больше, чем самих ИБ-специалистов, а на одну вакансию приходится всего 0,8 резюме (для сравнения в 2021 году было еще меньше — 0,4). Для сравнения, в ИТ-сфере в течение 2021 года конкуренция составляла 1,8, в 2022 — выросла до 3,9.

В 2022 году вопрос защиты данных стал более актуален в связи с усилением киберрисков и подписанием указа президента России № 250. Он касается не меньше 500 тыс. компаний и, по сути, обязывает организовать выделенную ИБ-службу. Среди таких организаций дефицит кадров испытывают

гораздо сильнее. Почти половина (48%) опрошенных представителей субъектов КИИ говорят о недостатке ИБ-специалистов, еще 24% отмечают, что дефицит в 2022 году усилился. Среди системообразующих предприятий, которые должны подчиняться требованиям указа, ситуация еще хуже. Хотя внимание к безопасности в обеих категориях организаций традиционно высокое, до сих пор не везде есть выделенная служба ИБ. Пятая часть опрошенных из системообразующих предприятий и 15% из КИИ сообщили об этом (рис. 1).

В разрезе бизнеса четко выделяются три отрасли по уровню спроса на ИБ-специалистов — это непосредственно ИТ-компании (доля в 2022–32%, +3 п.п.), финансовый сектор (15%, без изменений к 2021) и телеком (7%, — 3 п.п.). Госсектор нарастил долю в ИБ-вакансиях до 3% к концу 2022 года. На 1 п.п., до 6% выросла доля компаний, оказывающих b2b-услуги в сфере кибербезопасности (рис. 2).

В течение 2022 года рынок труда столкнулся с двумя волнами релокации — в марте (после объявления о начале СВО) и в сентябре-октябре

(после объявления о проведении частичной мобилизации), которые оказали влияние на ИТ-сферу, поскольку основной массив релоцированных, по оценкам hh.ru на основе страновых изменений в резюме, пришелся на ИТ-специалистов (каждое пятое резюме относилось к ИТ), есть в них и доля ИБ-специалистов.

В целом, фокус на удаленную работу или как минимум гибридный режим в ИТ сохраняется. Такие режимы в ИТ практиковались задолго до пандемии и событий 2022 года. Однако в конце 2022 года все чаще стали звучать сигналы разной степени настойчивости о возврате к офисному или гибриднему режиму на территории работодателя для ИТ-специалистов, имеющих отношение в работе к контуру кибербезопасности и персональных данных пользователей. При найме ИБ-специалистов удаленный режим не приветствуется: работодатели указывали его лишь в 3% вакансий в 2022 году.

ВЫЖИВАНИЕ — ЭТО ОБЪЕДИНЕНИЕ

В СФЕРЕ ОБРАЗОВАНИЯ НАБЛЮДАЕТСЯ ТЕНДЕНЦИЯ
К ОБЪЕДИНЕНИЮ УСИЛИЙ ПРОТИВ КИБЕРУГРОЗ

НОВАЯ ЗЕЛАНДИЯ

В этом году в Новой Зеландии начнёт работу Единая платформа Te Rito, объединившая ресурсы министерства образования, дошкольных учреждений и школ и позволяющая вести обмен и хранение информации обо всех учениках страны.

В 2021 г. министр образования страны Крис Хипкинс подготовил обоснования к созданию транстасманских стандартов для ПО, поставляемого в школы. По его мнению, возникла опасная ситуация, которая может привести к широкомасштабной утечке персональных данных учащихся. Дело в том, что каждая школа заказывает ПО у местных компаний, разработки которых не соответствуют стандартам ИБ, предъявляемым правительством к аналогичным решениям в других отраслях. Школьное ПО создаётся без учёта кибербезопасности как ключевого требования и чаще всего не обновляется по мере появления новых угроз. Многие поставщики ИТ-решений хранят персональные данные на серверах в офшорных зонах, не всегда подпадающих под юрисдикцию Новой Зеландии.

В связи с отсутствием критериев оценки ПО и требований к разработчикам и вендорам персонал учебных заведений не может оценить качество поставляемого ПО, которое в большинстве случаев содержит уязвимости. Особую обеспокоенность вызывают приложения, используемые в повседневной работе. В частности, системы управления учащимися, содержащие конфиденциальную информацию о школьниках.

Анализ проблемы показал, что на пересмотр школьных контрактов и устранение угроз безопасности может уйти от четырёх до пяти лет. Некоторые поставщики ИТ-решений могут модернизировать свои системы, но велик риск

того, что сделают это далеко не все. Звучали предложения перейти на облачные решения — они снизили бы многие риски, но одновременно экспоненциально увеличили бы число приложений, используемых школами. К тому же поставщики облачных решений сами подверглись кибератакам, в результате произошли серьёзные утечки персональных данных.

В марте 2022 г. были проведены исследования, согласно которым выяснилось недофинансирование образовательных учреждений в части ИТ: школы получали \$40 млн в год от правительства, а тратили \$59 млн. Больше всего затрат пришлось на средние школы.

Учителя и директора школ плохо осведомлены о кибербезопасности, их квалификации недостаточно для преподавания с использованием информационных технологий, их действия увеличивают киберугрозы.

Согласно опросу, проведённому в 2021 г. в 45 школах, только 46% школ установили фильтрацию электронной почты на наличие спама и/или нецензурной лексики, 78% директоров не проходили обучение ИБ. Только 18% школ проводили уроки кибербезопасности для учащихся и персонала хотя бы в каком-то виде. 82% респондентов были просто плохо информированы о вопросах ИБ и не всегда знают, где взять информацию и что предпринять для решения проблем кибербезопасности.

В связи с этим встали вопросы дополнительных инвестиций в сферу образования, повышения квалификации и информированности персонала в вопросах ИТ и ИБ, создания централизованной цифровой поддержки школ, разработки рабочей программы для решения долгосрочных проблем.

В соответствии с законодательством правительству было рекомендовано

установить минимальные стандарты и оказывать централизованную поддержку школам, учитывая опыт США и Великобритании, где средние и начальные школы массово пострадали от хакерских атак.

В 2022 г. из государственного бюджета Новой Зеландии на укрепление кибербезопасности школ и повышение качества обучения с использованием информационных технологий было выделено \$27 млн.

Для создания единой цифровой среды правительство выделило \$40 млн. По итогам рассмотрения проблемы принято решение создания транстасманских стандартов для образовательного ПО. Была разработана платформа Te Rito, которая объединяет ресурсы министерства образования, дошкольных учреждений и школ, включая школы маори. Платформа позволяет вести обмен и хранение информации обо всех учениках.

Полноценное внедрение системы Te Rito в школах было приостановлено в 2021 г. из-за описанных выше проблем. Ожидается, что платформа заработает в 2023 г. Te Rito также вошла в правительственные программы развития информационных технологий и кибербезопасности до 2030 г.

LANCASTER UNIVERSITY

Грант в размере £4 млн от Управления по делам студентов (OfS) позволит Университету Ланкастера изменить подходы к методам обучения по направлениям ИБ. Здание исследовательского центра InfoLab будет модернизировано. Флагманский квартал киберзащиты данных будет состоять из восьми специализированных лабораторий и полумерсивного театра принятия решений.

Благодаря инвестициям университет станет одним из крупнейших учебных заведений в стране, которое

предложит своим студентам образовательные программы в области базовых технологий. Здесь будут готовить бакалавров в области компьютерных наук, кибербезопасности и науки о данных, магистров в области науки о данных и кибербезопасности.

Сотрудники университета ожидают, что благодаря новой лабораторной базе они получают доступ к передовым технологиям обучения студентов, будут вести исследования в области кибербезопасности, что даст толчок развитию новых партнёрских отношений с различными организациями, расположенными на территории городка. А студенты на практике, пусть и в лабораторных условиях, отработают теоретические навыки и получают опыт работы по специальности.

В планах Университета Ланкастера запуск направления «Наука о безопасности и защите» — крупной инициативы, которая оценивается в £19 млн. Программа направлена на расширение возможностей университета в области кибербезопасности. Это не только подготовка специалистов и проведение исследований в области ИБ, но и приглашение более 30 преподавателей и учёных по различным дисциплинам, чтобы сосредоточиться на цифровых угрозах и поддержать основные национальные инициативы в области кибербезопасности на Северо-Западе Англии.

Помимо студентов и аспирантов, Университет готов предложить поддержку национальным и региональным отраслевым партнёрам, которые хотят проверить навыки или повысить квалификацию сотрудников, решающих задачи кибербезопасности.

Ожидается, что работы по созданию квартала киберзащиты завершатся к ноябрю 2023 года.

США

Число кибератак на американские школы K-12 растёт, учреждения страдают от программ-вымогателей, DDoS-атак и других угроз. Если в начале пандемии защита и ликвидация последствий кибератак были индивидуальным делом отдельного учебного заведения, сегодня школьные округа ведут борьбу, объединив усилия. Бесплатные федеральные



Исследовательский центр Университета Ланкастера

ресурсы и ресурсы штатов дают рекомендации и предлагают помощь в организации киберзащиты, специалисты в сфере ИБ и автоматизированные сервисы могут помочь школам получить максимальную отдачу даже в условиях ограниченных бюджетов.

С сентября 2022 г. инциденты становятся более частыми и серьёзными, отметил Дуг Левин, национальный директор Некоммерческого центра обмена информацией и анализа, который специализируется на кибербезопасности школ системы K-12. Только в результате кибератаки на систему объединённого школьного округа Лос-Анджелес могли быть скомпрометированы данные более 400 тыс. учащихся.

В 2021 г. было зарегистрировано 166 кибератак, затронувших 62 школьных округа в 38 штатах. Однако реальное

количество инцидентов, с которыми сталкиваются школы, намного превышает известные данные. Возможно, оно выше в 10 раз, считает Левин.

Школы полагаются на ПО для бэк-офиса, которое легко компрометируется хакерами. Плюс дополнительные риски, связанные с хранением персональных данных при ограниченных ресурсах для их защиты. Государственные школы подвергаются атакам программ-вымогателей, которыми пользуются не только хакеры, но и учащиеся.

Роберт Хакворт, CISO Департамента образования штата Кентукки, сообщил, что только его департамент наблюдал пять тысяч попыток входа в систему ведомства за четыре дня.

Школы также сталкиваются с проблемой предоставления цифровых услуг учащимся всех возрастов, при этом

далеко не все могут соблюдать требования безопасности в силу возраста: многофакторную аутентификацию для трёхлетних детей, даже если у них есть учётная запись в системе школы, сами учителя считают избыточной.

Школы K-12 рассматривают все доступные виды поддержки. Среди них киберстрахование представляется неоднозначной защитой. Страховщики реагируют на растущие угрозы и ущерб от кибератак повышением премиальных цен, сокращением страхового покрытия и требованием к клиентам соблюдать всё больше рекомендаций по кибербезопасности. Эти тенденции проявляются во всех секторах, но они чувствительны в секторе образования, который считается высокорисковой отраслью. Некоторые школьные округа просто не могут позволить себе внедрять методы кибербезопасности, требуемые страховщиками. И хотя страховка даёт средства для восстановления после кибератаки, она не предотвращает ущерб. Более того, уже есть случаи повторной кибератаки на школьный округ, причиной которого стало недостаточное страховое покрытие после первого заражения компьютерной сети. На её восстановление просто не хватило средств.

Страхование может стать важнейшей функцией принуждения руководства школьных округов улучшить обеспечение кибербезопасности, требования страховых компаний являются базовыми, при этом мотивирующим актором может стать привлекательная цена самих полисов.

Ограниченные ресурсы школ не позволяют решать все задачи, но некоторые правильно расставленные приоритеты могут иметь далекоидущие последствия, считает Майкл Кляйн, научный сотрудник по влиянию цифровой инфраструктуры Управления образовательных технологий Министерства образования США.

Заражение большинства компьютерных систем школ происходит по трём причинам: фишинговые рассылки, скомпрометированные пароли и не обновлённое ПО. Школы могут снизить киберриски, введя требования к генерации уникальных паролей, внедрив многофакторную аутентификацию,

блокируя вредоносные домены и регулярно обновляя ПО согласно рекомендациям Агентства по кибербезопасности и инфраструктурной безопасности (CISA). Школы должны уделять этим вопросам приоритетное внимание.

Чиновники призывают школы участвовать в обмене информацией, бесплатно присоединяясь к Центру анализа и обмена информацией (MS-ISAC). Многие рекомендации центров CISA и MS-ISAC могут помочь школам избежать кибератаки, создать план реагирования на киберинциденты и подготовить школы к действиям в чрезвычайной ситуации.

CISA даёт возможность школам провести бесплатную оценку киберустойчивости и средств защиты от программ-вымогателей, и многие уже воспользовались этим предложением.

Школы с ограниченными возможностями ИТ-команд (таких в США большинство) могут получить круглосуточную защиту, внедрив автоматизацию и услуги аутсорсинга. К их услугам большой спектр SOC-центров и решений класса SOAR, бесплатных ресурсов. Нередко нужные функции киберзащиты обнаруживаются в уже приобретённых школами инструментах — их нужно просто включить.

Источником финансирования части решений школьной киберзащиты могут стать гранты по программе кибербезопасности штатов и местных органов власти. Округа K-12 также могут обратиться за помощью к государственным ресурсам и добровольцам. Так, в штате Висконсин работают добровольные команды киберэкспертов для оказания помощи госучреждениям.

В департаменте образования штата Кентукки надеются, что один из центров информирования может помочь школам остановить деятельность учащихся, которые организуют DDoS-атаки на учебные заведения, и направят их энергию в правильное направление.

После сентябрьской остановки в результате кибератаки объединённого школьного округа Лос-Анджелеса Министерство образования США объединило различные киберресурсы в одном месте для удобства пользования. Школы, пострадавшие от кибератак,

также могут обратиться в Центр технической поддержки конфиденциальности за помощью в ликвидации последствий.

ОКЕАНИЯ

Университет Монаша (Мельбурн) в сотрудничестве с Центром кибербезопасности Океании (OCSC) проводит набор участников в новый проект, направленный на обучение организаций методам защиты от киберугроз.

Исследователи Университета ищут участников в 11 странах Индо-Тихоокеанского региона, ориентированных на кибербезопасность и информационные технологии, для бесплатного обучения передовой криптографии, которая может помочь защитить от угроз со стороны квантовых компьютеров.

Трёхлетняя программа «Постквантовая криптография в Индо-Тихоокеанском регионе» (PQCIIP) ориентирована на сотрудников организаций и правительственных органов Малайзии, Индонезии, Самоа, Тонги, Вануату, Новой Гвинеи, Кирибати, Микронезии, Тувалу, островов Кука и Науру.

Директор проекта, доцент факультета информационных технологий Университета Монаша Рон Стейнфелд считает, что шифрование является одной из ключевых мер защиты от утечки данных, но большинство используемых в настоящее время криптографических средств недостаточно устойчивы к атакам со стороны квантовых компьютеров. Они могут быстро расшифровывать большую часть зашифрованных данных. По мнению исследователя, такие компьютеры станут реальностью в ближайшие годы. На фоне роста числа кибератак и утечек данных критически важно помочь соседним с Австралией странам укрепить возможности противостоять существующим киберугрозам, одновременно готовясь к атакам следующего поколения.

С помощью программы PQCIIP эксперты по кибербезопасности из Университета Монаша и Центра кибербезопасности Океании проведут для желающих принять участие в проекте организаций и правительственных учреждений детальную оценку их текущих возможностей в области постквантовой кибербезопасности, курс



Университет Квинсленда

специализированного обучения, планирования и оценки киберугроз.

Руководитель отдела исследований и наращивания потенциала OCSC доктор Джеймс Бурман отмечает, что цель программы — дать участникам углублённое понимание постквантовой криптографии, всесторонние знания связанных с ней инструментов. Они смогут разработать собственный план перехода для защиты организаций от угроз квантовых вычислений. Обучение в рамках проекта будет адаптировано к местным потребностям, доступно онлайн для ознакомления после курса и бесплатно для всех, кто руководит или работает в сфере ИТ или кибербезопасности в большинстве государственных структур (за исключением военных, разведывательных или правоохранительных органов) или организаций в любой из 11 стран Индо-Тихоокеанского региона. Совместная стандартизация и повышение кибербезопасности в каждой из этих стран приведёт к укреплению взаимоотношений и защите данных во всём регионе.

RQCSIP финансируется Государственным департаментом США, части программы будут доступны для участников бесплатно.

КИБЕРАТАКА НА УНИВЕРСИТЕТ КВИНСЛЕНДА

Кибератака на второй по величине университет Квинсленда привела к тому, что принтеры кампуса начали массово распечатывать требования вымогателей. Университет отключил все ИТ-системы в качестве меры предосторожности, технический персонал и приглашённые специалисты в области ИБ проводят расследование.

Проректор университета, профессор Маргарет Шейл сказала, что её принтер был среди устройств, подвергшихся кибератаке. Принтер распечатывал требования хакеров до тех пор, пока в нём не кончилась бумага. Записка с требованием выкупа, подписанная «Royal ransomware», использовала хорошо известную схему вымогательства. Сообщение содержало угрозы не только шифрования, но и распространения предварительно скопированных данных в интернете, если не будет выплачено «скромное авторское вознаграждение».

Профессор Шейл отметила, что несколько систем Университета были скомпрометированы, но ни одна из основных (студенческих, штатных и финансовых) не была повреждена.

«Все чувствительные с точки зрения хранения данных системы мы закрыли, — сказала профессор Шейл. — Остановлена работа приёмной комиссии, некоторые внутренние системы для студентов и персонала. Есть некоторые скомпрометированные системы, они заблокированы в результате работы шифровальщика».

Технологический университет Квинсленда уже проинформировал персонал и студентов о киберинциденте. Сотрудники также общаются с абитуриентами, которые получили предложение учиться в университете, но не могут заполнить документацию до восстановления работоспособности всех систем.

О киберинциденте уведомлены федеральные власти, этот факт подтверждён и в Федеральном министерстве образования. Расследование продолжается.

Ранее министерство здравоохранения США выпустило предупреждение больницам о подобной программе-вымогателе, первые случаи нападениях шифровальщика зафиксированы в сентябре.

«Royal — это новая программа-вымогатель. О вредоносном ПО и его операторах пока мало известно», — сообщали власти США в Предупреждении для учреждений здравоохранения всех штатов.



КИБЕРСТАВКИ РАСТУТ

ВОЛНУЮТСЯ ВСЕ! КРОМЕ ХАКЕРОВ...

В то время как государства усиливают совместную регуляторную политику в области кибербезопасности, а хактивисты-антиглобалисты требуют вернуться в доколумбовы времена, хакеры продолжают собирать персональные данные и финансы.

ДИРЕКТИВА NIS2

Совет Европы принял закон о едином уровне кибербезопасности по всему Евросоюзу, направленный на повышение устойчивости и возможности реагирования на киберинциденты как в государственном, так и в частном секторах, а также ЕС в целом. Документ,

получивший название «Директива (ЕС) 2022/2555 (Директива NIS2) Европейского парламента и Совета от 14 декабря 2022 года о мерах по обеспечению высокого общего уровня кибербезопасности во всём Союзе, вносящая изменения в Регламент (ЕС) № 910/2014 и Директиву (ЕС)



2018/1972 и отменяющая Директиву (ЕС) 2016/1148», пришёл на замену Директиве NIS (Network and Information Security).

NIS2 устанавливает базовый уровень для мер контроля над рисками кибербезопасности во всех секторах, на которые распространяется действие директивы: энергетика, транспорт, здравоохранение и цифровая инфраструктура. Новая директива направлена на гармонизацию требований кибербезопасности и реализацию мер кибербезопасности в государствах —

членах ЕС. Установлены минимальные правила для нормативно-правовой базы и учреждены механизмы эффективного сотрудничества между соответствующими органами в каждом государстве ЕС.

Новая директива NIS2 вводит общее правило для идентификации организаций, подпадающих под соответствующее регулирование, и даёт чёткие критерии, позволяющие странам определить компании, на которые распространяется действие документа. Правила не будут применяться к организациям, осуществляющим деятельность в области обороны и национальной безопасности, не распространяется на общественную безопасность и правоохранительные органы. Из сферы действия документа также исключены судебная система, парламенты и центральные банки.

NIS2 в обязательном порядке применяется к государственным органам власти на высшем и региональном уровнях. Применима ли данная директива на местном уровне, должны решить сами государства — члены ЕС.

Директива приведена в соответствие с отраслевым законодательством, в частности, с Положением о цифровой операционной устойчивости для финансового сектора (DORA) и Директивой об устойчивости критически важных объектов (CER), чтобы обеспечить юридическую ясность и согласованность между всеми документами.

Новый закон также упорядочивает предоставление отчётности во избежание чрезмерной нагрузки и содержит график отчётов EU-CyCLONe — сети национальных органов власти в государствах-членах, отвечающих за управление киберкризисами, — перед Европарламентом и Советом Европы.

Государства — члены ЕС должны включить положения директивы в национальное законодательство до 17 октября 2024 г.

АНТИГЛОБАЛИСТЫ НА МАРШЕ

Представители хакерской группировки Guacamaya дали интервью изданию Global Voices. Группировка,

взломавшая компьютерные сети государственных и коммерческих структур нескольких стран Центральной и Южной Америки, объяснила журналистам свои мотивы и ожидания после массовых утечек конфиденциальной информации.

Хакеры выступают от имени «живых существ, населяющих Американский континент с доколумбовых времен», которые выражают озабоченность критической глобальной экологической ситуацией. Жизненно важные экосистемы региона — ледники, тропические леса Амазонии и коралловые рифы — страдают от деятельности пришельцев с Севера. Растёт температура окружающей среды, вырубается леса, тают ледники. В странах Латинской Америки более двухсот экологов были убиты за свою деятельность.

В сентябре 2022 г. Guacamaya взломали системы правительственных учреждений Мексики, Чили, Колумбии, Гватемалы, Венесуэлы, Бразилии и Эквадора; похищены почти 10 Тб информации, содержащей электронную переписку вооружённых сил и полиции латиноамериканских стран. Часть информации попала в открытый доступ. Хакеры утверждают, что правоохранители и военные, прошедшие подготовку в США, используются правительствами стран Латинской Америки для подавления протестов на местах.

Летом прошлого года хакеры взломали компьютерные системы нескольких горнодобывающих компаний и государственных учреждений стран Центральной и Южной Америки и похитили 2 Тб данных. Среди украденных материалов — электронная переписка нефтяных и горнодобывающих компаний из Эквадора, Бразилии, Венесуэлы, Чили и Колумбии, Министерства природных ресурсов Гватемалы, Агентства по углеводородам Колумбии.

Объясняя свои цели и задачи, хакеры отметили, что выбрали худшие компании и госструктуры, которые совершают наибольшее число злоупотреблений и фактов коррупции, встречают активное сопротивление со стороны местных сообществ. Прежде чем выложить похищенную

информацию в открытый доступ, киберпреступники изучают материалы на предмет важности утечек, поэтому не весь объём информации доступен широкой публике. В основном интерес группировки сосредоточен на военных архивах. Так, она опубликовала данные о причастности армии к подавлению социального напряжения в Чили в 2019 г., слежке с участием армейских специалистов за лидерами сообществ коренных народов в Мексике. Отдельное внимание уделено закупке шпионского программного обеспечения Regasus для слежки за журналистами, хотя мексиканское правительство отрицало факт покупки. Часть информации касается деятельности государственных структур Колумбии, в том числе украдены электронные письма Генеральной прокуратуры и Министерства обороны.

Конфиденциальность и безопасность в цифровом мире стали причиной растущей напряжённости между гражданским обществом и правительствами, считают хакеры. Слежки и насилие происходили на протяжении всей истории государств, сегодня они ведутся новыми средствами. Если правительства теперь могут приобретать программное обеспечение для защиты интересов нации, гражданские движения также могут получить доступ к новым инструментам, помогающим разоблачать коррупционеров, выявлять несправедливости или нарушения прав человека, считают хактивисты. Они хотят начать менять восприятие ситуации в регионе путём разоблачения коррумпированных чиновников и структур, которые якобы созданы на благо общества. Хакеры полагают, что благодаря их действиям люди восстанут на борьбу с «прогнившей системой». А хакерство станет тем инструментом, что вызовет достойный гнев.

Рассказывая о методах взлома, киберпреступники отметили, что использовали относительно простые технические знания и навыки, которыми может овладеть любой желающий. Доступ был осуществлён через известные уязвимости. Ранее хакерская группа Aнолутоис уже взламывала компьютерные системы правительств стран

Латинской Америки. Последний инцидент произошёл в августе 2020 г., когда были похищены 400 файлов, подтвердивших фальсификацию данных по COVID-19, опубликованных правительством Никарагуа.

Хакеры Гуасатама призывают обновить глобальный механизм разрушения, вернуться к основам и принципам, на которых воспитывались поколения коренных жителей Центральной Америки, предлагают жить в гармонии с миром и удовлетворять запросы сообщества, а не мировых корпораций. Хактивисты полагают, что земли региона дадут людям всё, что требуется для жизни: лес для строительства жилья, продовольствие, лекарства на основе местных растений... «Юг не нуждается в Севере, Север не может жить без эксплуатации Юга. Решение состоит в деколонизации умов, в том, чтобы перестать верить, что мы низшие существа, потому что живём на „Глобальном Юге“, изобретённом Западом», — считают хакеры-антиглобалисты.

В ШАГЕ ОТ ВСЕМИРНОГО ПРИЗНАНИЯ

Две специализированные медицинские организации — Агентство по оказанию медицинской помощи на дому Техаса и сеть клиник женского и семейного здоровья из Пенсильвании — сообщили о киберинцидентах с использованием программ-вымогателей. В результате хакерских атак затронуты персональные данные почти 600 тыс. человек.

Представители Агентства по уходу на дому Техаса обратились в прокуратуру штата 13 января с заявлением о киберинциденте, затронувшем данные порядка 124 тыс. жителей штата Техас и неназванное количество жителей Северной Каролины, сообщает портал BankInfoSecurity.

Об атаке программы-вымогателя стало известно в июне 2022 г. Неавторизованная сторона проникла и удалила некоторые файлы из компьютерных систем медицинской организации. Агентство уведомило правоохранительные органы и привлекло к расследованию специализированную компанию по ИБ. 15 ноября 2022 г. расследование было завершено. Анализ инцидента показал, что

неизвестные получили доступ к системам Агентства в период с 15 по 29 июня 2022 г. Затронутая информация включает персональные данные пациентов, медицинские сведения о лечении или диагнозе, а также информацию о назначенных лекарствах.

10 января Некоммерческая служба охраны здоровья матери и семьи в Уилкс-Барре (Пенсильвания, США), сообщила в прокуратуру штата Мэн об аналогичном киберинциденте, который затронул почти 461 200 человек, в том числе 68 жителей штата Мэн. Служба поддерживает сеть центров здоровья и питания в 17 округах Пенсильвании.

3 января Служба начала работу по уведомлению пострадавших лиц, включая действующих и бывших сотрудников, пациентов и поставщиков, об инциденте с программой-вымогателем, обнаруженной 4 апреля 2022 г. Расследование киберинцидента показало, что несанкционированный доступ к системам службы произошёл в период с 21 августа 2021 г. по 4 апреля 2022 г.

Хакеры получили персональные данные, финансовую и медицинскую информацию, имена пользователей и пароли в сети Службы. Компания заявила, что у неё нет доказательств последующего использования украденных в результате взлома данных. Однако она предлагает частным лицам 12 месяцев бесплатного кредитования и мониторинга личных данных, а также усиливает кибербезопасность систем.

Хакеры всё чаще выбирают своими целями медицинские организации различных типов и их поставщиков, включая более мелкие и специализированные компании, отмечает эксперты портала BankInfoSecurity.

«Медицинские данные очень прибыльны. Киберпреступники знают, что малые и средние компании, как правило, хуже защищены, чем более крупные организации», — считает Джерри Капонера, генеральный менеджер по киберрискам компании ThreatConnect.

Директор по информационным технологиям компании Critical Insights Майкл Гамильтон отмечает, что киберпреступники выбирают потенциальных жертв среди учреждений здравоохранения. «Выбор целей сопряжён

с минимизацией криминального риска. Киберинциденты с программми-вымогателями в организациях, которые не предоставляют услуг неотложной помощи, с меньшей вероятностью будут иметь последствия для пациентов, включая гибель людей, — отмечает Майкл Гамильтон. — Хакеры находятся на расстоянии вытянутой руки от признания их „террористами“, кем считает их администрация Байдена».

«Организации здравоохранения по всему миру сталкиваются с проблемами, которые в конечном итоге могут повлиять на кибербезопасность: сокращение расходов в связи с ростом инфляции, уменьшение выплат страховыми компаниями, увеличением расходов на медицинские услуги, — говорит Джерри Капонера. — Информационные технологии и кибербезопасность часто оказываются включёнными в общий перечень».

«Небольшие организации сектора здравоохранения, которым особенно не хватает ресурсов для кибербезопасности, должны идти по наименее затратному пути и создать политику реализации потребностей на личном устройстве, — считает Майкл Гамильтон. — На рабочих местах те, кому не нужна внешняя электронная почта, не должны её получать, а социальные сети должны быть заблокированы».

МЕТОДЫ РАЗНЫЕ, РЕЗУЛЬТАТ ОДИН

Онлайн-мошенничества и методы социальной инженерии популярны во всём мире. Мошенники всех стран ищут и находят новые способы проникнуть во все сферы жизни граждан, учитывая их национальный менталитет. И каждая страна сталкивается как с универсальным, так и с уникальным набором проблем, если речь заходит о мошенничестве и кибербезопасности.

По разным рейтингам, в топ-10 стран, где чаще всего можно встретиться с кибермошенничеством и вирусами в Сети, входят до 15 стран, включая Россию до февраля 2022 г. Однако пятёрка «лидеров» всех рейтингов одинаковая: Нигерия, Индия, Китай, Бразилия и Пакистан, приводит данные

австралийский портал Tech Business News.

Нигерийские «письма счастья» известны всему миру. В самой стране онлайн-мошенничество стало распространённым явлением, которое лишает ничего не подозревающих жертв денег, данных и даже личной безопасности.

С ростом онлайн-торговли мошенники изобрели хитроумные способы наживы. Лучшие нигерийские уловки — лотерейные аферы, криптомошенничество, сборы на «благотворительность» и предложения «удалённой работы».

С мошенничеством в Индии можно столкнуться на каждом шагу как в реальной жизни, так и в виртуальном пространстве. Мгновенная платёжная система в режиме реального времени Unified Payments Interface (UPI), разработанная Национальной платёжной корпорацией Индии, активно используется хакерами. Они создают фишинговые ресурсы, выдают себя за другое лицо, просят авансовые платежи или просто требуют у малообразованных граждан сообщить им логин, пароль и идентификатор UPI для совершения операций. Среди других схем лидируют фишинг, мошенничества с возвратом средств, технической поддержкой, предложения «скидок от правительства» и махинации в цифровом маркетинге.

Китайские мошенники действуют изощрённо, они используют целый ряд тактик для обмана жертв. В КНР лидируют мошенничества в чрезвычайных ситуациях, предложения налоговых или иных государственных льгот, сообщения от самозванцев, выдающих себя за важных персон, обман с обменом валют, предложения по созданию онлайн-бизнеса и трудоустройству.

Кибермошенничество в Бразилии находится на подъёме, преступники пользуются растущим цифровым присутствием компаний и частных лиц. Поэтому многие считают страну претендентом на звание мирового лидера в онлайн-мошенничестве. Страна одной из первых в мире внедрила системы онлайн-банкинга, что создало дополнительные возможности для краж. Согласно отчёту о фишинге «Лаборатории Касперского»,

Бразилия возглавляет список стран с самым высоким уровнем утечек данных пользователей.

Согласно исследованию Института Игарапе, немногие пойманные бразильские киберпреступники — это хорошо образованные мужчины в возрасте от 25 до 35 лет из верхов среднего класса.

В ассортименте бразильских киберпреступников — аферы, известные как «добрый самаритянин» и получение посылок в аэропорту, мошенничества со входом в Wi-Fi, а также скиммеры, установленные на банкоматах.

В Пакистане случаи мошенничества становятся всё более распространёнными. По данным Banking Mohtasib Pakistan, в 2021 г. было получено 37 364 жалобы на финансовые мошенничества, что на 46% больше, чем в 2020 г. В 2022 г. зарегистрировано 19 670 обращений. Пакистанские мошенники собирают персональные данные и каналы онлайн-платежей, любят мошенничество в цифровом маркетинге, аферы с лотереями и призами.

Среди популярных ухищрений мошенников всего мира эксперты по кибербезопасности выделяют фишинг, онлайн-мошенничества с покупкой кибервалют и биткоинов, фальшивые онлайн-переводы денег, интернет-покупками. Пользователи ведутся на фейковые предложения об удалённой работе, загружают поддельное антивирусное ПО, общаются с «липовой» техподдержкой, «продвигают» ресурсы с помощью «поисковой оптимизации», сталкиваются с мошенниками на сайтах онлайн-знакомств и в социальных сетях. Популярны у пользователей «списания долгов», «налоговые каникулы и льготы», «реструктуризация кредитов и ипотеки», «помощь чиновника высокого уровня», «социальные выплаты», фиктивные благотворительные сборы и «инвестиции в высокодоходные компании», а также фейковые новостные баннеры, ведущие на фишинговые ресурсы, собирающие персональные данные незадачливого пользователя.

По прогнозам Cybersecurity Ventures, глобальный ущерб от действий киберпреступников будет ежегодно расти на 15%, достигнув к 2025 г. 10,5 трлн \$ в год по сравнению с 3 трлн \$ в 2015 г.



Амина ЗАМУЛИНА
руководитель направления
Центра DPO, Сбербанк

СУРОВЫЙ ОПЫТ ПОДНЕБЕСНОЙ

СИСТЕМА РЕГУЛИРОВАНИЯ
ПЕРСОНАЛЬНЫХ ДАННЫХ
В КИТАЕ¹

ГРАЖДАНСКИЙ КОДЕКС КНР (2021)

中华人民共和国民法典

Глава 6 (ст. 1032–1039) Гражданского кодекса КНР (далее — ГК КНР) посвящена вопросам приватности и защиты персональной информации. Вводится понятие **приватность**, под которой понимается право физического лица на частную жизнь, на личное пространство, личные занятия и личную информацию, которую такое лицо не хочет раскрывать другим (ст. 1032). Отдельно акцентируется внимание на том, что никто не имеет права вмешиваться в личную жизнь человека, разглашать или публиковать её подробности.

ГК КНР вводит прямой запрет на действия, которые могут нарушить приватность человека ввиду их интрузивности. К числу таких действий относятся:

- ♦ осуществление телефонных звонков, отправка SMS и электронных писем, использование мессенджеров и т.д.;
- ♦ проникновение, фотографирование или подглядывание за личным пространством лица (например, домом или номером);
- ♦ фотографирование или подглядывание за интимными частями тела человека;
- ♦ обработка персональной информации человека и т.д.

Такие действия разрешены только при наличии предварительного явного

согласия или иных оснований, предусмотренных законом.

В соответствии со ст. 1034 ГК КНР, **персональная информация** — это информация, записанная электронно или иным образом, которая самостоятельно или в комбинации с иной информацией может использоваться для идентификации физического лица, включая имя, дату рождения, идентификационный номер, биометрическую информацию, адрес проживания, телефонный номер, адрес электронной почты, информацию о здоровье, местоположение и иное.

ГК КНР включает общие принципы обработки ПДн, такие как законность, минимизация данных и др., а также стандартные права субъектов

¹ Окончание. Начало в № 4 (47) 2022.



Согласно ст. 25 PIPL оператор данных не может разглашать обрабатываемые ПДн, за исключением случаев получения отдельного согласия на такое раскрытие. Ст. 1038 ГК КНР также запрещает раскрывать ПДн третьим лицам в отсутствие согласия субъекта ПДн.

Исходя из данных требований, представляется, что во всех случаях, прямо не предусмотренных законом, оператор обязан получать согласие субъекта на раскрытие его данных третьей стороне. В связи с тем остаётся открытым вопрос обеспечения правового основания на передачу ПДн в рамках договора поручения обработки ПДн. Так, PIPL прямо предусматривает обязанность получения отдельного согласия субъекта на передачу персональных данных между самостоятельными операторами. Однако законодатель опускает этот момент в положениях, регулирующих передачу данных от оператора обработчику, привлекаемому оператором по договору поручения.

Если исходить из того, что PIPL разрабатывался на базе GDPR, такое согласие не требуется, вместе с тем общие положения как гражданского законодательства, так и PIPL налагают запрет на раскрытие (предоставление/передачу) ПДн третьим лицам в отсутствие согласия субъекта.

ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПДн

В последнее время с Китаем связаны большие надежды и чаяния отечественного бизнеса. Многие отечественные компании принимают решение о перераспределении бизнеса с запада на восток и выходе на китайский рынок. В связи с этим приобретают особую актуальность вопросы, связанные с трансграничной передачей ПДн. Помимо общих требований к трансграничному обмену ПДн, предусмотренных в PIPL и Руководстве по защите персональной информации (信息安全技术: 个人信息安全规范), детальные вопросы трансграничной передачи ПДн представлены в Руководстве по сертификации деятельности по трансграничной обработке ПДн (网络安全标准实践指南 — 个人信息跨境处理活动安全认证规范) (далее — Руководство) и Мерах

по оценке безопасности трансграничной передачи ПДн (数据出境安全评估办法) (далее — Меры по оценке безопасности). Данные документы регулируют вопросы проведения оценки безопасности трансграничной передачи ПДн, требования к договору между экспортером и зарубежным импортёром данных, требования к назначению лица, ответственного за обработку ПДн (DPO), права субъектов ПДн в части трансграничной передачи, порядок подачи заявки в надзорный орган на прохождение государственной оценки безопасности трансграничной передачи ПДн и др. Например, при подаче заявки на прохождение государственной оценки безопасности трансграничной передачи оператор данных обязан представить в уполномоченный орган следующий пакет документов:

1. Заявку на прохождение оценки.
2. Результаты внутренней оценки безопасности трансграничной передачи.
3. Соглашение/договор, подлежащий подписанию экспортером и зарубежным импортёром данных.
4. Иные материалы по требованию проверяющего органа.

При этом государственная оценка безопасности трансграничной передачи требуется не всегда, а только в случаях, перечень которых содержится в Мерах по оценке безопасности:

♦ За рубеж передаётся «важная информация», т.е. данные, которые в случае их компрометации могут нанести ущерб национальной безопасности, экономической деятельности, социальной стабильности, общественному здравоохранению или безопасности.

♦ ПДн передаются за рубеж операторами критической информационной инфраструктуры или операторами ПДн, обрабатывающими личную информацию более 1 млн человек.

♦ За рубеж передаются ПДн более 100 000 физ. лиц или чувствительные ПДн более 10 000 физ. лиц.

В случае если государственная оценка безопасности трансграничной передачи ПДн не требуется, следует выполнить одно из стандартных условий, предусмотренных ст. 38 PIPL (приведены в первой части статьи).

ПДн — право на получение копий обрабатываемых данных, право на изменение и удаление ПДн.

Лицо, обрабатывающее данные, обязано уведомить надзорный орган и субъектов ПДн о нарушении безопасности ПДн.

В отличие от ГК КНР, PIPL не обязывает:

♦ операторов уведомлять субъектов ПДн в случае принятия достаточных мер для предотвращения негативных последствий для субъекта данных;

♦ обработчиков уведомлять о нарушении безопасности ПДн ни надзорный орган, ни субъектов данных.

Открытым остаётся вопрос, требуется ли отдельное согласие на передачу ПДн обработчику?

**ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОСТРОЕНИЮ СИСТЕМЫ ОБРАБОТКИ ПДН
В СООТВЕТСТВИИ С КИТАЙСКИМ ЗАКОНОДАТЕЛЬСТВОМ**

Учитывая повышенный интерес бизнеса к китайскому рынку, а также экстерриториальный характер действия PIPL, видится полезным предложить читателю практические рекомендации по приведению компании в соответствие с требованиями законодательства КНР о ПДн (таблица).

Описание мероприятия	Основание
1. Назначить лицо, ответственное за осуществление контроля за обработкой и защитой ПДн (далее — DPO)	Ст. 52 PIPL
2. Довести контактные данные DPO до надзорного органа Китая, а также опубликовать контактные данные DPO в публичном домене	Ст. 52 PIPL
3. Назначить лицо, ответственное за обеспечение кибербезопасности (далее — CISO)	Ст. 21 Закона о Кибербезопасности
4. Разработать и внедрить внутренние нормативные документы компании, включая: • Политику обработки ПДн; • Регламент (Положение) обработки ПДн; • форму реестра процессов, в которых осуществляется обработка ПДн; • типовые формы документов (договоры, согласия и т.п.); • порядок взаимодействия с субъектами ПДн и надзорным органом, формы уведомления о нарушении безопасности ПДн; • ВНД в области кибербезопасности; • порядок реагирования на инциденты безопасности ПДн	Ст. 14–17, 51, 55–57 PIPL Ст. 21 Закона о Кибербезопасности Ст. 25 Закона о Кибербезопасности ¹
5. Уведомить субъектов ПДн об обработке ПДн до её начала	Ст. 17 PIPL
6. Провести анализ и учёт процессов обработки ПДн: • выявить процессы, в которых осуществляется обработка ПДн; • определить цели, правовые основания и сроки обработки ПДн, перечень третьих лиц, которым осуществляется передача ПДн, для каждого из процессов; • обеспечить сбор и систематизированное хранение согласий на обработку ПДн в случае, когда согласие выступает основанием обработки ПДн; • имплементировать требования ВНД в процессы; • обеспечить сбор и обработку минимально необходимого объёма ПДн для достижения поставленной цели; • составить перечень (реестр) процессов обработки ПДн	Ст.ст. 6, 10, 13, 17, 19 PIPL
7. Организовать процесс удаления/уничтожения ПДн, обеспечить наличие артефактов, подтверждающих удаление/уничтожение ПДн	Ст. 47 PIPL
8. Провести оценку DPIA в случаях, предусмотренных законом, а также обеспечить фиксацию результатов проведённой оценки	Ст. 55, 56 PIPL; Руководство по оценке воздействия на защиту персональной информации, GB/T 39335–2020

¹ См. также Emergency Response Law of the People's Republic of China, Production Safety Law of the People's Republic of China

9. Обеспечить локализацию баз данных на территории КНР в случаях, предусмотренных законом: • компания признаётся оператором критической информационной инфраструктуры (в соответствии с Законом)²; • объёмы обрабатываемых данных достигают размеров, установленных регулятором (Cyber Security Administration)	Ст. 40 PIPL
10. Заключить договоры с третьими лицами, с которыми планируется обмен данными (по форме Оператор — Оператор, Оператор — Обработчик). Обеспечить наличие правового основания на передачу ПДн третьим лицам	Ст. 20, 21, 22, 23, 55, 59 PIPL
11. Обеспечить законность трансграничной передачи ПДн: • определить процессы обработки ПДн, предусматривающие трансграничную передачу ПДн, и внести соответствующую маркировку в Реестр процессов обработки ПДн; • исполнить <i>одно</i> из требований к трансграничной передаче, предусмотренных ст. 38 PIPL. – пройти государственную оценку безопасности (в Cyber Security Administration); – пройти оценку со стороны специализированного органа КНР; – заключить с контрагентом SCC установленного образца; • удостовериться, что получающая сторона соответствует критериям обработки ПДн, установленным PIPL; • уведомить субъектов ПДн о передаче ПДн за рубеж, включая информацию о получателе данных; • обеспечить сбор отдельного согласия субъекта на трансграничную передачу ПДн; • провести DPIA	Ст. 38–40 PIPL
12. Внедрить технические и организационные меры защиты ПДн, направленные на предотвращение несанкционированного доступа, утечек, искажения и утраты ПДн: • издать политики и процедуры в области защиты информации; • установить эксплуатационные ограничения при использовании ПДн; • систематически проводить обучение для сотрудников; • внедрить технические меры защиты, включая: – построение системы сетевой защиты; – внедрение технических мер защиты от компьютерных вирусов, кибератак и др.; – внедрение системы мониторинга и фиксации инцидентов безопасности; – внедрение мер классификации данных, – внедрение мер резервного копирования, шифрования, обезличивания и др.	Ст. 9, 51 PIPL Ст. 21 Закона о Кибербезопасности
13. Разработать и внедрить план реагирования на инциденты безопасности, включая порядок уведомления надзорного органа об инцидентах безопасности	Ст. 9, 51, 57 PIPL
14. Обеспечить проведение систематического аудита деятельности по обработке ПДн	Ст. 54 PIPL
15. Организовать для сотрудников регулярное обучение в области безопасности ПДн	Ст. 51 PIPL

² В соответствии со ст. 31 Закона о Кибербезопасности КНР финансовый сектор признаётся критической информационной инфраструктурой

3×10 ТРЕНДОВ ФИНАНСОВОГО РЫНКА НА 2023 ГОД

ИССЛЕДОВАНИЕ АССОЦИАЦИИ ФИНТЕХ

Ассоциация ФинТех в исследовании «3×10 трендов на 2023 год» проанализировала и выделила топ-10 бизнес-, ИТ- и финтехтрендов 2023 года. Анализ показал, что ключевыми направлениями развития в 2023 году станут кибербезопасность, гибкость и открытость бизнес-моделей, искусственный интеллект, дезинтермедияция и деглобализация бизнеса.

Тренды российского финансового рынка во многом будут совпадать с трендами международными, однако вопросы технологического суверенитета и необходимость создания стабильного механизма трансграничных транзакций будут иметь более высокий приоритет, чем в других странах.

Из «3×10 трендов на 2023 год» следует, что открытые данные — один из ключевых трендов отечественного финтеха. В 2023 году внимание будет сосредоточено на развитии открытых API и экосистем по модели «все-как-сервис» (XaaS). Актуально развитие цифровых госсервисов на базе интеграции, использования биометрии, сквозного ID и цифрового профиля юридических лиц для создания инновационных сервисов, где в удобных клиентских путях пересекаются клиент, бизнес и государство.

В 2023 году российский финансовый рынок будет развивать цифровые финансовые активы (ЦФА), продолжит искать практические бизнес-кейсы по токенизации финансовых инструментов в форме цифровых активов. Россия находится в глобальном тренде, запуская проект цифрового рубля. Это позволит повысить уровень финансовой доступности и даст возможность создавать новые цифровые продукты и сервисы.

Один из главных фокусов отечественного финансового рынка — создание инфраструктуры для экосистемы платёжных сервисов и трансграничных расчётов. При этом трансграничные платежи актуальны не только для экономического роста стран БРИКС, ШОС и России. Как показывает анализ международных источников,

регуляторы прочих стран также думают об изменении подхода к трансграничным транзакциям.

Поскольку искусственный интеллект (ИИ) стал одним из ключевых драйверов развития финансового рынка, углубляется и расширяется его проникновение в продукты и процессы финансовых организаций. Ещё большую актуальность приобретают задачи исследования перспективных инструментов на его основе, безопасного и конфиденциального обмена данными, решение вопросов повышения доверия, безопасности и соблюдения этических норм при его применении.

Для российского рынка одно из важнейших направлений работы — технологический суверенитет, то есть обеспечение независимости отечественной технологической инфраструктуры от зарубежных поставщиков и формирование основы для устойчивого развития. Причём иностранные источники также говорят о необходимости повышения уровня технологического суверенитета своих рынков с учётом прецедентов последнего времени.

Глубокое проникновение информационных и цифровых технологий во все аспекты деятельности государства, финансового рынка, отдельных организаций и каждого человека, а также современная глобальная геополитическая ситуация заставят уделять особое внимание задачам обеспечения кибербезопасности финансового рынка в 2023 году.

В целом исследование «3×10 трендов на 2023 год» показывает, что с точки зрения развития финтехрешений Россия остаётся конкурентоспособной. Российские финансовые технологии вобрали в себя лучшие черты как западных, так и восточных практик. Развитие независимых технологий и сервисов консолидированными усилиями участников финансового рынка при поддержке регулятора имеет реальные перспективы.

3X10 КЛЮЧЕВЫХ ТРЕНДОВ НА 2023 ГОД



10 БИЗНЕС-ТРЕНДОВ

Новый клиентский опыт

- Клиентоцентричность**
Выстраивание бизнес-модели вокруг потребностей клиентов
- Иммерсивный клиентский опыт**
Использование VR, AR и MR-технологий в процессах взаимодействия с клиентом
- Персонализация продуктов и сервисов**
Обеспечение кастомизированного подхода с использованием доступности больших данных

Трансформация бизнес-модели

- Компонуемый бизнес**
Экономика возможностей и создание бизнес-модели компании из взаимозаменяемых «строительных блоков» путем компоновки и оркестрации
- Развитие экосистем**
Построение сети сервисов вокруг клиентов на основе единой технологической платформы
- Развитие бигтехов**
Выход крупных технологических компаний на новые для себя рынки, в частности рынок финансовых услуг

Цифровизация процессов

- Гибкость и адаптивность**
Способность оперативно адаптировать свои процессы и операционную модель
- Дезинтермедиация процессов**
Исключение или минимизация участия посредников
- Тотальная кибербезопасность**
Продвинутая защита критически важных систем от широкого спектра кибератак
- Устойчивый бизнес**
ESG – повестка и практика устойчивого ведения бизнеса

10 ТЕХНОЛОГИЧЕСКИХ ТРЕНДОВ

Инновационные решения

- Суперприложения**
Сочетают в себе функции приложения, платформы и экосистемы в одном месте, предоставляя третьим сторонам платформу для разработки и публикации своих продуктов
- Адаптивный ИИ**
Позволяет изменять поведение модели после развертывания с помощью обратной связи в реальном времени и непрерывно обучать модели
- Метавселенные**
Позволяют воспроизводить или виртуально дополнять свою активность в реальном мире путем использования комбинации Web3, пространственных вычислений и цифровых двойников в проектах на основе метавселенных

Масштабирование

- Отраслевые облачные платформы**
Отраслевые облака создают ценность для организаций за счет включения облачных сервисов в компонуемые отраслевые решения
- Платформенная инженерия**
Объединение SaaS, PaaS и IaaS с индивидуальной отраслевой функциональностью, которую можно использовать для более легкой адаптации к новым вызовам
- Реализация потенциала беспроводных технологий**
Интеграция нескольких беспроводных технологий позволяет использовать такую технологическую базу, которая позволиткратно сократить издержки

Оптимизация

- Цифровая иммунная система**
Совокупность саморегулируемых инструментов мониторинга рисков информационной безопасности
- Прикладная наблюдаемость данных**
Практическое использование широкого спектра доступных данных для принятия быстрых и правильных решений
- Управление доверием, рисками и безопасностью ИИ**
ИИ требует новых форм управления доверием, рисками и безопасностью, которые не обеспечивают традиционные элементы управления
- Устойчивые технологии**

10 ТРЕНДОВ ФИНТЕХА

Датацентричные экосистемы

- Вездесущий AI**
Монетизация накопленных данных и расширение областей применения AI
- Экосистемы идентификации**
Сквозной ID и экосистемы идентификации в различных сервисах, включая биометрию и eKYC
- Открытые API**
Создание новых бизнес-моделей на основе обмена данными в парадигме «все-как-сервис» [XaaS]

Транзакционная революция

- Развитие экосистем платежных сервисов**
Новые форматы платежных сервисов, включая встроенные платежи в приложениях сторонних игроков
- Трансграничные платежи**
Организация надежной и безопасной инфраструктуры трансграничных платежей для ведения бизнеса международного масштаба

Оцифрованные активы

- Цифровые финансовые активы и DeFi**
Новый рынок финансовых инструментов, использующий преимущества блокчейна и смарт-контрактов
- Цифровые валюты центральных банков**
Третья форма денег, повышающая безопасность, удобство и инновационность расчетов

Надежная основа

- Цифровое регулирование**
Развитие цифровых решений RegTech, SupTech и LegalTech в целях снижения рисков и ускорения взаимодействия на финансовом рынке
- Деглобализация**
Трансформация глобальной экономической и финансовой модели в направлении многополярности
- Устойчивые финансы**
Этичный метод принятия инвестиционных решений с фокусом на низкоуглеродную экономику



ГОРИЗОНТ — 0-10+ ЛЕТ

ПРОГНОЗ ВЛИЯНИЯ ПЕРСПЕКТИВНЫХ ТЕХНОЛОГИЙ НА ЛАНДШАФТ УГРОЗ КИБЕРБЕЗОПАСНОСТИ

Михаил АНИСТРАТЕНКО
Лаборатория
кибербезопасности
ПАО СберБанк

Илья БОЛОТОВ
Лаборатория
кибербезопасности
ПАО СберБанк

Дмитрий КУДИЯРОВ
Лаборатория
кибербезопасности
ПАО СберБанк

Александр КУЗЬМИН
Лаборатория
кибербезопасности
ПАО СберБанк

Лаборатория кибербезопасности Сбера выпустила аналитический отчёт «Прогноз влияния перспективных технологий на ландшафт угроз кибербезопасности» (Hypervector 2022). Новые технологии — виртуальная и дополненная реальность, 5G, генеративный искусственный интеллект, распределённые вычисления, дипфейк и многие другие — влияют на все аспекты нашей жизни. В том числе используются для кибератак и, напротив, для защиты от них. Поэтому в отчёте Hypervector 2022 каждая такая технология проанализирована и оценена с точки зрения степени влияния на ландшафт киберугроз. Также указан период времени, в течение которого технология, предположительно, достигнет зрелости и начнёт применяться массово. Более того, для каждой из рассмотренных технологий приведены примеры возможных угроз или её использования в кибербезопасности.

ВВЕДЕНИЕ

Появление и развитие новых киберугроз неразрывно связано с развитием технологий

Развивающиеся технологии изменяют ландшафт угроз, так как создают новые возможности для атак, или же находят применения как средства атаки или защиты. Поэтому данный анализ рассматривает новые и развивающиеся технологии как основу для прогноза возможных изменений в ландшафте киберугроз.

В качестве источников для прогноза развития технологий были использованы исследования и прогнозы развития технологий из научных публикаций, публикации Gartner, Institute for The Future и других.

Каждая из развивающихся технологий была проанализирована и оценена с точки зрения степени влияния на ландшафт киберугроз, и приведён временной промежуток, в который прогнозируется достижение данной технологией зрелости для широкого промышленного применения.

Цель данного анализа — предоставить структурам кибербезопасности в различных компаниях прогноз относительно сроков возникновения новых или существенной трансформации

существующих угроз для своевременной выработки методов противодействия им.

МЕТОДОЛОГИЯ

В отчёте приводится анализ развивающихся технологий с точки зрения их влияния на ландшафт угроз.

Оценка влияния на ландшафт угроз имеет три градации:

1. Высокое — технология существенно влияет на ландшафт угроз, создаёт возможности для реализации принципиально новых атак, создаёт новые поверхности атаки или существенно изменяет существующие. Также влияние оценивается как высокое, если технология может быть использована для защиты от киберугроз и имеет существенное преимущество по сравнению с уже используемыми методами защиты.

2. Среднее — технология влияет на ландшафт угроз, не создаёт возможностей для принципиально новых атак или методов защиты, но при этом позволяет значительно повысить эффективность существующих методов атаки или защиты.

3. Низкое — технология практически не влияет на ландшафт угроз, не порождает новых угроз или методов защиты. Обеспечивает лишь небольшой рост эффективности атак или методов защиты от них.

Помимо этого, рассмотренные технологии отнесены к одному из трёх временных промежутков, в зависимости от того, когда прогнозируется достижение пика зрелости технологии, делающее возможным её широкое промышленное применение в различных сферах.

При этом важно отметить, что прогнозирование сроков возникновения тех или иных технологий не является целью данного отчёта. В этом вопросе отчёт опирается на прогнозы известных аналитических агентств, таких как Gartner, а также на прогнозы в научных и аналитических публикациях.

БЛИЖНИЙ ГОРИЗОНТ — 1-5 ЛЕТ

Технологии с высоким уровнем влияния на ландшафт киберугроз:

Управление рисками человеческого фактора (Human Risk Management). Согласно исследованию Стэнфордского университета и

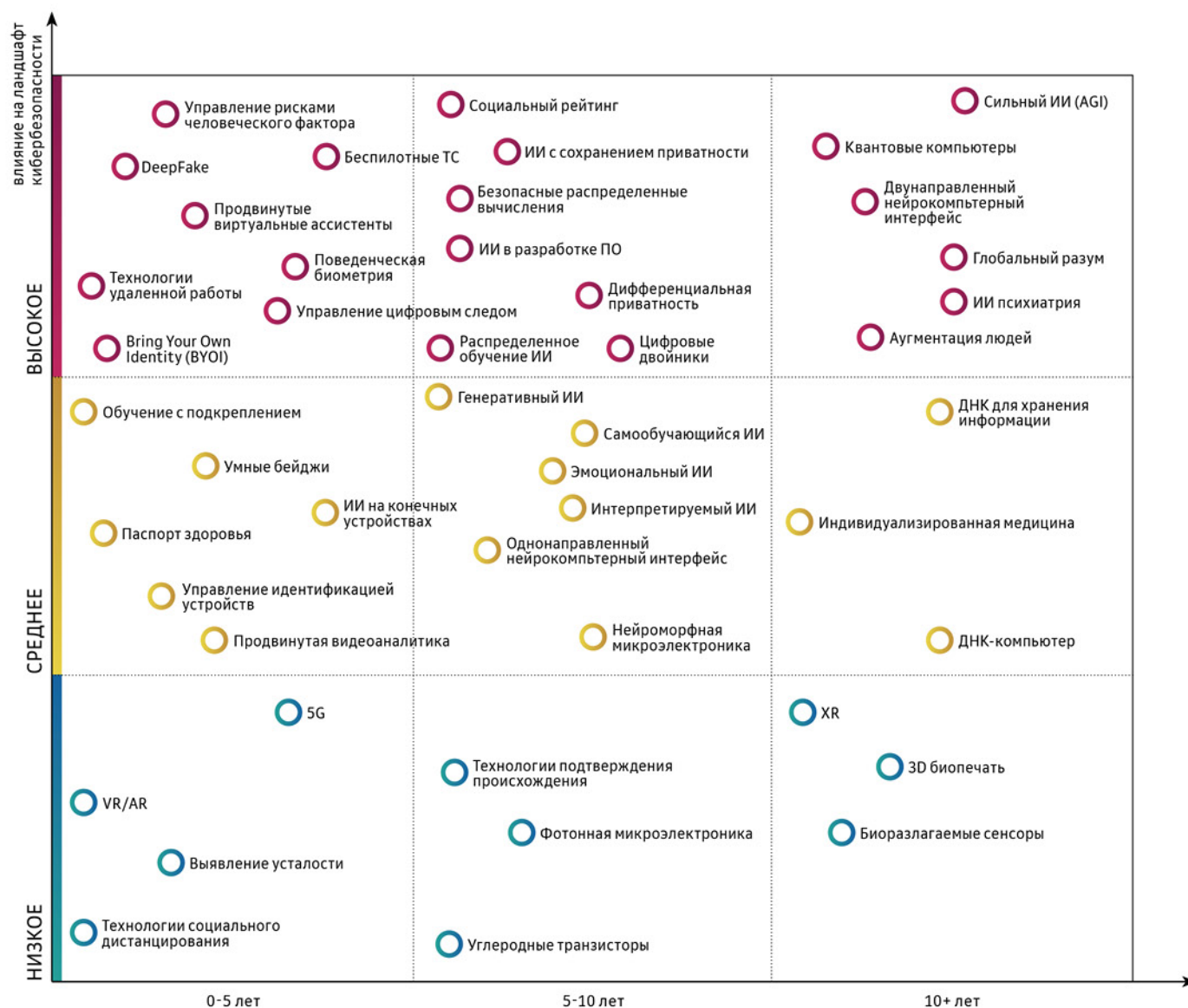


Рисунок 1. Hypervector — итоговый прогноз влияния технологий на ландшафт киберугроз. Ось X на графике — время в годах, разделённое на три промежутка: от 0 до 5 лет, от 5 до 10 лет, более 10 лет. Ось Y — влияние на ландшафт кибербезопасности, также разделённое на три промежутка: низкое, среднее и высокое

компании Tessian причиной 88% кибератак и утечек данных является человеческий фактор. Похожие цифры (85%) называет и Verizon в своём 2021 Data Breach Investigation Report. При этом данные показатели не меняются на протяжении многих лет, несмотря на значительные усилия и ресурсы, затрачиваемые на повышение осведомлённости сотрудников об угрозах кибербезопасности. Именно поэтому текущий рынок решений класса Security Awareness начинает постепенный переход от предложения своим клиентам тренингов для сотрудников и фишинговых учений к комплексному решению по управлению рисками человеческого

фактора — Human Risk Management Platform. Определение и составные элементы подобного решения пока не сформированы окончательно, и каждый вендор видит их несколько по-своему, но в целом важными элементами подобной платформы видятся следующие:

- ♦ Оценка осведомлённости сотрудника до начала обучения и выявление «слабых мест» для формирования индивидуальной программы обучения.
- ♦ Регулярное персонализированное обучение небольшими порциями информации (micro learning) — отдельный сеанс обучения не должен занимать более 5 минут, при этом само

обучение должно происходить часто, до нескольких раз в неделю.

- ♦ Оценка подверженности тем или иным рискам по результатам обучения, тестов и различных симуляций (не только фишинг, но и вишинг, смишинг и другие виды атак) — по результатам такой оценки для каждого сотрудника строится и регулярно обновляется профиль подверженности различным типам рисков кибербезопасности.

- ♦ Использование принципов поведенческой психологии для формирования кибербезопасного поведения, а не только знаний о нём. В том числе важным видится использование теории подталкивания (nudge theory) для уведомления пользователя о возможном риске в момент его возникновения.

- ♦ Оценка вероятности возникновения того или иного риска кибербезопасности для сотрудника в зависимости от профиля и характера его рабочей деятельности.

- ♦ Использование элементов и механик геймификации для вовлечения пользователя в обучающий процесс и поддержания интереса.

- ♦ Подобное решение позволит комплексно оценивать риски человеческого фактора на уровне каждого отдельного сотрудника и формировать у сотрудников устойчивые поведенческие паттерны, направленные на минимизацию этих рисков.

DeepFake. Методика синтеза изображения, видео, аудио или другой информации с помощью технологии искусственного интеллекта. Например, обучив нейронную сеть на фото или видео лица человека, можно создать крайне реалистичное видео с участием этого человека, где он говорит то, что в реальности никогда не говорил, или совершает действия, которые никогда не совершал. Изначально данная технология использовалась для генерации развлекательного контента, но на сегодняшний день уже зафиксирован целый ряд случаев, где дипфейки используются для мошенничества и других противоправных действий. Помимо этого,

Лабораторией кибербезопасности был проведён ряд исследований, демонстрирующих возможность обхода систем лицевой и голосовой биометрической аутентификации с использованием видео- и аудиодипфейков. По мере развития технологии и появления простых в использовании инструментов для создания дипфейков количество подобных случаев будет только расти, в связи с чем влияние данной технологии на ландшафт киберугроз оценивается как высокое.

Продвинутые виртуальные ассистенты (Advanced Virtual Assistants). Данная технология является естественным развитием технологии виртуальных ассистентов и чат-ботов, уже широко используемых сегодня, и подразумевает использование технологий искусственного интеллекта, в частности обработки естественного языка (Natural Language Processing) и глубоких нейросетей для понимания смысла запросов пользователей, ведения диалога, формирования прогнозов и помощи в принятии решений. Продвинутого виртуального ассистента, по определению Gartner, также должен включать возможность мультимодального взаимодействия с пользователями (голос, текст, графический интерфейс и т.д.). Уже сейчас виртуальные ассистенты «Салют» используются в большом количестве приложений как для клиентов, так и для внутреннего пользователя. По мере развития их возможностей, для которых потребуется доступ к различным системам и информации, масштаб угроз будет расти и виртуальный ассистент может стать важным вектором атаки на человека или информационную систему. Потенциальное влияние данной технологии на ландшафт киберугроз оценивается как высокое в силу широких возможностей применения в различных сферах деятельности и бизнес-процессах, что открывает новые возможности для атаки на бизнес и людей. Помимо этого, продвинутые виртуальные ассистенты могут быть использованы и в интересах кибербезопасности как удобный способ взаимодействия с сервисами и как канал оперативного информирования о состоянии различных аспектов кибербезопасности.

Поведенческая биометрия (Behavioral Biometrics). Технологии биометрической аутентификации, использующие в качестве фактора поведенческие характеристики человека, например голос, походку, рукописный или клавиатурный почерк. В отличие от статической биометрии, данные факторы могут оцениваться не только при входе в систему или приложение, но и на протяжении всего сеанса

По мере развития возможностей, для которых потребуется доступ к различным системам и информации, масштаб угроз будет расти и виртуальный ассистент может стать важным вектором атаки на человека или информационную систему

взаимодействия и при этом не требуют от пользователя совершения дополнительных действий для аутентификации.

Система может непрерывно оценивать соответствие поведения пользователя поведенческому биометрическому слепку и в случае существенного отклонения сигнализирует о возможной компрометации службе безопасности и/или блокирует доступ, что делает проблематичным перехват сессии пользователя злоумышленником. Подделка или компрометация поведенческих факторов и их использование без участия владельца на сегодняшний день представляется крайне сложной задачей. На данный момент промышленное применение поведенческой биометрии ещё не получило широкого распространения, и её используют в отдельных случаях, когда нужны дополнительные уровни аутентификации, например при проведении крупных транзакций или допуске к особо важным данным, но технология развивается, и в ближайшем будущем такие методы смогут значительно сократить риски в сфере безопасности.

Технологии удалённой работы (Remote Work Solutions). Из-за пандемии COVID-19 существенно выросло количество сотрудников, работающих удалённо, что сильно стимулирует развитие решений и технологий удалённой работы. При этом существенно меняется ландшафт угроз кибербезопасности, так как сотрудник уже не находится в пределах периметра с многослойной защитой, но при этом для выполнения своих рабочих обязанностей ему, как правило, требуется доступ к корпоративным системам и данным разной степени конфиденциальности. Скорее всего, развитие тренда на удалённую работу также подстегнёт кибербезопасность компаний к переходу от модели защиты периметра, внутри которого все доверяют всем, к модели нулевого доверия (Zero Trust), где доверие конкретному пользователю и устройству оценивается каждый раз при инициации соединения и на протяжении всего сеанса взаимодействия. Помимо этого, возрастает риск атаки с использованием имперсонации при удалённом взаимодействии. Поэтому влияние данного набора технологий на ландшафт киберугроз оценивается как высокое.

Bring Your Own Identity (BYOI). Концепция, упрощающая регистрацию и вход пользователей в новые сервисы, за счёт аутентификации через другой сервис, где пользователь уже зарегистрирован (например, Login with Google, Facebook, Apple ID, Сбер ID). С одной

Подделка или компрометация поведенческих факторов и их использование без участия владельца на сегодняшний день представляется крайне сложной задачей

стороны, такой подход существенно упрощает жизнь пользователям и улучшает пользовательский опыт, а также существенно уменьшает поверхность атаки на пользовательские данные, которые хранятся централизованно у одного identity-провайдера (IdP), а не в сотнях различных сервисов. Но, с другой стороны, IdP превращается в единую точку отказа, и компрометация IdP даёт злоумышленнику доступ к сразу десяткам, если не сотням, а в будущем, возможно, даже тысячам различных сервисов, вход в которые реализован через данного IdP (кража данных, кража личности, имперсонация). Также такой подход открывает возможность для кражи данных пользователя через мошеннический сервис или фишинговую атаку. Помимо этого, использование BYOI может упростить процесс создания реалистичных синтетических личностей с цифровым присутствием во множестве сервисов. По причинам, обозначенным выше, влияние данной технологии на ландшафт угроз кибербезопасности оценивается как высокое.

Беспилотные транспортные средства (Autonomous Vehicles). Транспортные средства, управляемые искусственным интеллектом без участия живого водителя, уже давно тестируются на дорогах общего пользования, а в ряде стран и регионов, в том числе и в некоторых регионах России, уже используются в режиме пилотной коммерческой эксплуатации. При этом массовое внедрение БПТС в коммерческую эксплуатацию существенно влияет на ландшафт угроз и открывает злоумышленникам новые возможности для атаки, например:

- ♦ взлом БПТС с целью угона, совершения преступлений или терактов — «ИИ-камикадзе»;
- ♦ получение несанкционированного доступа к системам управления интеллектуальной транспортной инфраструктурой или внесение нарушений в её работу может приводить к печальным последствиям — к ДТП, нарушению работы общественного транспорта, нарушению регулирования дорожного движения вплоть до полного транспортного коллапса, совершению терактов;



♦ также в связи с распространением применения беспилотных транспортных средств в военных целях возникает угроза их компрометации или перехвата. Это несёт в себе большую угрозу, чем атаки на гражданские беспилотники, так как злоумышленник получает доступ в том числе и к вооружению беспилотника.

В свете вышеперечисленного влияние технологий беспилотных ТС на ландшафт кибербезопасности оценивается как высокое.

Управление цифровым следом (Digital Footprint Management). Количество времени, проводимого человеком онлайн, как и среднее количество используемых им онлайн-сервисов, стабильно растёт из года в год и, скорее всего, продолжит расти и далее. Каждый пользователь оставляет всё больше и больше различной информации о себе, своих действиях и предпочтениях в посещаемых сервисах. При этом среднестатистический пользователь зачастую даже не представляет, какая информация о нём и в каком объёме хранится в том или ином сервисе. Более того, существенная часть этой информации может собираться и использоваться без его ведома и информированного согласия. Это открывает огромные возможности для злоупотребления этой информацией

как со стороны недобросовестных сервисов, так и со стороны злоумышленников, получивших несанкционированный доступ к ней. Что, в свою очередь, упрощает проведение атак на человека с использованием методов социальной инженерии, так как позволяет быстро завоевать доверие пользователя при атаке. Даже при наличии возможности управлять информацией о себе в отдельно взятом сервисе общее количество используемых сервисов и разрозненность хранимой информации делает эту задачу крайне сложной.

Это создаёт необходимость в разработке решений по управлению цифровым следом пользователя в сети Интернет, которые могут помочь в решении следующих задач:

- ♦ контроль и ограничение сбора информации о пользователе со стороны различных сервисов;
- ♦ централизованное хранение согласий на обработку информации о пользователе от различных сервисов с возможностью их отзыва;
- ♦ выявление источника утечки информации и своевременное уведомление пользователя о факте утечки.

Влияние данной технологии на ландшафт угроз кибербезопасности оценивается как высокое.

ТЕХНОЛОГИИ СО СРЕДНИМ УРОВНЕМ ВЛИЯНИЯ НА ЛАНДШАФТ КИБЕРУГРОЗ

Обучение с подкреплением (Reinforcement Learning). Один из способов машинного обучения, в ходе которого испытуемая система (агент) обучается, взаимодействуя с некоторой средой. Обратная связь от среды на действия агента формирует его поведение, итеративно обучая его оптимальным вариантам взаимодействия. Сама концепция была сформулирована в 1960-х годах, но развитие вычислительных мощностей и применение нейросетей существенно расширили возможности обучения с подкреплением, которое в наше время переживает «второе рождение».

Данная технология может быть использована в интересах кибербезопасности для обучения интеллектуальных агентов на выполнение различных задач по реагированию и расследованию инцидентов кибербезопасности, выявлению мошеннических транзакций и прочих. Но не стоит забывать, что обучение с подкреплением также может быть взято на вооружение злоумышленниками для проведения кибератак и их лёгкого масштабирования.

Умные бейджи (Smart Badges). Бейджи со встроенным вычислительным и запоминающим устройством для реализации дополнительных функций, например записи, транскрипции и диаризации диалога с клиентом, видеозаписи, геолокации, контроля выполнения рабочих обязанностей, связи с коллегами, получения инструкций и задач от руководителя. Технология умных бейджей уже развивается силами ряда технологических компаний. В зависимости от реализованных на бейдже модулей и их функционала возможны различные угрозы: кража или подмена данных (голос, видео), несанкционированный доступ к устройству для прослушки или отслеживания передвижения, имперсонация руководителя.

Паспорт здоровья (Health Passport). Данная технология позволяет в цифровом виде безопасно хранить и предъявлять по требованию подтверждённую информацию об иммунном статусе предъявителя в отношении различных заболеваний, а также другую информацию о состоянии здоровья, с возможностью её верификации и защитой от несанкционированной модификации. Развитие данной технологии существенно ускорила эпидемия COVID-19. Уже сейчас различные варианты паспорта здоровья используются во многих странах для

подтверждения иммунного статуса человека при получении доступа к различным мероприятиям и услугам, сопряжённым с физическим контактом с другими людьми.

Компрометация паспорта здоровья может приводить к различным нежелательным последствиям: подделка паспорта для получения привилегий, кража персональных данных (массовая — при централизованном хранении), неправомерный доступ к конфиденциальным данным, нарушение паспорта для отказа в привилегиях.

Искусственный интеллект на конечных устройствах (AI at Edge). Развитие технологий искусственного интеллекта и рост вычислительной мощности конечных устройств позволяет производить всё больше вычислений непосредственно на конечном устройстве, что позволяет увеличить скорость работы и уменьшить задержки. Соответственно, поверхность атаки на инфраструктуру перераспределяется в сторону от более защищённого ядра к более доступным для атак конечным устройствам. Помимо этого, миниатюрные устройства с производительным вычислителем на борту позволяют упростить и повысить эффективность слежки, так как ряд интеллектуальных функций может быть реализован на самом устройстве, например распознавание лиц и голосов, распознавание и транскрипция речи.

Управление идентификацией устройств (Machine Identity Management). Данный класс технологий подразумевает управления секретами и доступами устройств, приложений и сервисов. Распространение устройств, приложений и сервисов, взаимодействующих друг с другом без непосредственного участия людей, требует реализации функций управления секретами, доступами и полномочиями, защиты данных и самих устройств, и приложений по аналогии с тем, как это реализовано при взаимодействии человека с устройствами, приложениями и сервисами. При этом угрозы, реализуемые от эксплуатации или кражи «цифровой личности» устройства, по большому счёту такие же, как и в случае с человеком, в то время как признаки взлома или эксплуатации могут быть заметны человеку, но не будут «заметны» устройству или приложению.

Продвинутая видеоаналитика (Advanced Video Analytics). Технология, использующая методы компьютерного зрения для автоматизированного получения различных данных на

Технологии виртуальной реальности могут быть использованы для работы с конфиденциальными данными, снижая риск утечки через визуальный канал

основании анализа последовательности изображений, поступающих с видеокамер в режиме реального времени или из архивных записей. Развитие технологий искусственного интеллекта существенно упростило процесс автоматизированного анализа видеопотока и расширило его возможности. Уже сейчас технологии продвинутой видеоаналитики позволяют автоматически выявлять различные инциденты на видео, осуществлять быстрый поиск в обширном архиве записей нужных людей или событий по различным критериям (пол, возраст, цвет одежды, волос, кожи человека, совершаемые действия или движение, наличие определённых предметов или объектов и прочее).

Данные технологии существенно упрощают расследование инцидентов и преступлений сотрудниками физической безопасности и правоохранительных органов, но также могут быть легко использованы злоумышленником для быстрого сбора информации при планировании атаки в случае компрометации системы видеоаналитики.

ТЕХНОЛОГИИ С НИЗКИМ УРОВНЕМ ВЛИЯНИЯ НА ЛАНДШАФТ КИБЕРУГРОЗ

Сети мобильной связи пятого поколения (5G). Сети мобильной связи пятого поколения, активно внедряемые в ряде стран, обещают существенное увеличение скорости подключения и сокращение задержек при пересылке данных. Ряд компаний (аэропорты, крупные промышленные предприятия) рассматривают возможность использования частных 5G-сетей на своих объектах для обеспечения оперативной связи между сотрудниками, а также управления и автоматизации производственного процесса. В то же время с точки зрения кибербезопасности рост скорости подключения и количества подключённых устройств даёт злоумышленникам возможность создавать более масштабные бот-сети, в том числе и из 5G-IoT-устройств, а также реализовывать более масштабные DDoS-атаки. Уже сейчас существуют масштабные бот-сети из IoT-устройств (например, одна из самых известных сетей — Mirai), а доступность и скорость 5G только увеличит данную угрозу. Отдельно стоит отметить, что для обеспечения

обратной совместимости в сетях 5G могут использоваться устаревшие протоколы с давно известными уязвимостями, что может упростить работу злоумышленников по получению несанкционированного доступа к инфраструктуре сети.

Виртуальная и дополненная реальность (VR/AR). Виртуальная реальность подразумевает полное замещение реального окружающего пространства синтезированным, в то время как дополненная реальность — комбинацию объектов реального и виртуального мира.

Решения виртуальной и дополненной реальности в настоящее время нашли широкое применение в сфере развлечений. Также возможность их применения активно исследуется в сфере образования, промышленного производства, медицины и ряде других. Также AR/VR рассматривается как один из основных вариантов взаимодействия в метавселенной. Данная технология может быть применена в кибербезопасности для визуализации и анализа большого количества данных в трёхмерном пространстве, которые сложно визуализировать на двухмерном экране монитора. Также технологии виртуальной реальности могут быть использованы для работы с конфиденциальными данными, снижая риск утечки через визуальный канал, например, как описывается в патенте Apple — 3d document editing system.

Выявление усталости (Drowsiness Detection). Выявление усталости, как правило, реализуется за счёт мониторинга физиологических показателей и поведенческих маркеров усталости/сонливости. Может применяться на производствах и в процессах, где усталость или невнимательность работника несёт большие риски для безопасности или производственного процесса. Основной угрозой, реализуемой через эксплуатацию данной технологии, является умышленный или непреднамеренный саботаж производственного процесса (например, атака на модель-классификатор, подмена данных на входе или на выходе). Атака может реализовываться сторонним злоумышленником (с целью получения выгоды или саботажа) или даже самим работником (например, с целью максимизации заработка при почасовой оплате за счёт более продолжительного периода работы и сокращения перерывов на отдых). Также данная технология может найти применение и в работе отделов и ситуационных центров по кибербезопасности, так как внимательность аналитиков является важным фактором в расследовании инцидентов и противодействии им.



Технологии социального дистанцирования (Social Distancing Technologies). Для минимизации рисков заражения в период пандемии COVID-19 государственные органы и коммерческие организации по всему миру стремятся обеспечить соблюдение социальной дистанции между людьми. Для помощи в этой задаче возник целый спектр решений, использующих различные подходы: мобильные приложения, Bluetooth, носимые устройства, Wi-Fi или видеоаналитику. На данном этапе подобные решения показывают невысокую эффективность, но технологии развиваются дальше, чтобы закрыть растущую потребность. При этом использование подобных технологий создаёт целый ряд рисков приватности и кибербезопасности в случае их компрометации: раскрытие персональных

данных, несанкционированная слежка, сбор информации для подготовки к атаке и прочее. На данный момент в силу того, что пандемия COVID-19 пошла на спад и ограничения повсеместно снимаются, востребованность технологий социального дистанцирования снижается. Но вспышки новых заболеваний могут возродить к ним интерес, уже сегодня прогнозируются новые волны COVID-19, а также фиксируется распространение вируса обезьяньей оспы. Помимо этого, разработанные для социального дистанцирования методы и подходы могут быть востребованы в других сферах деятельности, в том числе и в военных целях (например, в системах свой — чужой).

(Продолжение в следующем номере)



НОВАЯ КНИГА МЕДИА ГРУППЫ «АВАНГАРД»

СТАЛИНГРАД И КРИПТОГРАФИЧЕСКИЙ ФРОНТ

Слово «СТАЛИНГРАД» стало символом. Символом высочайшего напряжения сил и самоотверженности, символом перелома во Второй мировой войне, символом грядущей Победы.

Победе в Сталинградской битве, как и всем крупным успехам антигитлеровской коалиции СССР, США и Великобритании, непременно предшествовали победы на незримом криптографическом фронте. Этот фронт борьбы за контроль над секретной информацией, передаваемой по каналам связи, в военные 1939–1945 годы

уже охватывал большую часть земной поверхности.

Эта книга посвящена творцам Победы, одержанной в напряжённой борьбе на криптографическом фронте.

Так сложилось, что укрепление позиций бойцов союзного криптографического фронта и поступательное развитие их успехов оказалось в значительной степени связанным со Сталинградской битвой и её временем. Отсюда особенное предпочтение авторов к этой эпопее.

Основой книги стали очерки, опубликованные известным историком

криптографии, кандидатом физико-математических наук Борисом Столпаковым в BIS Journal в 2018–2022 годах. Её иллюстративный базис составили документы Центрального архива министерства обороны РФ (ЦАМО), размещённые в преддверии 75-летия Великой Победы на интернет-портале «Память народа».

Книга выходит в издательстве «Медиа Группы „Авангард“» и продолжает серию «История криптографии». Приобрести книгу можно на мероприятиях «Медиа Группы „Авангард“» и в книжных магазинах.



Борис СТОЛПАКОВ
историк криптографии, кандидат
физико-математических наук

СТАЛИНГРАД 1942–1943

ПОБЕДА В СРАЖЕНИИ ЗА ИНФОРМАЦИЮ

Сталинград... Это слово хорошо знакомо всем нам ещё со школы, да и за пределами России оно широко известно. Именно в Сталинграде и на прилегающей к нему обширной территории свершился коренной и решительный перелом не только в Великой Отечественной, но и во всей Второй мировой войне. Долгожданный перелом был немалым без успехов как в защите собственной секретной информации, так и во вскрытии секретов связи противника.

ИЗ ОБОРОНЫ — В НАСТУПЛЕНИЕ

События Сталинградской битвы происходили, как известно, с середины июля 1942 г. по 2 февраля 1943 г. Вначале это было оборонительное сражение. Оно завязалось на подступах к городу, а затем, с 23 августа 1942 г., проходило и в самом Сталинграде. Именно в тот день произошла массированная бомбардировка города. Образовавшийся в результате пожаров гигантский огненный вихрь сжёг Сталинград. Уже к вечеру немецкие танки появились в километре от цехов тракторного завода. Это было лишь предвестие будущего противостояния, пока же бои шли в основном в городских предместьях.

Растянувшиеся на четыре месяца — июль–ноябрь 1942 г. — оборонительные бои Красной Армии сменились неожиданно для противника её контрнаступлением. Начавшись 19 ноября, оно привело к окружению немецких войск уже спустя четыре дня. Тогда кольцо окружения замкнулось в районе Калача-на-Дону. Ещё через 50 дней сильно ослабленный враг сдался.

ПЕРЕЗРЕВШАЯ ПРОБЛЕМА

Тернистым был путь связистов и фронтовых частей радиоразведки к такому успеху. В конце весны и начале лета 1942 г. радиоразведчики не имели возможности контроля за перемещениями крупных соединений противника, не смогли они вскрыть и разделение группы армий «Юг» на две новые группы — «А» и «Б». Первая из них продолжила наступление на Северный Кавказ, а целью группы армий «Б» стали Волга и Сталинград. В группу армий «Б» вошли 6-я армия Ф. Паулюса и 4-я танковая армия Г. Гота, а также две румынских, итальянская и венгерская армии, хорватский легион.

В период отступления от Харькова, с конца июня 1942 г., радиодивизионы ОсНаз находились в общем потоке отступавших войск. В создавшейся обстановке всё острее проявлялась общая недооценка использования армейских радиосредств. Эту проблему красноречиво иллюстрирует директива, подготовленная Главным управлением связи РККА.

Директива Ставки Верховного Главнокомандования командующим фронтами и 7-й отдельной армией — 24 июля 1942 г.

Опыт боёв показывает, что управление войсками у нас остаётся на недопустимо низком уровне. К сожалению, приходится снова отмечать, что основным видом связи большинство наших командиров продолжают считать проводную связь.

Управление войсками осуществляется до тех пор, пока существует проволочная связь, но стоит только нарушиться

проводной связи, как сразу же теряется и управление. Радиосредствами связи пользуются по-прежнему неохотно, вынужденно, о радиостанциях не заботятся, держат их далеко от командных пунктов, а иногда и при вторых эшелонах штабов. Подготовке радистов уделяется недостаточно внимания, радисты наши в большинстве работают медленно и слабо знают технику радиосвязи.

Потери связи — есть потеря управления, а потеря управления войсками в бою ведёт неизбежно к поражению.

Дальше такое положение не может быть терпимо.

Ставка Верховного Главнокомандования приказывает:

1. Под личную ответственность командиров и комиссаров всех степеней, в кратчайший срок устранить недооценку радиосредств связи в штабах, частях связи и у командно-политического состава частей и подразделений. При организации связи с войсками считать связь надёжной только в том случае, если имеется хорошо налаженная радиосвязь, и этому вопросу уделять первостепенное значение при организации любого вида боя или маневра войск. Свободное пользование радиосвязью на передачу допускать во всех случаях боевой деятельности войск, если не последовало запрещения вышестоящего начальника или штаба. Ограничение пользоваться радиосвязью на передачу производить только в периоды перегруппировки и сосредоточения войск.

2. Разрешить открытые передачи по радио в соединениях и частях от дивизии и ниже в следующих случаях:

а) при передаче команд по управлению огнём;



Иллюстрация 1. Мамаев курган и его окрестности

б) при передаче донесений с самолётов о наблюдаемых целях, передвижениях войск противника, целеуказаний при корректировании артиллерийского огня с воздуха;

в) всех команд в бою в танковых частях внутри рот, батальонов и бригад.

3. Разрешить радиообмен клером (открытым текстом — Б. С.) в армейском звене в следующих случаях:

а) донесения о получении приказов, о начале действий, достижениях определённых приказом районов и рубежей;

б) вызовы артиллерийского огня, авиации, танковых частей. При этом наименования частей и карту кодировать.

Все остальные передачи производить только шифром, в особенности боевые приказы.

4. В связи с разрешением открытых передач по радио облегчаются условия взаимной информации частей, но для этого в штабах от дивизии и выше

необходимо чётко организовать информационный радиоприём, а также создать условия взаимопонимания. Для этого нужно, чтобы штаб армии разработал единую кодированную карту и кодовую таблицу для всех частей и соединений, входящих в армию и имеющих рации.

5. Разрешение об открытых передачах по радио довести до сведения всего начальствующего состава и радистов всех раций. Командному составу строго вменить в обязанность делать на документе, подлежащем открытой передаче по радио, отметку, указывающую порядок передачи — «открыто», и ставить свою подпись.

6. К выполнению директивы приступить немедленно и об исполнении довести.

По поручению Ставки Верховного Главнокомандования
Василевский.

НАД МАМАЕВЫМ КУРГАНОМ

В сентябре бои шли в городе, часто уже в 150–200 метрах от берега Волги. Естественным центром борьбы среди городских руин стал Мамаев курган, поскольку с него можно было наблюдать и обстреливать большую территорию. На илл. 1 помещён снимок немецкой авиаразведки, сделанный над Мамаевым курганом. Обращённые в сторону Волги овражистые склоны кургана удерживались защитниками Сталинграда до победного завершения боёв.

В.И. Чуйков, командовавший 62-й армией, оборонявшей Сталинград, 13 сентября организовал там свой командный пункт. Но под вражеским огнём «...то и дело обрывалась проводная связь, радиоприём работал с большими и частыми перебойми <...> За весь день 13 сентября мне только один раз удалось поговорить с командующим фронтом».

СРАЖЕНИЯ НЕ ЗАТИХАЛИ НИ ДНЁМ, НИ НОЧЬЮ

Сражения на 20-километровой полосе вдоль Волги не затихали ни днём, ни ночью. Постепенно, в сентябре-ноябре, основные бои сместились в северную часть города — район рабочих посёлков и крупных заводов. Именно там располагались цеха Сталинградского тракторного (СТЗ), Красного Октября и завода Баррикады (илл. 2).

«КИЛОМЕТР БЫЛ ЗАМЕНЁН МЕТРОМ...»

Немецкий генерал Г. Дерр так вспоминал о характере войны в Сталинграде: «Километр как мера длины был заменён метром <...> Несмотря на массированные действия авиации и артиллерии, выйти за рамки ближнего боя было невозможно». Английский историк А. Кларк отмечал, что в Сталинграде «каждое сражение превращалось в схватку между отдельными людьми. Солдаты осыпали бранью противника на другой стороне улицы; они часто слышали дыхание врага в соседнем помещении, пока перезаряжали оружие; в густом дыму и кирпичной пыли шли рукопашные схватки на ножах и лопатах, с кирпичами и прутьями арматуры».

«К началу контрнаступления советских войск радиоразведка вскрыла группировку немцев и их союзников перед Юго-Западным, Донским и Сталинградским фронтами».

Для переговоров по радиосети
встречного взаимодействия Главное



№ 3989 СОВ. СЕКРЕТНО.

ТАБЛИЦА Приложение № 4

РАДИОСИГНАЛОВ ВЗАИМОДЕЙСТВИЯ НА ОПЕРАЦИИ СОГЛАСНО ДИРЕКТИВЫ Д-3. № 10.44. от 2.11.42.

УПРАВЛЕНИЕ	Сигнал	ДОНЕСЕНИЕ	Сигнал
Войти в прорыв и атаковать в направлении.....	258	1. Выходу в прорыв.....	165
Атаковать в направлении.....	342	2. Вышел тыл-противника район.....	666
Атаковать пехоту районе.....	556	3. Противник контратакует со стороны.....	175
Атаковать танки районе.....	558	4. Авиация противника бомбит район.....	122
Атаковать артиллерию в районе.....	421	5. Огонь артиллерии противника из района.....	184
Выслать истребителей прикрывать район.....	222	6. Противник отходит в направлении.....	555
Артиллерия открыла огонь по району.....	166	7. Резервы противника сосредоточены районе.....	568
Прекратить огонь по району.....	172	8. ТК/КК/атакует противника районе.....	536
Донесите обстановку и положение своих войск. Место-КП.....	145	9. ТК/КК/вышел рубеж № 1.....	267
Нала авиация бомбит район.....	111	10. Сигнал получен, выполняю.....	384
Прикрыть фланг в направлении.....	214	11. Несу большие потери.....	231
«Овернуть фронт наступления в направлении.....	338	12. Авиация вышла на прикрытие района.....	188
«Преследовать отходящего противника в направлении.....	444	13. Атака неудачна, повторяю.....	199
Закрепиться на достигнутом рубеже.....	255	14. Б/приказ №...получен.....	190
Перенести огонь вперед.....	328	15. Вышел рубеж.....	332
Продолжать выполнение задачи.....	623	16. Переходу новый КП пункт.....	223
Выйти и сосредоточиться в районе.....	283	17. ТК/КК/вышел рубеж № 2.....	315
Обозначьте свое положение.....	238	18. ТК/КК/вышел рубеж № 3.....	902

Иллюстрация 4. Таблица радиосигналов взаимодействия для Юго-Западного фронта

управление связи разработало и разослало в войска подробную инструкцию и специальную таблицу радиосигналов» (илл. 4).

САД-ДУБ «444»

Таблицу радиосигналов взаимодействия дополнили переданные вместе с ней позывные командования и частей, а также примеры их боевого использования.

«<...> 3. Порядок применения радиосигналов и позывных следующий:

а) Ком. ЮЗФ — Ком. 3 Гв. кав. корпуса; преследовать отходящего противника, направлении...; САД-ДУБ „444“

б) К-р 3 Гв. кав. корпуса — Команд. ЮЗФ: Сигнал „444“ получен, выполняю. ДУБ-САД „334“

в) название населённых пунктов по прилагаемой при сём кодированной карте».

ПО ДРУГУЮ СТОРОНУ ФРОНТА

Читатель может оценить осведомлённость и прозорливость разведки вермахта по доступному ныне документу, подготовленному отделом иностранных армий Востока Генштаба сухопутных войск 12 ноября 1942 г. Тогда этот отдел, представлявший собой оперативную армейскую разведку, возглавлял Р. Гелен.

«Отдел иностранных армий Востока. Штаб. 12.11.1942. Краткая оценка противника на 12.11.1942.

<...> Перед группой армий „В“ постепенно всё отчётливее вырисовывается намерение противника предпринять на участке союзных армий наступление, которое предполагалось уже ранее.

Наряду с обнаруженным сосредоточением двух ударных группировок перед флангами 3-й румынской армии, где,

- 4. 178

П. ДИСЛОКАЦИЯ РАДИОСТАНЦИЙ ШТАБОВ ПРОТИВНИКА ПО ДАННЫМ РАДИОРАЗВЕДКИ ПО СОСТОЯНИЮ НА 20.11.42 г.

Штаб командования арм. группы В	СТАРОБЕЛЬСЬК.
Штаб 6 армии	РИШИНО-ПАСНОЯРСКИЙ.
Штаб 8 армии	КРИВОМУЗГЕНСКАЯ.
2 эшелон Штаба 6 армии	ОСИОВКА.
Штаб 4 танковой армии	ВЕРХНЕ-КАРИЦКАЯ.
Штаб 3 армии румын	КОРСОЗОВСКИЙ.
2 эшелон Штаба 3 армии румын	ЧЕРНОВЕЦКАЯ.
Штаб 14 танк. корпуса	ТАРИНСКАЯ.
Штаб 14 танк. корпуса	КАРЛОВСКАЯ.
2 эшелон Штаба 14 танк. корпуса	ДЕРЕВНЯ Ш. РАЛ.
Штаб 48 танкового корпуса	КАЛОГАРОВАЯ.
Штаб 24 танкового корпуса	КАЛАЧ КУРТАКА.
Штаб 8 ак	БЕЛАНОВО.
Штаб 31 ак	ПЕСКОВАТКА.
2 эшелон штаба 31 ак	ГУЛРАТ.
Штаб неустановленного ак	КАЛО-НАВАТОВСКИЙ.
Штаб неустановленного ак	ЧЕРНОВЕЦКАЯ.
Штаб 5 ак румын	ПЕКАЛОВСКИЙ.
Штаб неустановленного ак румын	вис. 240 (20 км ю.в. Клетская).
Штаб неустановленного ак румын	ПЕКАЛОВСКИЙ.
Штаб 14 тд	ВОКОВСКАЯ.
Штаб 16 тд	ВЕРХНЕ-БУЗИНОВКА.
Штаб 24 тд	(сез.-вост. Орловка)
Штаб 3 мд	БАБАЕВО.
Штаб 20 мд	РАЙОН ОРЛОВКА.
Штаб 30 мд	ИГОЛНИ.
Штаб 71 пд	КУЛЬТСТАН.
Штаб 76 пд	РАЙОН ОРЛОВКА.
Штаб 79 пд	ВЕРТАЧИ.
Штаб 113 пд	ГОРОДИЩЕ.
Штаб 235 пд	НИЖНЕ-БУЗИНОВКА, подчиненные: ЛАТТЕВ, БОЛЬШАВАНТОВСКИЙ, ОСИНО-ЛОГОВСКИЙ (рации в движении).
Штаб 297 пд	ГУМРАК.
Штаб 305 пд	СИБЕЧКО.
Штаб 389 пд	РАЗУЛЬСКАЯ.
Штаб неустановленной пд	СТАЛИНГРАДСКИЙ.
	СВЯТЫНОВСКИЙ / 24 км южн. Клетская /.

Радиостанции 44 и 384 пд в работе не отмечены. Радиостанции 5 ак румын в движении на юго-восток.

21.11 отмечены в районе: вис. 240 (20 км юго-вост. Клетская), СВЯТЫНОВСКИЙ (23 км южн. Клетская), ВЕРХНЕ-БУЗИНОВКА.

Данными открытого перехвата, на Северном направлении установлено действие 63 артиллерии румын. (Требуется подтверждения)

Иллюстрация 5. Дислокация радиостанций штабов противника на 20.11.42

как надо полагать, противник уже готов к наступлению, растут признаки стягивания сил далее к западу, преимущественно в районе Калача (посёлок в Воронежской области — Б.С.), а также, возможно, и перед венграми. Общая картина группировки сил в отношении места, времени и их количества ещё не ясна. Признаков возможности наступления нет.

Оценка общих намерений противника при этой неясной картине представляется пока невозможной. Однако следует ожидать вскоре наступления против 3-й румынской армии с целью перерезать дорогу на Сталинград и тем самым поставить под угрозу находящиеся восточнее немецкие войска и добиться отвода немецких войска, расположенных под Сталинградом, чтобы снова овладеть водным путём по Волге. Для более крупных операций

имеющиеся у противника силы слишком малы <...>.

Пока ещё не ясно, можно ли ожидать крупного наступления через Дон против 8-й итальянской и 2-й венгерской армий — цель Ростов? — которое по времени последует после операции против 3-й румынской армии, или противник наряду с наступлением против 3-й румынской армии предпримет наступательные операции с ограниченной целью против 8-й итальянской и 2-й венгерской армий...»

20 ноября 1942 г. оценка положения на фронте отделом Р. Гелена стала более определённой.

«Развитие обстановки в полосе действий группы армий в течение сегодняшнего дня подтверждает сделанную нами ранее оценку противника как по целям, так и по использованию сил и средств (цель — выход к железной дороге Морозовск — Сталинград с одновременным нанесением удара южнее Бекетовки, чтобы уничтожить 6-ю армию или вынудить её отойти от Сталинграда). <...>

3-я румынская армия

Хотя обстановка в местах прорыва противника ещё окончательно не ясна, вполне вероятно, что назревает кризис крупного масштаба. Надо полагать, что для развития наступления в южном направлении будут введены ещё незадействованные силы из тыловых районов...»

РАДИОРАЗВЕДКА В ХОДЕ НАСТУПЛЕНИЯ

С начала операции «Уран» радиодивизионы постоянно контролировали перемещение штабов врага (илл. 5).

После 23 ноября, когда кольцо окружения сомкнулось, радиодивизионы сообщили о штабах противника, попавших в окружение, а затем следили за их передислокацией.

ПЛОДЫ ЛИШЬ ОДНОГО ДНЯ НА ОДНОМ НАПРАВЛЕНИИ

«На Городищенском направлении за 27.11.42 г. радиоразведкой установлено: работа радиостанции штаба 14 тк в ДМИТРИЕВКА (23.11 отмечалась в Бирючов); радиостанция из сети 14 тк, отмечавшаяся 23.11 в ИЛЛАРИОНОВСКИЙ, запеленгована

в НОВОАЛЕКСЕЕВСКИЙ; радиостанция корпусного типа, отмечавшаяся 22.11 в направлении КРАСНЫЙ ОКТЯБРЬ — ОРЕХОВО, запеленгована — АЛЕКСАНДРОВСКИЙ (25 км южн. Чернышевская); радиостанции танковых подразделений 14 тд запеленгованы: в районе 7 км юго-зап. ПЕСКОВАТКА, ЕРМОХИНСКИЙ (12 км вост. Нижне-Чирская), МОРОЗОВСКИЙ, ВЕРХНЕ-СОЛОНОВСКИЙ (23 км южн. Суровикино); радиостанция сети 16 тд, отмечавшаяся 23.11 в РЮМИНО-КРАСНОЯРСКИЙ, запеленгована в ЕРМОХИНСКИЙ; радиостанция штаба 3 мд, отмечавшаяся 24.11 в НОВО-АЛЕКСЕЕВСКИЙ запеленгована в районе отм. 135,0 (37 км северо-вост. Калач), подчинённые СТЕПАНО-РАЗИНСКИЙ (18 км юго-вост. Тормосин), ИЛЛАРИОНОВСКИЙ и в районе южнее отм. 135,0; радиостанции 60 мд — БОРОДКИН — КУЗЬМИЧИ; радиостанция штаба неустановленной пд, отмечавшаяся 24.11 в ПЕРЕПОЛЬНЫЙ, запеленгована в районе северо-зап. СОКОРЕВКА, её подчинённые в ДМИТРИЕВКА и в районе южнее ДМИТРИЕВКА; радиостанция штаба неустановленной пд в ЗАПАДНОВКА, радиостанция штаба неустановленной пд в районе вост. ПЕСКОВАТКА.

Впервые отмечены радиостанции: корпусного типа в РЕМОНТНАЯ (находится в связи с радиостанцией в Староминская (90 км юго-зап. Ростов), радиосеть 3 мд с главной — 6 км южнее Подсобное Хозяйство и подчинённые в БОЛ. РОССОШКА, ДМИТРИЕВКА, ЗАПАДНОВКА.

Радиостанция корпусного типа впервые запеленгована в ШАХТЫ.

В связи с аэродромами отмечена работа радиостанций 170 самолётов, из них: бомбардировщиков — 49, бомбардировщиков-разведчиков — 6, транспортных — 110, румынских — 4, неустановленного типа — 1. На аэродроме в районе хут. ГОНЧАРА отмечается первая штурмовая истребительная эскадра, ранее базировавшаяся в ТАЦЫНСКАЯ.

ВЫВОД: 1. Противник заканчивает вывод остатков дивизий

СИРОТИНСКОЙ группировки на левый берег р. Дон.

2. Продолжается перегруппировка войск противника в пределах внешнего обвода бывшего СТАЛИНГРАДСКОГО укреплённого района».

НЕ ДОПУСТИЛИ ДЕБЛОКАДУ

Донесение Маништейна в Генеральный штаб от 19 декабря 1942 г.

«Начальнику Генерального штаба сухопутных войск для немедленного доклада фюреру.

В связи с развитием событий в группе армий „Б“ и в связи с тем, что вследствие этого перерезаны пути подвоза новых сил, в группе армий „Дон“ создалось такое положение, что нельзя более рассчитывать на деблокаду 6-й армии в ближайшее время. <...> Продовольствия в „котле“ хватит ещё до 22 декабря. Заметно резкое истощение сил солдат (уже 14 дней они получают по 200 гр. хлеба). По сведениям командования армии, основная масса конского состава съедена или погибла от истощения».

9 января немцам предъявили ультиматум, на следующий день, 10 января, советские войска начали операцию «Кольцо». 2 февраля окружённый противник сдался.

ПОСЛЕ СТАЛИНГРАДА

Перемены в военной обстановке и немецком общественном мнении были восприняты германским руководством. По свидетельству генерала К. Типпельскирха, выступая незадолго до начала наступления на Курской дуге «перед лицами высшего командного состава, на которых возлагалось проведение операции, Гитлер заявил о своём твёрдом решении перейти к стратегической обороне. Германия, сказал он, должна отныне изматывать силы своих врагов в оборонительных сражениях, чтобы продержаться дольше, чем они; предстоящее наступление имеет целью <...> лишь выпрямление дуги, необходимое в интересах экономии сил <...> Основная мысль этих рассуждений вполне совпадала с точкой зрения военного руководства».

ТРИ ФРАГМЕНТА СТАЛИНГРАДСКОЙ ЭПОПЕИ

ИЗ ОБЩЕЙ КАРТИНЫ МНОГОДНЕВНЫХ БОЁВ ВЫДЕЛИМ
ЛИШЬ ТРИ ФРАГМЕНТА, СУЩЕСТВЕННО ПРИБЛИЗИВШИХ
ПОБЕДНЫЙ ИТОГ СРАЖЕНИЙ

ЗАДАЧА: ЗАБЛОКИРОВАТЬ ВРАГА С ТЫЛА

Важная роль в операции «Уран» принадлежала войскам Юго-Западного фронта. Они должны были заблокировать сталинградскую группировку врага с западного направления, с тыла.

Разведчики, в их числе 313-й радиодивизион ОсНаз, выяснили состав и расположение противостоящих сил противника. В его группировку входили более 20 дивизий, в основном румынских и итальянских. В плане операции учитывалась и возможная переброска дальних немецких резервов: «Танковая дивизия может появиться на второй день операции. При использовании автотранспорта немецкие пехотные дивизии могут появиться также на второй день операции и с утра третьего дня совместно с танковой дивизией принять участие в общем контрударе».

Во фронтовом плане операции особо отмечены меры по обеспечению секретности: «Использование радиосвязи до начала наступления запрещается. Штаб фронта подготавливает все документы по скрытому управлению и для взаимодействия; кодированные карты; таблицу радиосигналов».

КАК ПРЕОДОЛЕТЬ ДОН?

Существенной преградой для наступавших войск являлась и река Дон. Единственный мост через Дон в полосе наступления танковых корпусов (ТК) 5-й танковой армии Юго-Западного фронта располагался близ сталинградского Калача (точнее, Калача-на-Дону), лежащего на восточном берегу Дона.

Немцы отлично понимали значение этого моста. Для прикрытия подступов к нему при первых известиях о прорыве на фронте был создан плацдарм на западном, высоком берегу реки. Он был обращён фронтом на запад, в немецкий тыл, отсюда ожидался подход советских войск в направлении Калача. Мост подготовили к уничтожению. Но случилось так, что враг не сумел ни удержать мост, ни подорвать его.

ОТВЕТСТВЕННОЕ ЗАДАНИЕ

Приказ о скорейшем занятии переправы у Калача получил 26-й ТК генерал-майора А. Г. Родина. Корпус насчитывал около ста танков, в него входила и 14-я мотострелковая бригада подполковника Г. Н. Филиппова. Корпус Родина ввели в бой во втором эшелоне, вслед за стрелковыми дивизиями, обеспечившими прорыв румынской обороны. К полудню 20 ноября, преодолев две линии обороны противника и потеряв 30 танков, корпус вышел на оперативный простор и устремился к Калачу. По бездорожью, степи и оврагам. Погода была нелётная. Густая облачность, туманы и снегопад уберегли от атак вражеской авиации. 60-километровый бросок по тылам противника не вызвал существенных проблем, несмотря на встречавшиеся очаги сопротивления. К вечеру 21 ноября авангард корпуса завязал бой на главном рубеже обороны немцев у Калача. До переправы через Дон оставалось около 15 км.

Вечером подполковник Филиппов, кадровый офицер-дальневосточник, получил от командира корпуса отдельную

задачу: «Вам лично с двумя ротами мотопехоты и шестью танками во что бы то ни стало, любой ценой, захватить переправу через реку Дон и удерживать её до подхода частей корпуса». В состав отряда Филиппова вошли две роты мотострелкового батальона на грузовиках, пять танков и один бронеавтомобиль.

КОГДА ДЕЙСТВУЮТ СМЕЛЫЕ И... УМЕЛЫЕ

Согласно записи в журнале боевых действий, в 05:00 22 ноября отряд на полном ходу неожиданно «врезался в передний край обороны противника и внезапно так его ошеломил, что он, опомнившись, открыл огонь только после того, как проскочило три автомашины во главе с подполковником Филипповым, пять танков и бронемашина». Остальной части колонны пришлось принять бой. Прорвавшаяся часть отряда встретила местного жителя, он и показал дорогу к действующей переправе, построенной немцами и военнопленными. Обогнув с включёнными фарами немецкую зенитную позицию, танки и грузовики в 08:15 въехали на мост и захватили его вместе с прилегающей территорией, разогнав охрану.

На илл. 1 приведена немецкая фотография этого моста. На заднем плане можно видеть высокий западный берег Дона, отсюда прибыли бойцы Филиппова.

Отряд Филиппова закрепился на восточном берегу и уже в 10:00 попытался проникнуть в северную часть Калача, но был встречен огнём противника. После этого отряд немедленно



Иллюстрация 1. Мост у Калача-на-Дону, осень 1942 г.

оборудовал свою позицию и занял круговую оборону в ожидании подмоги. Под началом Филиппова состояли полторы сотни бойцов, пять танков и одна бронемашина.

РЕАЛЬНОСТЬЮ СТАЛО ПОЛНОЕ ОКРУЖЕНИЕ

Потеря переправы стала шоком для немецкого командования, это событие полностью изменяло оперативную обстановку. Ведь одновременно, начиная с 09:00 22 ноября, в штаб 6-й армии Паулюса стали поступать донесения о появлении советских танков с южного направления у посёлка Советский, это в 15 км восточнее Калача. Реальностью стало полное окружение 6-й армии.

Тем временем скопившиеся в Калаче обозы устремились к выезду из города в сторону Сталинграда. Всё же командование местного гарнизона решило мост пока не уничтожать, ввиду слабости противника и необходимости моста для нужд вермахта. Так, накануне на западный берег переправилась 24-я танковая дивизия, получившая приказ пресечь советское наступление.

Но сломить сопротивление дерзкого противника и вернуть мост немцам не удалось. Несмотря на непрерывающийся обстрел с обоих берегов,

бойцы Филиппова стойко держались под вражеским огнём. И выстояли! Хотя потеряли две трети своего состава. Передовые части 26-го ТК подошли к мосту около 20:00.

Вскоре штаб Юго-Западного фронта получил сообщение о захвате моста и немедленно отдал приказ переправить на восточный берег Дона 4-й ТК для развития наступления и соединения с войсками Сталинградского фронта.

Ещё ранее, в 19:00, из 6-й армии в штаб группы армий «Б» ушла шифрованная радиোগрамма, начинавшаяся словами: «Армия окружена». Хотя, как известно, кольцо окружения замкнулось на следующий день, 23 ноября. Тогда же 26-й ТК взял Калач.

«Я ПРЕДПРИМУ ВСЁ...»

Сплошного фронта окружения не было. Хотя общая протяжённость внешнего фронта превышала 450 км, фактически советскими войсками прикрывались лишь 270 км. При этом минимальное расстояние между внешним и внутренним фронтами составляло всего 15–20 км (в районе посёлка Советский, в 70 км от Сталинграда). Именно там противник мог нанести деблокирующий удар. Правда, новую линию обороны немцам ещё только предстояло



Иллюстрация 2. Г.Н. Филиппов (1902–1978)

создать. Пока же в их фронте была пробита брешь шириной свыше 300 км.

23 ноября Паулюс сообщил в Берлин: «Армия окажется в ближайшее время на краю гибели, если не удастся, сосредоточив все силы, нанести поражение войскам противника, наступающим с юга и запада. Для этого необходимо немедленно снять все дивизии из Сталинграда <...> Следствием этого должен быть прорыв в юго-западном направлении...». 24 ноября Гитлер приказал держаться: «Войска 6-й армии временно окружены русскими <...> Личный состав армии может быть уверен, что я предприму всё для того, чтобы обеспечить нормальное снабжение армии и своевременно освободить её из окружения...». Как мы знаем, Паулюс выполнил приказ и в результате спустя два месяца был вынужден капитулировать вместе с остатками своей армии.



Иллюстрация 3. Направления ударов немецких и советских войск

ПАМЯТИ ДОСТОЙНЫ

В 1955 г. неподалёку от места встречи танкистов Юго-Западного и Сталинградского фронтов появился памятник, посвящённый этому событию. Рядом с ним надпись на тумбе: «Потомки наши не забудут никогда величия духа и сказочной крепости русских солдат у берегов Дона и Волги...»

Геннадия Николаевичу Филиппову 14 февраля 1943 г. присвоили звание Героя Советского Союза, его 14-я мотострелковая бригада стала 1-й гвардейской, а 26-й танковый корпус 5-й танковой армии получил наименование 1-го гвардейского. Г. Н. Филиппов (илл. 2) ещё много лет посвятил воинской службе.

РЕЗУЛЬТАТ ПРЕВЗОШЁЛ ОЖИДАЕМОЕ

Первоначально советское командование считало, что под Сталинградом окружено менее 100 тыс. человек, а

ведь фактически попавших в «котёл» было более 300 тыс. Поэтому операция осложнилась и затянулась, ликвидация столь мощной группировки врага потребовала истощения его сил. Кроме того, необходимо было укрепить внешнее кольцо окружения и отразить деблокирующие удары противника.

ПЕРВЫЙ КАВАЛЕР ОРДЕНА СУВОРОВА

Аэродром в станции Тацинской благодаря радиоразведке, находился под постоянным вниманием советского командования. Этот крупный аэродром, близко расположенный к узловой железнодорожной станции в Ростовской области, стал базовым для снабжения окружённой армии Паулюса. И его захват или уничтожение стали одной из целей наступления войск Юго-Западного и Воронежского фронтов, известного как операция «Малый Сатурн». Такая задача была поставлена 24-му танковому

корпусу генерал-майора В. М. Баданова. Связь с командованием и с подчинёнными ему бригадами предполагалась по радио с использованием кодовых переговорных таблиц. Рейд корпуса начался с плацдарма в районе Верхнего Мамона на юге Воронежской области (илл. 3). Ныне именно там автомагистраль М-4 «Дон» преодолевает реку Дон.

Войдя 18 декабря в прорыв, пробитый войсками фронта в обороне противника, танковые подразделения 24-го корпуса вечером 23 декабря подошли к Тацинской, преодолев 240 км. Это за шесть дней постоянных боёв и под ударами немецких штурмовиков без авиационного прикрытия. Нелишне, вероятно, упомянуть и преодоленные снежные поля, и крепкие морозы. Манштейн был вынужден направить к Тацинской две танковые дивизии, но они не успели помешать танкистам Баданова. Утром 24 декабря



Иллюстрация 4. В. М. Баданов (1895–1971)

начался разгром немецких войск и тыловых частей в станице и на аэродроме, несмотря на их отчаянное сопротивление. Вот как в 1952 г. описал в немецкой газете бой на аэродроме в Тацинской бывший лётчик К. Шрайт: «Самолёты вспыхивали, как факелы <...> Со всех сторон на взлётную полосу выезжают и стартуют самолёты. Всё это происходит под огнём противника и в свете разгоревшихся пожаров. Небо распростёрлось багровым колоколом над тысячами погибающих солдат, лица которых выражали безумие. Вот один транспортный самолёт Ю-52, не успев подняться в воздух, врежется в советский танк и взрывается со страшным грохотом. Вот уже в воздухе сталкиваются „Хейнкель“ с „Юнкерсом“ и разлетаются на мелкие обломки вместе со своими пассажирами. Рёв авиадвигателей и танковых двигателей смешивается с рёвом взрывов, орудийным огнём и пулёмётными очередями, формируя чудовищную музыкальную симфонию».

На аэродроме и в Тацинской были уничтожены 46 самолётов, большое количество запасных частей, запасы боеприпасов, горючего и продовольствия. Чтобы доложить о выполнении боевой задачи, Баданов впервые за несколько дней связался по радио с командованием.

Уже 26 декабря 1942 г. за проявленные воинское мастерство, отвагу и мужество 24-й ТК стал 2-м гвардейским ТК и получил почётное наименование Тацинского. Тогда же Василий Михайлович Баданов (илл. 4) стал первым кавалером ордена Суворова, полководческой награды, учреждённой незадолго до этих событий.

Гвардейцы оказались в окружении с остатками боеприпасов и горючего. Оборону держали, используя трофеи. А проблему отсутствия горючего к своим танкам они решили, используя вместо дизельного топлива смесь авиационного бензина, керосина и масел. 28 декабря подразделения корпуса Баданова вышли из окружения и соединились с войсками фронта. Правда, к этому времени в строю осталась лишь десятая часть бойцов. При этом гвардейцы вывели за время операции более четырёх с половиной тысяч пленных. Результатом рейда танкистов Баданова в Тацинскую стало немедленное ухудшение снабжения окружённой армии Паулюса. Пригодные к использованию транспортной авиацией аэродромы отделились от блокированных войск ещё на 100 км, заодно возникли новые проблемы с прикрытием перевозок истребительной авиацией. Итог скоро стал ясен. 2 февраля окружённый противник сдался.

Я УБИТ ПОДО РЖЕВОМ...

Я убит подо Ржевом в безымянном болоте,
В пятой роте на левом, при жестоком налёте.
Я не слышал разрыва, я не видел той вспышки, —
Точно в пропасть с обрыва — и ни дна ни покрышки.
И во всём этом мире, до конца его дней,
Ни петлички, ни лычки с гимнастёрки моей...
Летом горького года я убит. Для меня —
Ни известий, ни сводок после этого дня.
Посчитайте, живые, сколько сроку назад
Был на фронте впервые назван вдруг Сталинград...
Удержались ли наши там, на Среднем Дону?..
Этот месяц был страшен, было всё на кону.
Неужели до осени был за ним уже Дон
И хотя бы колёсами к Волге вырвался он?
Нет, неправда. Задачи той не выиграл враг!
Нет же, нет! А иначе даже мёртвому — как?
И у мёртвых, безгласных, есть отрада одна:
Мы за родину пали, но она — спасена...»

Александр Твардовский

«Я УБИТ ПОДО РЖЕВОМ...»

Рассказ о Сталинградской эпопее будет неполон, если не упомянуть о наступлении советских войск на Ржев и Великие Луки с 24 ноября 1942 г. до середины января 1943 г. Тогда удалось сковать германские войска на Ржевско-Вяземском плацдарме и не допустить их переброски под Сталинград.

Этот удобный для немцев плацдарм (160 км в глубину, 200 км по фронту в 200 км от Москвы) возник зимой 1942 г. при отступлении врага после Московской битвы. 13 месяцев, с января 1942 г. до марта 1943 г., там располагались основные силы группы армий «Центр». Против них было сосредоточено до 30% всех боевых частей Красной Армии. Противостояние много раз переходило в кровавые наступления и контр наступления. Обстановку на этом участке фронта и её связь со Сталинградской битвой хорошо передают пронзительные строки Александра Трифоновича Твардовского.

Вскоре после завершения Сталинградской битвы, 2 марта 1943 г., германские войска сами оставили Ржев, а затем и весь Ржевско-Вяземский плацдарм, засвидетельствовав тем самым глубину свершившихся перемен.

ЧТО В ИМЕНИ ТЕБЕ МОЕМ?



Александр ИГОНИН
эксперт BIS Journal

Мне всегда очень импонировал армейский способ организации порядка, когда всё одинаковое, зелёное и квадратное — как говорится, «пострижено, покрашено и засеяно песком». При многих своих очевидных недостатках такой подход имеет и плюсы, особенно хорошо заметные в большой корпоративной среде. В этой статье хотелось бы остановиться на вопросе выбора имён/идентификаторов для различных сущностей.

Практически в любом крупном SOSe есть набор однотипных объектов, счёт которым идёт на сотни, если не на тысячи. Самый яркий пример — правила корреляции в SIEM, хотя то же самое справедливо и для её коннекторов/агентов, отчётов и так далее. И довольно часто (по крайней мере, в моей практике) приходится отвечать на типовые вопросы, как то:

- ♦ а сколько у нас всего правил корреляции?
- ♦ сколько из них работают (или, по крайней мере, должны работать), а сколько — тестируются или выведены из эксплуатации?
- ♦ сколько из них непосредственно генерируют алерты, а сколько выполняют вспомогательные функции?
- ♦ на каких источниках событий (логах) основаны эти правила?
- ♦ какой тактике/технике MITRE соответствуют эти правила?
- ♦ к какому типу (по различным классификациям) относятся эти правила?
- ♦ и так далее и тому подобное...

Ваш покорный слуга регулярно получал большинство из перечисленных выше вопросов либо от руководства, либо от аудиторов. Первоначально для поиска ответа приходилось каждый раз искать/придумывать ключевые слова для фильтрации этого списка в «Экселе», а затем сводить результат в единый отчёт. Очень быстро проявились побочные эффекты такого способа: покраснение глаз, боль в голове, долгое время выполнения запроса, ненависть к аудиторам. Спустя некоторое время нашлось простое, но оказавшееся очень эффективным решение: выработать единую конвенцию именования правил и воплотить её в жизнь.

Затраты на мероприятие: два совещания для брейншторминга, пара дней на составление списка «старое имя — новое имя», а также несколько недель на собственное переименование правил в SIEM (как выяснилось, массовое переименование правил может сносить ей крышу, так что пришлось это делать небольшими пачечками).

Для примера приведу вариант схемы имени правила (разумеется, список полей будет уникальным для каждого SOC'a — их надо подбирать под себя):

```
PRD-client_1-0123-042-P1-AD-TA0006-T1056,  
T1556-Login Page Code Changed  
DEV-client_2-0124-000-P2-Windows, Unix—High  
CPU Utilization Detected.
```

Как видно, схема очень проста:

- ♦ между различными полями используем одинаковый разделитель (в нашем случае это дефис);
 - ♦ если поле пустое, то этот разделитель всё равно сохраняем на месте;
 - ♦ если в поле нужно дописать более одного значения, то используем внутрипольный разделитель (в примере это запятая);
 - ♦ вводимые в поле данные не должны содержать приведённые выше разделители.
- Некоторые примеры полей:
- ♦ тип правила (генерирует алерты / вспомогательное / в разработке / выведено из эксплуатации);
 - ♦ клиент/подразделение, в интересах которого работает правило (либо же «глобальное», если работает для всех);
 - ♦ уникальный числовой идентификатор правила;
 - ♦ версия правила (счётчик, увеличивается на 1 после каждого изменения);
 - ♦ приоритет (удобно для построения квадратно-гнездового SOCa на раннем этапе зрелости, когда приоритет алерта ещё не получилось сделать динамическим);
 - ♦ источник(и) событий для правила;
 - ♦ тактика(и) и техника(и) MITRE;
 - ♦ имя правила.

После того как все правила переименованы, экспортируем полный список в «Эксель», разбиваем на колонки, используя выбранный разделитель, исправляем обнаруженные ошибки. Когда все ошибки исправлены, у нас получается несколько громоздкие, но удивительно удобные для построения разнообразнейших отчётов имена. Если вы такое ещё не внедрили, задумайтесь!

Конференция

Кадры и образование по ИБ в России: настоящее и будущее



РЕГИСТРАЦИЯ

Соорганизаторы:



Минцифры
России



Университет
Сириус



positive
technologies

infotecs

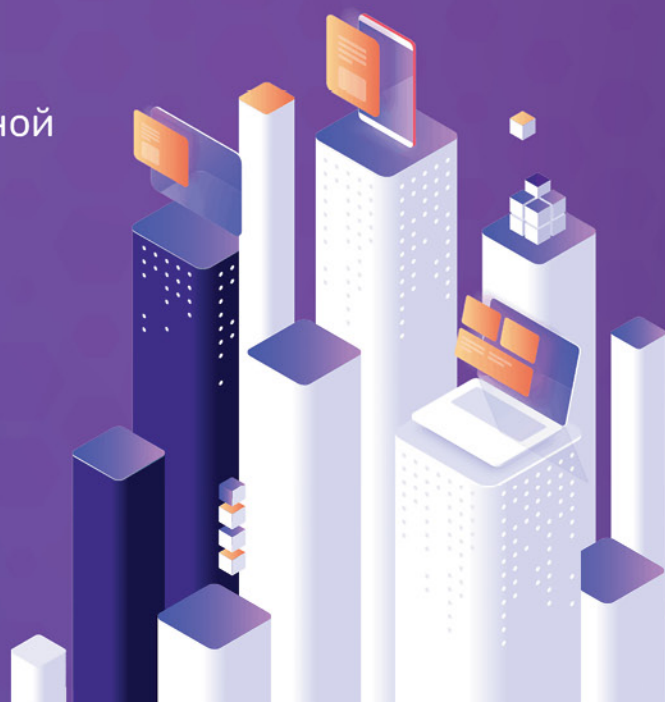
Обсуждаемые вопросы:

- ✓ Развитие компетенций по ИБ для инженерных специальностей
- ✓ Система непрерывного образования в области ИБ.
Где граница между СПО, ВО и ДПО?
- ✓ Инфраструктура для практикоориентированной подготовки специалистов: профильные лаборатории, онлайн-платформы, физические и виртуальные полигоны и др.
- ✓ Стратегия государства по развитию кадров отрасли ИБ.
Потребности рынка труда vs Профессиональные стандарты
- ✓ Национальная система сертификации и аттестации кадров по ИБ

Целевая аудитория:

Представители органов государственной власти, профильные вузы и учебные организации, компании-разработчики и интеграторы по ИБ, предприятия различных отраслей экономики

9–11 марта 2023 года
Федеральная территория
«Сириус»



Kaspersky Symphony XDR



Новое звучание технологий
киберзащиты



kaspersky АКТИВИРУЙ
БУДУЩЕЕ

