

BIS

JOURNAL

ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ
БИЗНЕСА

№2 (57) 2025

**Игорь
ШЕРЕМЕТ**
РАН
К независимости
без изоляции
→ 38



**Василий
ПИСКАРЕВ**
Госдума
«Мы работаем!»
→ 48



**Защита данных.
Все только
начинается...**

→ 4-37

**Три кита РБПО.
1. Статический
анализ**

→ 72-84



**Елена
БУТКОВА**
Мингосуправления
Московской
области
«Даю согласие на
обработку...» → 8



**Дмитрий
ПОНОМАРЕВ**
ООО НТЦ
«Фобос-НТ»
Испытания
статических
анализаторов → 72



**Андрей
ЖАРКЕВИЧ**
Start X
Анатомия
корпоративного
конфликта → 85



КОНСОРЦИУМ
ИССЛЕДОВАНИЙ
БЕЗОПАСНОСТИ
ТЕХНОЛОГИЙ
ИСКУССТВЕННОГО
ИНТЕЛЛЕКТА

20.05.2025

МОСКВА, КЛАСТЕР «ЛОМОНОСОВ»

III ФОРУМ

ТЕХНОЛОГИИ ДОВЕРЕННОГО ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

РЕГИСТРАЦИЯ

ib-bank.ru/trust-ai



ОРГАНИЗАТОРЫ

ПРИ ПОДДЕРЖКЕ



Национальный
технологический центр
цифровой криптографии



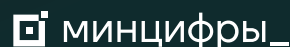
Институт системного
программирования
им. В.П. Иванникова РАН



Академия криптографии
Российской Федерации



Медиа Группа
«Авангард»



Министерство цифрового
развития, связи и массовых
коммуникаций РФ



Сергей ПАЗИЗИН
научный редактор
BIS Journal

В связи со вступлением в действие 30 мая 2025 года закона «Об оборотных штрафах» за утечку информации (ФЗ от 30.11.2024 № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях») кардинально ужесточается ответственность за действия и бездействие, повлекшие за собой утечку персональных данных. Это серьезный повод для компаний пересмотреть свое отношение к защите данных — проанализировать слабые места и выйти на новый уровень зрелости в части обеспечения безопасности информационных ресурсов.

В данном номере мы подробно рассмотрим изменения в законодательстве о защите персональных данных и предоставим возможность экспертам высказать свое мнение по данному вопросу. Расскажем о необходимости инвентаризации данных, комплексном подходе к обеспечению безопасности информации и используемых технических средствах.

В нашей постоянной рубрике о разработке безопасного программного обеспечения проинформируем о проводимых под патронажем ФСТЭК России испытаниях открытых и коммерческих отечественных статических анализаторов исходных кодов компилируемых и динамических языков программирования. Целью указанных испытаний является оценка технологических возможностей анализаторов в соответствии с требованиями ГОСТ Р 71207-2024 в части полноты обнаружения критичных дефектов, количества ложных срабатываний, поддерживаемых методов анализа и потребности в ресурсах. Читатель познакомится с планом этих испытаний и их основными участниками. Информацию о применяемых техниках тестирования и результатах будем публиковать на страницах журнала по мере поступления.

Также в целях повышения эффективности взаимодействия и обмена опытом между научным и практическим направлениями в сфере обеспечения информационной безопасности мы начинаем сотрудничество с журналом «Вопросы кибербезопасности», занимающим ведущие позиции в области публикации научных результатов. Планируем в дальнейшем обмениваться с коллегами рефератами наиболее интересных статей и новостными материалами.



BIS JOURNAL

ИЗДАЁТСЯ С 2010 ГОДА

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Батранков Д. В. — директор по продуктам ИБ ИКС Холдинг
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 «ЦНИИХМ»

Вихорев С. В. — советник генерального директора ООО «Умные решения»

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. — управляющий директор Центра информационной безопасности дочерних и зависимых обществ Газпромбанка (АО)

Курило А. П. — советник по вопросам ИБ ФБК и FBK CyberSecurity, кандидат технических наук

Левиев Д. О. — председатель Совета НП «Партнёрство 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

Одудалов М. В. — директор службы Управления по обеспечению информационной безопасности ДБ Банка ВТБ (ПАО)

Окулесский В. А. — вице-президент по информационной безопасности ЦМРБанка, кандидат технических наук

Пазизин С. В. — заместитель начальника Управления по обеспечению информационной безопасности ДБ Банка ВТБ (ПАО), кандидат физико-математических наук, научный редактор журнала

Сабанов А. Г. — главный эксперт Научно-технического комплекса технологий информационного общества АО «НИИАС», доктор технических наук

Филипчук А. А. — руководитель Службы архитектуры, УК Деметра Холдинг

Хайретдинов Р. Н. — заместитель генерального директора ГК «Гарда»

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

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И. В.**

Коммерческий директор: **Минаков А. В.**

Директор по развитию: **Абрамов А. В.**

Арт-директор: **Мельников Н. С.**

Обозреватели: **Оздемиров У. У., Покатаева Е. Н.**

Иллюстрация на обложке: **Виктор Миллер Гаусса**

Фото в номере: **Freerik**

Цветокорректор: **Наumenko М. В.**

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-bank.ru/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) как «BIS Journal — Информационная безопасность банков».

Зарегистрирован 11 июля 2023 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) как «BIS Journal — Информационная безопасность бизнеса». Свидетельство ПИ № ФС77-85487 от 11.07.2023 г.

Все права на материалы, опубликованные в номере, принадлежат журналу «BIS Journal — Информационная безопасность бизнеса». 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 21.03.2025. Тираж 7000 экз.

Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

ТЕМА НОМЕРА: ЗАЩИТА ДАННЫХ

- 4 Илья Башкиров (ГК InfoWatch)
Изменения в регулировании ПДн и оборотные штрафы
- 8 Елена Буткова (Министерство государственного управления, информационных технологий и связи Московской области)
«Даю согласие на обработку...»
- 10 Александр Горбачев (Инфосистемы Джет)
Миф или реальность?
- 12 Сергей Добрушский (Сайберпик)
Платформенный подход к защите данных
- 14 Алексей Парфентьев (СёрчИнформ)
Прививка от оборотных штрафов
- 16 Денис Суховей, Анна Горшкова (Аладдин Р.Д.)
Как не допустить оборотных штрафов за утечку персональных данных
- 17 Дмитрий Слободенюк (ARinteg)
Как ARZip помогает...
- 18 Василий Севостьянов (Доктор Веб)
Защита данных и противостояние киберугрозам
- 21 Роман Душков (Security Vision)
Защита данных как работа оркестра
- 23 Вячеслав Половинко (АМТ-ГРУП)
Между доменами
- 25 Николай Перемышленников (эксперт BIS Journal)
Об усилении ответственности за нарушение порядка обработки ПДн
- 30 Андрей Жаркевич (Start X)
Цугцванг по-русски
- 34 Сергей Петренко (UserGate)
«Кибербез перестал быть чем-то кулуарным и становится частью жизни»
- 36 Кирилл Зюбанов (Wildberries и Russ)
**Wildberries и Russ:
«Персональные данные – не товар»**

ИНТЕРВЬЮ НОМЕРА

- 38 **Цифровые прорывы**
Игорь Шеремет (Научный совет РАН «Информационная безопасность»)
К независимости без изоляции
- 46 **Содружество ИБ**
Алексей Марков (журнал «Вопросы кибербезопасности»)
BIS Journal – «Вопросы кибербезопасности»: диалог друзей

РЕГУЛЯТОРЫ

- 48 **Госдума**
Василий Пискарев (Государственная Дума РФ)
«Работаем над тем, чтобы сделать эффективнее борьбу с киберпреступниками и телефонными мошенниками»
- 50 **Парад законов**
Екатерина Рачкова (BIS Journal)
Квартальный отчет
- 53 **Есть мнение**
Сергей Вихорев (Умные решения)
Школа балльных танцев, Вам говорят...

УГРОЗЫ И РЕШЕНИЯ

- 56 **Банки**
Вероника Горячева (BIS Journal)
Под шквалом яростных DDoS
- 58 **Attack Surface Management**
Николай Степанов (F6 Attack Surface Management), Владимир Соловьев (ДиалогНаука)
Если не контролировать свой периметр, его будут контролировать другие
- 61 **Модель угроз**
Дмитрий Слободенюк (ARinteg)
Конструктор-У
- 62 **Импортозамещение**
Михаил Иванов (С-Терра СиЭсПи)
«Мы создаём продукт, который отвечает вызовам времени»

УГРОЗЫ И РЕШЕНИЯ

- 64 **On-premise**
Сергей Андриенко (Servicerpipe)
Локальная защита от ботов – реальность или утопия?
- 66 **Маркетинг**
Татьяна Белей, Елена Шедова (S&Bi Group)
Продукт, понятный и нужный рынку

ИНФРАСТРУКТУРА

- 68 **Деловые мероприятия**
Усам Оздемиров (BIS Journal)
«Цифровая устойчивость промышленных систем – 2025»

РБПО. СТАТИЧЕСКИЙ АНАЛИЗАТОР КОДА

- 72 Дмитрий Пономарев (НТЦ Фобос-НТ)
Испытания статических анализаторов
- 75 Андрей Белеванцев (ИСП РАН)
Svace
- 76 Дмитрий Шмойлов (Kaspersky)
Статические анализаторы в коммерческой разработке
- 77 Виталий Вареница (НПО Эшелон)
Анализатор кода вычислительных систем АК-ВС 3
- 80 Роберт Арустамян, Нелли Магакелова, Илья Антипов (НПО Эшелон)
Как работают инструменты статического и динамического анализа кода
- 83 Михаил Гельвих (ПВС)
Сертификация ПО
- 84 Антон Башарин (AppSec Solutions)
Пилот, чтобы SAST «летел» в пять раз быстрее

КИБЕРКУЛЬТУРА

- 85 **ИБ и бизнес**
Андрей Жаркевич (StartX)
Почему безопасники не хотят закрывать таски
- 88 **Open Source Intelligence**
Дмитрий Кузеванов (UserGate)
«OSINT не станет оружием киберпреступников, если мы будем лучше осведомлены»
- 90 **OS Windows**
Ярослав Прокушев (Банк ВТБ)
Без дополнительных средств

ЗА РУБЕЖОМ

- 94 **Обзор ИноСМИ**
Усам Оздемиров (BIS Journal)
Утечки персональных данных
- 98 **Законодательство**
Александр Виноградов (ФГУП «ЦНИИХМ»),
Сергей Меншиков (Belarusian InfoSecurity Community),
Андрей Ситнов (независимый эксперт), Наталья Казанцева (независимый эксперт)
Республика Узбекистан
- 103 **Китай**
Мария Козлова (BIS Journal)
«Так похоже на Россию...»

СУБЪЕКТЫ

- 108 **Книги**
Владимир Матюхин (Академия криптографии России)
«Эхо эфира Победы»
- 110 **История**
Борис Столпаков (историк криптографии)
Победу приближали как могли и за ценой не стояли
- 116 **Заметки безопасника**
Александр Игонин (BIS Journal)
Заветные 0,1 %

ИЗМЕНЕНИЯ В РЕГУЛИРОВАНИИ ПДН И ОБОРОТНЫЕ ШТРАФЫ

КАК ПОДГОТОВИТЬСЯ И СНИЗИТЬ РИСКИ



**Илья
БАШКИРОВ**
юрист по ИБ
ГК InfoWatch

В 2025 году кардинально ужесточается ответственность за утечку и неправомерное использование персональных данных (ПДн) граждан. Нормы законов, предусматривающие уголовную ответственность за незаконное использование ПДн, действуют уже с 11 декабря 2024 года, с 30 мая 2025 года начнут применяться оборотные штрафы для компаний. Главная цель нового регулирования — снизить количество утечек данных, которые стали источником множества угроз для бизнеса и потребителей, включая различные виды мошенничества и социальную инженерию. Каким образом компаниям, которые оперируют ПДн, подготовиться к нововведениям и снизить риски?

КАКИЕ ЗАКОНЫ ПРЕДУСМАТРИВАЮТ НОВОЕ РЕГУЛИРОВАНИЕ

Изменения в регулирование обработки ПДн вводят два основных до-

кумента, которые были утверждены Президентом России 30 ноября прошлого года.

Первый из них — это **федеральный закон № 420-ФЗ от 30.11.2024 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (КоАП РФ)**. Этот документ ужесточает ответственность за нарушения при обработке (в т.ч. хранении) ПДн, вводит новые формы штрафов, новые составы правонарушений и вместе с этим предусматривает новые способы уменьшения размера ответственности.

Второй нормативный акт — **федеральный закон № 421-ФЗ от 30.11.2024 «О внесении изменений в Уголовный кодекс Российской Федерации» (УК РФ)**. Документ предусматривает ответственность за получение ПДн без установленных законом оснований, а также за неправомерный доступ к ним, меняет структуру рисков, на которые ранее ориентировались специалисты по информационной безопасности.

Вступают в силу эти законы в разное время. В частности, уголовная ответственность за незаконное использование ПДн действует уже с 11 декабря 2024 года. Штрафы за допущение утечек данных, нарушение обработки ПДн и отсутствие уведомления Роскомнадзора о факте утечки будут применяться с 30 мая 2025 года. Второй пункт для бизнеса более трудоемкий с точки зрения

организационных мер — к 30 мая компаниям необходимо провести тщательную проверку внутренних документов, которые регулируют порядок обращения с ПДн, направить в Роскомнадзор уведомление об их обработке и провести аудит средств защиты информации.

Замечу, что новое регулирование в сфере ПДн призвано не только напомнить об угрозах, которые несет в себе недобросовестное обращение с ПДн, но и мотивировать бизнес переходить на новый уровень цифровой зрелости и пересматривать подход к защите данных внутри компании. Предположу, что с принятием новых законов в этом направлении надзор будет усилен, поэтому повышение защищенности информации и внедрение новой системы оценки рисков уже сейчас стали для бизнеса приоритетным вопросом.

ФЗ №421: ОСНОВНЫЕ ИЗМЕНЕНИЯ В УГОЛОВНЫЙ КОДЕКС РФ

Изменения, которые вводит ФЗ № 421, выглядят следующим образом:

- ♦ вводится статья 272.1 УК РФ — ответственность за использование ПДн, полученных незаконным путем, включая сбор без согласия субъекта или за рамками такого согласия;
- ♦ в УК РФ вводятся 6 новых составов преступления, ответственность по ним — до 10 лет лишения свободы;
- ♦ нарушение неприкосновенности частной жизни (ст. 137 УК РФ) теперь

отделено от сбора ПДн без законного основания. Таким образом, могут измениться подходы к проверке сотрудников, контрагентов и другие внутренние процедуры, которые опирались на привычную практику, сформированную применением статей УК РФ и ФЗ «О персональных данных».

♦ новая статья УК РФ 272.1 описывает ответственность за неправомерное использование незаконно полученных ПДн. Помимо общих для уголовного права отягчающих обстоятельств более тяжкие составы предусмотрены за незаконное использование ПДн специальных категорий (сведения о здоровье, расовой принадлежности, политических взглядах и т.д.), данных несовершеннолетних, биометрии и незаконную трансграничную передачу ПДн. В случае причинения тяжких последствий или совершения преступления организованной группой максимальная ответственность — лишение свободы на срок до 10 лет и штраф до 3 млн руб.

Стоит обратить внимание, что в новой статье нет конкретики об использовании ПДн, и это значит, что офицерам безопасности предстоит оценить все существующие в компании практики использования ПДн с точки зрения потенциальных рисков. Например, при проверке контрагентов и сотрудников, поиске по открытым источникам и так далее.

В свете нововведений компаниям важно провести внутренний аудит с точки зрения разграничения ответственности и в целом внутреннего регулирования доступа к ПДн: какой доступ и у каких сотрудников есть, как он зафиксирован в документах организации, какие полномочия предусмотрены. Также обязательно нужен локальный нормативный акт, который определяет компетенции сотрудников ИБ и сотрудников служб безопасности по использованию ПДн. Рассматривать нововведения как прямую угрозу сотрудникам ИБ и СБ не стоит, но изменение регулирования наверняка потребует пересмотра отдельных бизнес-процессов.

Увеличение штрафов

по уже существовавшим нарушениям

НАРУШЕНИЕ	СЕЙЧАС рублей	БУДЕТ рублей
Нарушение цели и объема обработки ПДн (ч.1)	Для ЮЛ от 60 000 до 100 000	Для ЮЛ от 100 000 до 300 000 Для ФЛ от 5 000 до 10 000 Для должностных от 50 000 до 100 000
Повторное нарушение цели и объема обработки (ч.1.1)	Для ЮЛ от 60 000 до 100 000	Для ЮЛ от 300 000 до 500 000 Для ФЛ 15 000 до 30 000 Для должностных от 100 000 до 200 000
Неуведомление РКН об намерении обрабатывать персональные данные	Для ЮЛ 5 000 (ст. 19.7 КоАП)	Для ЮЛ от 100 000 до 300 000 Для ФЛ от 5 000 до 10 000 Для должностных от 30 000 до 50 000
Неуведомление РКН об утечке	Для ЮЛ 5 000 (ст. 19.7 КоАП)	Для ЮЛ от 1 млн до 3 млн Для ФЛ от 50 000 до 100 000 Для должностных от 400 000 до 800 000

Рисунок 1. Как вырастут штрафы за нарушение цели и объема обработки ПДн, а также отсутствие уведомления Роскомнадзора

ФЗ №420: УВЕДОМЛЕНИЯ РКН, ШТРАФЫ И ОСНОВНЫЕ ИЗМЕНЕНИЯ В КОАП РФ

Изменения, которые вводит ФЗ № 420, выглядят следующим образом:

♦ увеличиваются все размеры ответственности вплоть до оборотного штрафа (1–3 % от всех доходов компании);

♦ вводятся 9 новых составов правонарушений (части 9–18 ст. 13.11 КоАП РФ);

♦ меняется подход законодателя к нарушениям в сфере ПДн, усиливается значимость обеспечения ИБ для организации;

♦ увеличивается ответственность за неуведомление Роскомнадзора о начале обработки данных;

♦ повышается важность внутреннего расследования инцидентов ИБ.

А теперь разберем их подробнее. По тем нарушениям, которые были предусмотрены в законодательстве раньше, ФЗ № 420 повышает размер штрафов, предусмотренных статьями 13.11 КоАП РФ. В частности, за

нарушение цели и объема обработки ПДн максимальная сумма штрафа для юридических лиц выросла до 300 тыс руб., за повторное нарушение — 500 тыс руб. (ранее сумма была 100 тыс руб.).

Из новшеств появились штрафы за то, что организация не уведомила Роскомнадзор о своем намерении обрабатывать ПДн, — сумма штрафа от 100 до 300 тыс руб. Такое уведомление компания обязана направлять в ведомство заблаговременно. Форма такого уведомления закреплена на сайте Роскомнадзора. Важный нюанс, который стоит учесть: если речь идет о группе компаний или другой корпоративной структуре, где несколько юрлиц работают с ПДн, то уведомление должно быть направлено от каждой компании, которая попадает под определение оператора ПДн, приведенное в п. 2 ст. 3 ФЗ «О персональных данных». Это связано с тем, что по закону о ПДн оператором ПДн является индивидуальное юридическое лицо.

Нововведение — ответственность за утечку:

Часть ст. 13.11 КоАП	Утечка	Штраф (для ЮЛ)
12	От 1 000 до 10 000 субъектов От 10 000 до 100 000 идентификаторов	→ От 3 млн до 5 млн руб.
13	От 10 000 до 100 000 субъектов От 100 000 до 1 млн идентификаторов	→ От 5 млн до 10 млн руб.
14	Более 100 000 субъектов Более 1 млн идентификаторов	→ От 10 млн до 15 млн руб.
15	Повторное совершение одного из нарушений, предусмотренных частями 12-14 КоАП – то есть повторная утечка данных от 1 000 субъектов / 10 000 идентификаторов	→ Штраф в размере от 1 до 3 процентов от дохода за год, либо от собственных средств кредитной организации (но не менее 20 и не более 500 млн)
16	Утечка ПДн специальной категории	→ От 10 млн до 15 млн руб.
17	Утечка биометрии	→ От 15 млн до 20 млн руб.
18	Действия или бездействие, которые повлекли утечку биометрии или специальных категорий данных после утечки обычных данных, которая была квалифицирована по ст. 12-14 КоАП	→ Штраф в размере от 1 до 3 процентов от дохода за год, либо от собственных средств кредитной организации (но не менее 25 и не более 500 млн)

Рисунок 2. Штрафы за допущение утечки данных — фиксированные и оборотные

Более крупные штрафы предусмотрены за несвоевременное уведомление об утечке ПДн или отсутствие такого уведомления, то есть сокрытие факта утечки — они составляют от 1 до 3 млн руб. Уведомлений об утечке должно быть два. Первое необходимо направить в течение 24 часов после инцидента, в нём необходимо указать информацию об организации, сумму предполагаемого ущерба, оценку предполагаемого объема утечки данных и категорию скомпрометированных ПДн. Второе уведомление необходимо направить в Роскомнадзор в течение 72 часов, в нем должны быть приведены результаты внутреннего расследования по итогам утечки данных. Важно, что уведомлять об утечке данных необходимо вне зависимости от ее масштабов, и отсутствие каждого из уведомлений образует отдельный состав нарушения. То есть максимальный размер штрафа — 6 млн руб. за одну утечку.

Таким образом, в течение трех дней компания должна провести большой объем внутренних работ, чтобы оценить ущерб и масштабы инцидента. При этом, согласно данным исследований экспертно-аналитического центра InfoWatch, на сегодняшний день более половины российских компаний не имеют сформированных методик оценки ущерба от утечек информации. И в этом направлении бизнесу предстоит масштабная работа.

По всем этим нарушениям также вводятся штрафы для физических и должностных лиц в компании — они составляют от 5 до 100 тыс руб. в зависимости от конкретного нарушения (рис. 1).

По текущим изменениям в регулировании можно сделать вывод о том, что в настоящий момент у законодательства есть две важные цели: создать объективный реестр операторов ПДн и замотивировать их обеспечивать должный уровень защиты ПДн и ИБ в целом. Подчеркну,

что задача заключается не в сборе штрафов, а именно в мотивации — экономия на средствах защиты информации будет обходиться дороже, чем выстраивание адекватной и эффективной системы защиты данных внутри компании.

ФЗ №420: ОБОРОТНЫЕ ШТРАФЫ И КОГДА ОНИ МОГУТ БЫТЬ СНИЖЕНЫ

Кроме санкций за сокрытие факта утечки и отсутствие уведомления Роскомнадзора новый закон вводит фиксированные штрафы за допущенную утечку, а за повторное допущение утечки — оборотные штрафы. Последние грозят компании самыми крупными выплатами.

Сумма штрафа за допущение утечки будет зависеть от масштаба инцидента. Чтобы его определить, в законе приведены две количественные метрики — это число субъектов ПДн (физических лиц, чьи данные были скомпрометированы) и идентификаторов (записи в базе данных, по которым можно определить субъекта ПДн). Диапазон сумм — от 3 до 15 млн руб., подробная разбивка на рис. 2.

Оборотные штрафы за повторную утечку данных составят 1–3 % от совокупного дохода компании, но в определенных законом пределах — не менее 20 млн руб. и не более 500 млн руб. Если повторно утекли ПДн специальной категории или биометрия, то минимальный размер штрафа выше — 25 млн руб.

И здесь есть важнейший нюанс — у бизнеса есть возможность повлиять на размер возможных штрафов, поскольку в законодательстве предусмотрена возможность снизить их до 0,1 % от дохода компании. На это смогут рассчитывать организации, которые соответствуют трем условиям. Первое условие — компания в течение трех лет до инцидента направляла не менее 0,1 % своего дохода на услуги и решения организаций, которые имеют лицензию на разработку средств шифрования и средств защиты конфиденциальной информации. Сюда же можно будет

отнести услуги по внедрению и интеграции таких решений с тем условием, что они напрямую связаны со средством защиты или продуктом. В будущем, возможно, к этому добавятся и расходы на обучение сотрудников вопросам ИБ.

Второе условие — в течение года до инцидента компания должна в полном объеме соблюдать требования по обработке персональных данных, то есть Постановление Правительства № 1119, требования ФСТЭК, требования к сертификатам, к крипто-

шифрованию и другие. И, наконец, третье условие — компания не должна привлекаться к ответственности за нарушение требований к защите информации или использование несертифицированных технических средств.

ПОДГОТОВКА К НОВЫМ ТРЕБОВАНИЯМ: ДОРОЖНАЯ КАРТА

Работа большинства заказчиков InfoWatch напрямую связана с обработкой ПДн, и мы сформировали для них дорожную карту подготовки к новому регулированию сферы ПДн. Нашей целью было помочь бизнесу провести действительно качественную оценку потенциальных рисков, найти пути их устранения и при этом не перегрузить компанию операционной работой.

♦ **Аудит перемещения ПДн.** Инструменты — опрос всех подразделений, составление карты передачи и обработки ПДн в периметре компании.

♦ **Аудит средств защиты информации и информационных систем персональных данных (ИСПДн).** Оценка перечня средств защиты информации, которые используются в компании, как организован доступ к ним, как выстроена система защиты информации.

♦ **Подготовка локальных нормативных актов и политик, а также внешних документов** — например, согласия на обработку ПДн для клиентов и сотрудников, политик обработки ПДн для внешних пользователей, и т.д. Создавать их необходимо на базе той информации, которую получили по итогам первого и второго пунктов.

♦ **Утверждение регламентов проведения мероприятий информационной безопасности** и реагирования на инциденты. В первую очередь это методика оценки утечки информации, ущерба от нее, положение о реагировании на инциденты, документы, разграничивающие ответственность компании и сотрудника. В случае утечки это позволит оперативно среагировать и собрать данные для уведомления Роскомнадзора.

♦ **Направление уведомлений о намерении начать обработку ПДн в Роскомнадзор.**

♦ **Организация текущего контроля и отчетности.** Это важно, чтобы показать контролирующим органам добросовестность компании на протяжении длительного периода и в случае повторной утечки снизить размер оборотного штрафа.

РЕШЕНИЯ INFOWATCH ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

ГК InfoWatch адаптировала свои решения к новым требованиям по защите ПДн реагированию на инциденты ИБ, которые предусматривают изменения в законодательстве. Ключевой продукт линейки по защите данных, DLP-системы Traffic Monitor, позволяет отслеживать и строить карты перемещения ПДн внутри компании, оценивать возможность утечки данных, обращать внимание офицера ИБ на потенциальные риски и слабые места.

В 2024 году ГК InfoWatch запатентовала технологию для защиты ПДн — «Способ автоматического анализа выгрузок из баз данных». Этот подход реализован в DLP-системе Traffic Monitor и позволяет анализировать неструктурированную информацию и контролировать исходящие потоки данных, защищая таким образом ПДн от несанкционированной передачи. Решение вошло в ТОП-10 лучших изобретений в области ИБ и кибербезопасности по версии Роспатента.

Также в InfoWatch разработаны три авторские методики для аудита документов и процессов на предмет соответствия требованиям законодательства. Методика аудита персональных данных позволяет создать объективную картину использования ПДн в компании, выявить уязвимости систем и несовершенство организационно-правовых процессов. Методика сбора, обработки и анализа сведений об утечке решает задачу проведения расследования инцидента в сжатые сроки. Методика сбора и обработки информации об ущербе позволяет определить реальный объем утечки и выявить дополнительные критические факторы ИБ.

«ДАЮ СОГЛАСИЕ НА ОБРАБОТКУ...»

НАШИ СОГЛАСИЯ НЕ ЗАЩИЩАЮТ ДАННЫЕ,
А ЛИШЬ СНИМАЮТ ОТВЕТСТВЕННОСТЬ С ОПЕРАТОРА



Елена БУТКОВА

главный инспектор Управления информационной безопасности Министерства государственного управления, информационных технологий и связи Московской области

Сегодня нам приходится давать согласия на обработку своих (и не только) персональных данных практически на каждом шагу: получение государственной услуги, регистрация на маркетплейсе, оказание медицинских, банковских, образовательных услуг и т.д. Как правило, на срок согласия и объём предоставляемых персональных данных внимания не обращаем. Тем не менее Федеральным законом № 152-ФЗ «О персональных данных» чётко описаны эти рамки: хранение персональных данных — не дольше, чем требуют цели обработки и уничтожение (обезличивание) — по достижении (утраты достижения) целей.

А ЧТО НА ПРАКТИКЕ?

«Ночь, улица, фонарь, аптека...».

Банк, справка об открытых счетах в банке, согласие на 50 (!) лет по 28 (!) позициям, включая выписку об остатке материнского капитала, сведения из электронной трудовой книжки, сведения об отнесении гражданина к категории граждан предпенсионного возраста, данные транспортных средств. В медицине и образовании пошли ещё дальше: бессрочное предоставление согласия (будем верить, для того чтобы быть проактивными и находить решения до возникновения

проблем). Поражает объём избыточности запрашиваемых для обработки сведений, которые никак не соотносятся с целью. Срок в 50 лет очень удивляет (особенно если подписать согласие лет так в 60–70).

«Бессмысленный и тусклый свет...».

Очевидно, чем больше объём информации (что неизбежно при её избыточном получении), тем больше ресурсов потребуется для её защиты. В ноябре 2024 года заместитель председателя правления Сбербанка С. Кузнецов на SOC-форуме заявил, что около 90 % взрослого населения, к сожалению, в той или иной части какие-то персональные данные имеют в открытом доступе. Роскомнадзор зафиксировал за 2024 год 135 случаев утечки баз данных, в которых содержались более 710 млн записей о россиянах. Утечки неизбежны, но потеря базы данных с двумя позициями всё же предпочтительнее, чем с двадцатью восьмью и бессрочной возможностью кражи.

«Живи ещё хоть четверть века...».

Конечно, так не везде. Как правило, в государственных информационных системах персональные данные уничтожаются (обезличиваются) по достижении цели. Сегодня в Московской области находится в эксплуатации более 70 государственных информационных

систем, в 70 % из них осуществляется обработка персональных данных. Для защиты информации проводится аттестация. Аттестационные испытания представляют собой комплекс мероприятий, целью которых является подтверждение соответствия объекта информатизации требуемому уровню безопасности при обработке информации ограниченного доступа. 100 % эксплуатируемых государственных информационных систем Московской области имеют аттестат соответствия требованиям безопасности информации. Наличие аттестата позволяет быть уверенным в том, что информация надёжно защищена (в рамках установленных требований). И проактивность здесь кстати: ведь удобно при замене паспорта в связи с изменением фамилии одновременно поменять ещё права и заграничный паспорт!

«Всё будет так. Исхода нет».

Реализовать требования безопасности единоразово, под конкретные аттестационные испытания несложно, а вот в условиях эксплуатации и динамично меняющейся архитектуры системы, её программно-аппаратного обеспечения (например, в рамках импортозамещения) и категорий и (или) количества обрабатываемых персональных данных — уже труднее. Например, сейчас применяются технологии виртуализации и контейнеризации: при увеличении нагрузки системы оркестрации могут автоматически запускать необходимые виртуальные машины или контейнеры, не указанные в техническом паспорте. Или добавились данные для получения государственной услуги, что привело к обработке, например, специальной категории персональных данных.

Беспокоит и то, что базы данных содержат информацию с определённым законодательством сроком хранения. Например, документы по обращениям граждан — 5 лет, далее — уничтожение. Каким образом соблюдается этот срок в реальных условиях? Сложности возникают как в организационно-управленческой сфере, так и в технической. Необходимо внедрение (или разработка) программных продуктов, реализующих механизмы подсчёта сроков хранения и последующего уничтожения персональных данных.

«Умрёшь — начнёшь опять сначала!»

Федеральный закон от 08.08.2024 № 233-ФЗ установил требование для операторов — применять для уничтожения персональных данных только средства защиты информации, которые прошли в установленном порядке процедуру оценки соответствия и в составе которых реализована функция уничтожения информации. Это означает, что ПО, используемое для уничтожения персональных данных, должно стать сертифицированным (по аналогии с ПО для защиты информации). Сейчас такое отдельное сертифицированное ПО найти крайне сложно. Понятно, что можно повторно сертифицировать уже имеющиеся средства защиты информации (в которых предусмотрена возможность удаления данных) и как «ПО, используемое для уничтожения персональных данных». Но, думается, не того хотел законодатель.

А если попробовать обезличить персональные данные?

«И повторится всё, как встарь...»

Федеральный закон от 08.08.2024 № 233-ФЗ по-новому определяет особенности обработки обезличенных персональных данных при формировании составов данных и предоставления доступа к ним. Заместитель министра цифрового развития, связи и массовых коммуникаций РФ А. Шойтов во время беседы с журналистами РИА «Новости» заявлял о создании центра обезличивания. Предполагалось, что полноценный макет, в котором будут реализованы различные варианты исходных данных,



создадут на базе Национального технологического центра цифровой криптографии к концу 2024 года. В процессе работы с обезличенными данными есть две ключевые задачи: обеспечить невозможность восстановления исходной личной информации конкретного гражданина по обезличенным данным и сохранение данных в максимально качественном виде для их дальнейшего использования. Возможно, для тестирования работоспособности информационной системы (обрабатывающей персональные данные) до ввода её в эксплуатацию или обучения технологий ИИ.

Не секрет, что основная цель обезличивания — вывод данных из-под действия Федерального закона № 152-ФЗ. Бывает, что уничтожать информацию нельзя и организовать её правильное хранение невозможно (затратно), а обезличенные данные можно хранить и обрабатывать без требуемой законом защиты информации, а также обменивать (продавать) без согласия субъектов. Очень удобно для тестирования новых приложений банков, работающих с огромными пользовательскими массивами данных. Здесь обезличка — в помощь!

«Ночь, ледяная рябь канала...»

С 01.09.2025 вводится обязанность операторов персональных данных

по передаче обезличенных сведений в закрытую государственную информационную систему по запросу Министерства цифрового развития, связи и массовых коммуникаций РФ. Состав таких данных, сроки передачи, порядок обезличивания ещё будут определены Правительством РФ совместно с ФСБ России. В дальнейшем доступ в закрытую государственную информационную систему предоставят государственным и муниципальным органам, гражданам России и российскому бизнесу. Очень заманчивая идея: пользоваться готовыми обезличенными данными (надемся, бесплатно).

«Аптека, улица, фонарь»

. Возвращаясь к началу. Важно понимать, что согласия на обработку персональных данных по существу не защищают наши данные, а лишь снимают ответственность с оператора, который их обрабатывает, и ситуация не изменится, даже если давать своё согласие не рукописной, а электронной подписью или отпечатком пальца. Будьте внимательнее, осмотрительнее, бережливее со своими персональными данными. Уважайте и цените свою личную «информацию, относящуюся к прямо или косвенно определённом или определяемому физическому лицу».

МИФ ИЛИ РЕАЛЬНОСТЬ?

ЗАЩИТА ИНФРАСТРУКТУРЫ БЕЗ СРЕДСТВ ЗАЩИТЫ



Александр ГОРБАЧЕВ
архитектор инфраструктуры информационной безопасности «Инфосистемы Джет»

Часто организации сосредотачиваются на приобретении самых современных и дорогостоящих средств защиты, полагая, что это является гарантией безопасности. Однако, как показывает практика, бреши в системе безопасности могут возникнуть не из-за отсутствия модных технологий, а из-за пренебрежения базовыми мерами безопасности. Рассказываем, как повысить уровень защищенности организаций, не полагаясь исключительно на дорогостоящий и сложный софт.

Представьте компанию среднего размера с головным офисом и разветвленной филиальной сетью, где все бизнес-процессы завязаны на стандартном наборе информационных систем: электронная почта, система управления предприятием (например, 1С), файловые серверы и т.д. И вот однажды в результате неосторожных действий сотрудника или целенаправленной атаки злоумышленника в сеть проникает вирус-шифровальщик со всеми вытекающими последствиями.

Что привело к печальному исходу? Безусловно, существует множество факторов, но, если проанализировать ситуацию более детально, то, как правило, выявляются одни и те же типичные ошибки и упущения в области информационной безопасности.

Полное отсутствие или частичная сегментация сети. Все устройства, включая рабочие станции, серверы и сетевое оборудование, на-

ходятся в одной подсети, что значительно упрощает распространение вредоносного программного обеспечения. Злоумышленник, получив доступ к одному устройству в сети, может беспрепятственно перемещаться по всей инфраструктуре, заражая все больше и больше систем.

Пренебрежение политиками безопасности или их формальное соблюдение. В компании могут существовать формальные политики безопасности, регламентирующие порядок использования информационных ресурсов, требования к паролям и т.д. Однако если эти политики не доводятся до сведения сотрудников, не контролируется их соблюдение и не проводятся регулярные проверки, то их практическая ценность стремится к нулю.

Отсутствие или ненадлежащая организация процесса обновления программного обеспечения. Использование устаревших версий операционных систем, приложений и другого программного обеспечения, содержащих известные уязвимости, — это огромный риск для безопасности всей инфраструктуры. Злоумышленники постоянно сканируют сети в поисках уязвимых систем, и использование устаревшего программного обеспечения делает компанию легкой добычей.

Недостаточное внимание к защите резервных копий данных. В данном случае именно незащищенность резервных копий стала критическим фактором, приведшим к полному параличу деятельности

компании. Если бы существовали надежные резервные копии данных, изолированные от основной сети, то восстановление работоспособности сети и возобновление бизнес-процессов заняло бы гораздо меньше времени.

К сожалению, подобные ситуации не являются чем-то исключительным. Подобные сценарии регулярно повторяются в различных организациях, демонстрируя, что пренебрежение базовыми мерами безопасности может привести к катастрофическим последствиям.

ЧТО ТАКОЕ ХАРДЕНИНГ И ПОЧЕМУ ОН ЯВЛЯЕТСЯ ФУНДАМЕНТОМ БЕЗОПАСНОСТИ?

Под термином «харденинг» подразумевается комплекс мер и мероприятий, направленных на повышение уровня безопасности информационной системы путем безопасной настройки ее компонентов. Харденинг — это не просто набор технических приемов, а целостная стратегия, охватывающая все уровни ИТ-инфраструктуры, начиная с операционных систем и заканчивая сетевым оборудованием.

В основе харденинга лежат три ключевых принципа:

1. Безопасная конфигурация. Изменение параметров, направленное на повышение защищенности, отключение ненужных сервисов и функций, настройка прав доступа и применение других технических мер, направленных на усиление защиты системы.

2. Использование встроенных средств защиты. Современные операционные системы и приложения, как правило, оснащены встроенными механизмами безопасности, которые при правильной настройке могут обеспечить высокий уровень защиты. К таким средствам относятся встроенные межсетевые экраны, системы контроля учетных записей, антивирусные программы и пр.

3. Минимизация поверхности атаки. Отключение ненужных сервисов и функций, которые могут быть использованы злоумышленниками для проникновения в систему. Чем меньше поверхность атаки, тем меньше уязвимостей, которыми может воспользоваться злоумышленник.

Помимо харденинга, важные значения имеют безопасные архитектурные решения, такие как сегментация сети, выделение демилитаризованной зоны (DMZ) для общедоступных сервисов, использование нескольких каналов связи с интернетом для повышения отказоустойчивости и др. Решения позволяют значительно повысить устойчивость инфраструктуры к различным видам атак. Нельзя забывать и о процессах обеспечения информационной безопасности, которые должны быть внедрены и поддерживаться в каждой организации: регулярный контроль доступа к информационным ресурсам, управление уязвимостями программного обеспечения, своевременное обновление программного обеспечения и т.д.

Реализация этих мер не гарантирует стопроцентную защиту от всех возможных угроз, однако значительно снижает вероятность атаки и увеличивает время, необходимое злоумышленнику для достижения своих целей.

ПРЕОДОЛЕНИЕ СЛОЖНОСТЕЙ И ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ

Внедрение базовых мер безопасности нередко сопряжено с определенными трудностями, которые необходимо учитывать на начальном этапе. Одной из самых распространенных проблем является неопределенность в выборе приоритетов. Компании часто задаются вопросом: с чего же начать? Обновлять программное обеспечение, настраивать политики безопасности или сразу приступать к сегментации сети? Отсутствие четкого плана и координации усилий может привести к хаотичному выполнению множества задач, что в конечном итоге снижает общую эффективность. Важно изначально вы-

Нельзя подходить к защите всех систем одинаково. Необходимо четко понимать, какие системы и данные являются наиболее ценными для бизнеса, и в первую очередь сосредоточить основные усилия на их защите

работать стратегию, определив наиболее важные направления.

Еще одной сложностью является потенциальный конфликт интересов между ИТ-подразделением и службой ИБ. Чтобы не затягивать процесс внедрения необходимых изменений, необходимо сформировать единую команду, работающую над обеспечением безопасности всей инфраструктуры. Важно, чтобы каждый понимал роль и ответственность другой стороны, а решения принимались на основе коллегиального обсуждения.

Помимо организационных проблем, часто возникают трудности, связанные с восприятием и пониманием стандартов безопасности. Они, как правило, содержат в себе полный перечень всех возможных рекомендаций, что затрудняет их практическое применение. В этом случае необходимо адаптировать их к конкретным условиям организации, выделив наиболее важные рекомендации, которые будут применимы к информационным системам и бизнес-процессам.

Наконец, важным аспектом является правильная оценка критичности отдельных компонентов инфраструктуры. Нельзя подходить к защите всех систем одинаково. Необходимо четко понимать, какие системы и данные являются наиболее ценными для бизнеса, и в первую очередь сосредоточить основные усилия на их защите. Для этого рекомендуется использовать анализ влияния на бизнес (Business Impact Analysis, BIA), который позволяет определить потенциальные последствия для бизнеса в случае отказа или компрометации тех или иных систем. Использование BIA позволяет расставить приорите-

ты и направить ресурсы на защиту наиболее важных активов.

С ЧЕГО НАЧАТЬ?

1. Составьте подробный перечень всех устройств, программного обеспечения и данных, которые используются в вашей организации.

2. Создайте подробные схемы вашей сети, отражающие структуру сети.

3. Установите последние версии прошивок и операционных систем на все сетевые устройства, чтобы устранить известные уязвимости.

4. Настройте безопасные параметры операционных систем, серверов и другого оборудования.

5. Разделите сеть на сегменты, чтобы ограничить распространение вредоносного программного обеспечения в случае успешной атаки.

6. Определите, кто и к каким ресурсам должен иметь доступ, и настройте соответствующие права доступа.

7. Начните с внедрения базовых процессов контроля доступа, управления уязвимостями и резервного копирования данных.

Базовая гигиена информационной безопасности — это основа любой надежной системы защиты. Ее внедрение не требует больших финансовых вложений, но требует времени, внимания и грамотного подхода. Безопасность — это непрерывный процесс, а не разовая акция. Не ждите идеальных условий — начните действовать прямо сейчас. Даже небольшие шаги в правильном направлении могут принести значительные результаты. Помните, что информационная безопасность — это ответственность каждого сотрудника, а не только ИБ-специалистов.

ПЛАТФОРМЕННЫЙ ПОДХОД К ЗАЩИТЕ ДАННЫХ

ОПЫТ КОМПАНИИ «САЙБЕРПИК»



**Сергей
ДОБРУШСКИЙ**
директор
по развитию
продуктов
компании
«Сайберпик»

Вопрос защиты данных для любой компании с каждым годом становится всё более актуальным. Причин популярности несколько: это и принятые оборотные штрафы за утечку ПДн, новости о которых находятся в информационном поле сотрудников отделов ИБ и собственников бизнеса длительное время. Это и растущее количество атак, нацеленных как на кражу, так и на уничтожение (например, шифрование) данных. Это и растущий уровень компетенций по информационной безопасности в стране. Сейчас редко возникает вопрос, нужно ли защищать данные. Чаще звучит другой: какие данные необходимо защищать в первую очередь и какие из инструментов стоит применять. Если говорить про крупнейшие холдинги страны, то вопрос того, какие классы продуктов информационной безопасности должны входить в состав системы защиты данных, как правило решен. Однако уверенно говорить, что данные, расположенные внутри компании, надежно защищены, достаточно сложно.

ОДНО ОКНО ДЛЯ ЗАЩИТЫ ВСЕХ ДАННЫХ

Давайте для начала разберемся, когда речь идет о защите данных, то о

какой именно информации говорят и где она может находиться.

В это понятие мы включаем весь огромный массив файлов и документов, которые каждый день создают сотрудники, и важная часть этих данных — чувствительная информация, представляющая непосредственную ценность для компании. В зависимости от отрасли в понятие «чувствительной информации» может включаться проектная документация, чертежи, спецификации на оборудование, выгрузки клиентов, всё, вплоть до исходного кода, если речь идет об ИТ-компаниях.

Где эта информация может находиться, вроде понятно: это файловые хранилища, рабочие станции, системы общего обмена файлами, корпоративные порталы, базы данных и многочисленные информационные системы. Но, как показывают результаты аудитов, которые эксперты компании «СайберПик» проводят для промышленных внедрений наших систем и в рамках пилотных проектов, далеко не все понимают всё многообразие инфраструктуры компании и систем, которые в ней расположены.

В начале 2024 года мы в компании «СайберПик» приняли решение, что наш флагманский продукт «Спектр | DCAP» (система для защиты файловых хранилищ и контроллеров домена) необходимо развивать в сторону платформы защиты данных, чтобы задачу защиты максимально большого количества мест хранения информации можно было покрывать одним продуктом из одного окна или глубоко интегрированными между собой продуктами. Именно так мы вышли на новый не только для себя, но и в целом для нашей страны, рынок продуктов класса Data Security Platform (DSP).

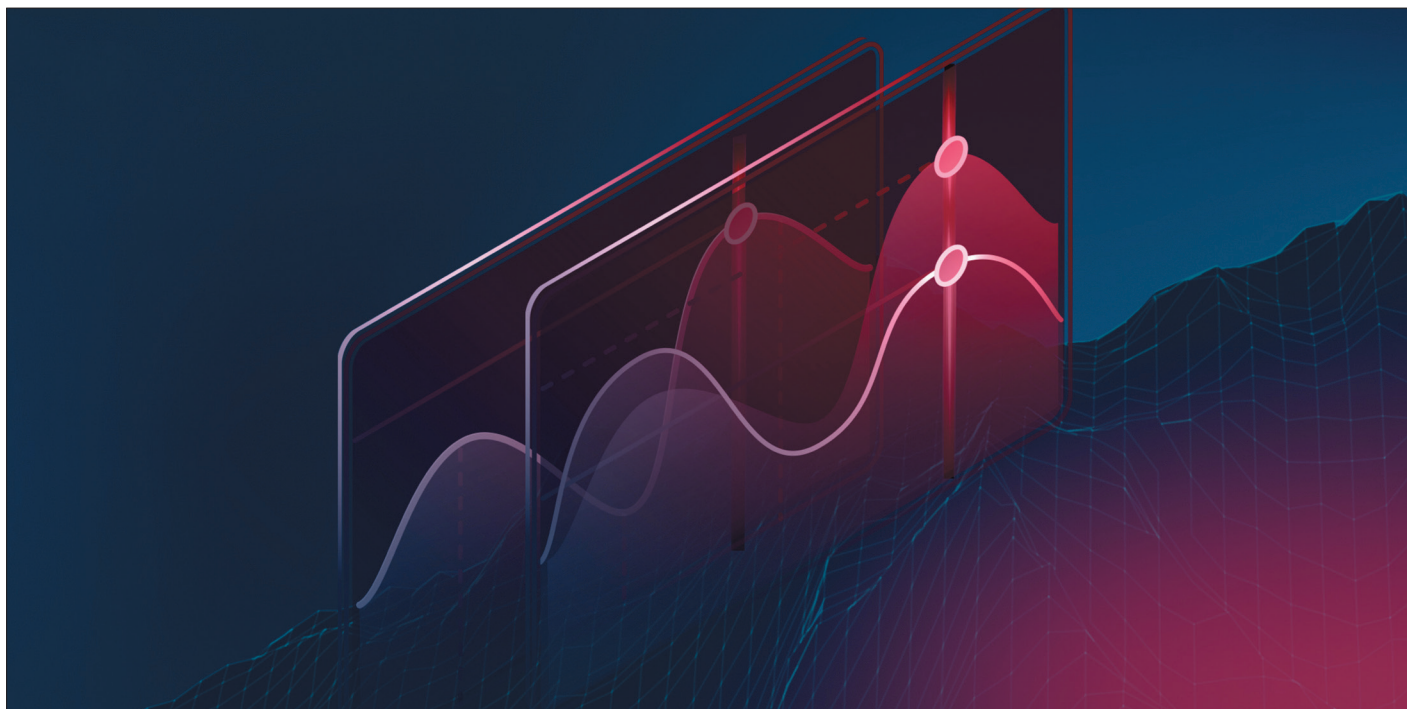
Общая концепция платформы защиты данных «Спектр», которую по праву можно отнести к концепции Data Security Platform, — это комплексная защита максимального количества данных, как расположенных в состоянии «покоя» в компании, так и на всех этапах жизненного цикла работы с ними.

Начнем с базовых задач, решаемых платформой защиты данных, которые стоят в каждой компании, независимо от отрасли, уровня зрелости ИБ, выстроенных процессов, и др.

ИНВЕНТАРИЗАЦИЯ АКТИВОВ

Прежде чем подходить к защите данных, необходимо определиться с масштабами, а именно понять, какая информация расположена в инфраструктуре компании, где расположена наиболее ценная, а от какой информации, наоборот, можно избавиться. Для этого платформа защиты данных «Спектр» обладает встроенным механизмом классификации данных. Это универсальный инструмент, который позволяет, настраивая и используя унифицированные правила, анализировать большинство мест хранения данных, от рабочих станций, файловых серверов, облачных хранилищ до баз данных. Ключевое, что на выходе дает классификация, это возможность сузить круг информации, на защите которой стоит сконцентрироваться.

На выходе система предоставляет крайне ценный инструмент для департамента информационной безопасности и не только — это полноценный каталог данных (data catalog), т.е. единая система, к которой в любой момент можно обратиться и найти любую интересующую информацию. Причем поиск будет доступен как по контенту, так как платформа защиты данных «Спектр» позволяет



провести полнотекстовую индексацию данных, так и по различным метаданным (от даты создания, автора, заканчивая специфичными свойствами того или иного файла).

Классификация — это не быстрый процесс и его скорость напрямую зависит от объемов анализируемой информации, но, уже получая первые результаты, можно подходить к решению двух других задач, которые платформа защиты данных «Спектр» способна решить.

МИНИМИЗАЦИЯ ПРАВ ДОСТУПА СОТРУДНИКОВ

Эта задача может быть спроецирована практически на любые данные, хотя система выдачи привилегий способна отличаться. Оптимизируя права доступа, даже в не очень большой инфраструктуре, мы всегда рекомендуем начинать с наиболее ценных активов, плавно переходя и к менее важным ресурсам.

Параллельно с минимизацией прав доступа задачу защиты информации можно решать и альтернативным путем — при помощи чистки и переноса чувствительных данных из нецелевых мест хранения.

Тут также помогает задача классификации, т.к. параллельно с ней происходит и анализ прав доступа к

каждому анализируемому объекту — будь то файл или таблица в СУБД. Таким образом, чувствительные данные в нецелевых местах хранения, либо же данные с расширенными привилегиями, можно автоматически переместить в карантинные папки, снизив риск утечки к нулю.

НЕПРЕРЫВНЫЙ АУДИТ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ

Вышеописанные задачи в первую очередь относятся к защите «данных в покое», при этом нужно не забыть про данные, которые находятся «в движении». Это и периодические изменения в документах, их перемещение и удаление, создание новых таблиц в СУБД с последующей вставкой туда информации, и изменение внутри каталогов домена — создание новых УЗ, групп, модификация групповых политик. Все эти события необходимо в полной мере контролировать и оперативно реагировать на потенциально опасные операции.

Одной из задач, которая стоит перед платформой защиты данных «Спектр», безусловно является сбор всех событий, их корреляция, сохранение и различные способы реагирования на выявленные инциденты.

Нам удалось внутри единой системы с общим интерфейсом, общей системой фильтрации и общими политиками реагирования собрать все эти события. Более того, сравнивая такой подход с разрозненным сбором этих событий и последующей пересылкой в SIEM, выделим ряд ключевых отличий. Пока данные находятся внутри платформы, они обладают контекстом, т.е. они обогащены правами доступа, категориями классификации, обнаруженными в таблице СУБД или файле. Часто при расследовании инцидентов эта информация бывает крайне полезна. При этом большинство крупных компаний в дополнении настраивают и перенаправление событий в SIEM, чтобы SOC содержал в себе максимум событий с прикладных систем.

Конечно, это далеко не всё, что позволяет называть нашу платформу защиты данных «Спектр» действительно комплексным решением для защиты всех данных компании, но, пожалуй, я перечислил её ключевые аспекты. В заключение отмечу, что подход Data Security Platform хоть и появился на рынке недавно, но, учитывая его главную задачу — экономию ресурсов без потери качества защиты информации, спрос на него и его популярность растут.

ПРИВИВКА ОТ ОБОРОТНЫХ ШТРАФОВ

КАК DСАР ПОМОГАЮТ ЗАЩИТИТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ



Алексей ПАРФЕНТЬЕВ
заместитель генерального директора
по инновационной деятельности «СёрчИнформ»

Ответственность за утечки ПДн становится строже. Виновникам сливов теперь грозят сроки до 10 лет по новой статье 272.1 УК РФ. А если до уголовного преследования не дойдет, компанию оштрафуют: и размеры штрафов выросли в 150 раз. Сейчас первая утечка ПДн карается штрафом до 100 тыс. рублей, а с 30 мая — до 15 млн. Повторная повлечет штраф до 3 % от оборота компании вместо максимальных 300 тыс. рублей, как это было раньше. Это касается любой организации, поскольку каждая компания работает с ПДн клиентов, сотрудников, третьих лиц.

Компаниям становится выгоднее защищать ПДн, чем разбираться с наказаниями за утечки и прямыми потерями от них. Законодатели ввели смягчающие обстоятельства: если компания регулярно вкладывается в ИБ и соблюдает ИБ-требования, штраф за повторный инцидент снижается в 10 раз. Теперь организациям остается решить, какие инструменты защиты ПДн быстро внедрить уже сейчас, чтобы снять риски в будущем.

МЕТОДИКА ЗАЩИТЫ ПО ЗАКОНУ

152-ФЗ регламентирует обработку ПДн в России и содержит конкретные требования по их защите. Согласно ему, любая организация, которая работает с данными граждан, обязана:

- ◆ Установить правила доступа к ПДн, обрабатываемым в организации.
- ◆ Обеспечить регистрацию и учет всех действий, совершаемых с ПДн в информационных системах.
- ◆ Обнаруживать факты несанкционированного доступа к ПДн.
- ◆ Восстанавливать ПДн, модифицированные или уничтоженные вследствие несанкционированного доступа к ним.
- ◆ Контролировать меры по обеспечению безопасности ПДн и защищенности информационных систем ПДн.

То есть, прежде чем бороться с утечками ПДн, компании должны обеспечить прозрачность и безопасность их обработки. Эффективно решает эти задачи DСАР-система — решение для защиты неструктурированных данных «в покое». DСАР обнаруживает критичный контент (в данном случае ПДн) в корпоративных хранилищах, отслеживает, кому доступны такие данные, и что с ними происходит.

Система контролирует права пользователей и все их операции с документами. В результате видна реальная картина хранения ПДн и риски при их обработке. DСАР обеспечивают базовый уровень защиты данных и минимизируют риск утечки.

Разберемся, как это работает на примере DСАР «СёрчИнформ FileAuditor».

ЗАЩИТА НА ПРАКТИКЕ

В компании стоит задача: обезопасить ПДн. Что для этого нужно?

1. Найти и классифицировать все файлы, которые содержат ПДн.

Это могут быть базы контактных данных клиентов с номерами телефонов, сканы паспортов сотрудников, заявления или договоры с реквизитами документов подписанта. FileAuditor автоматически определяет самые распространенные виды ПДн и офисных документов.

Чтобы их обнаружить, FileAuditor сканирует содержимое корпоративных хранилищ: персональных компьютеров (ПК) и локальных серверов, сетевых папок, «облаков», FTP-обменников и пр. Вычитывает каждый файл, чтобы определить тип содержимого. Система не пропустит ПДн, в каком бы виде они ни хранились: изображения распознаются с OCR, текстовые документы оцениваются вплоть до смысловой схожести с заданным образцом. Всего в системе больше 10 аналитических алгоритмов, поэтому качество классификации высоко.

Классификацию можно запустить без долгой предварительной настрой-

ки, в FileAuditor для этого более 450 готовых правил. По желанию их можно дополнить. Например, ввести минимальный порог входа (не менее N совпадений в документе) или учитывать только файлы, где одновременно встречаются не менее N комбинаций из, скажем, номеров паспорта и телефона. Или проверять только свежие документы, с определенным именем, расширением, расположением и т.п. То есть настройки максимально гибкие.

По результатам классификации FileAuditor присваивает файлам метки. Они остаются на документе, пока внутри есть критичный контент. То есть: пока в договоре вписаны ФИО клиента, метка «ПДн» на нем сохранится. Как только эти сведения удалят — пропадет. При этом системе не важно, если файл был переименован, перемещен, поменял расширение и т.д. А если содержимое документа копируют в другой файл, метка автоматически появляется и на нем.

2. Отследить, кто и как с ними работает.

FileAuditor показывает, каким сотрудникам или группам доступен конкретный файл, и наоборот: какие файлы и папки доступны тому или иному пользователю. Программа получает сведения о правах доступа пользователей из файловой системы и системы управления доменом, контролирует их изменение. Видны и действия администраторов, которые распределяют права для новых пользователей, или меняют разрешения для действующих сотрудников. Это удобно, чтобы сразу фиксировать ошибки в раздаче доступов к ПДн.

Следующая ступень контроля — выявить, как этими доступами пользуются, то есть кто и как работает с защищаемыми файлами. Система регистрирует все действия пользователя с файлами: чтение, изменение, сохранение, удаление. Например, если сотрудник взял из архива заполненный договор и использует как шаблон на своем ПК — DCAP сначала зафиксирует, что у файла появился дубликат, а потом покажет, как менялось его содержимое. Историю редакций документа FileAuditor сохраняет: это

убережет от нежелательных правок, порчи и потери важных файлов.

Так DCAP обеспечивает контроль за обработкой ПДн, причем FileAuditor автоматически оповещает обо всех нарушениях.

3. Создать безопасные сценарии обработки ПДн.

FileAuditor управляет доступом к ПДн, чтобы внутри компании они не попали к тем, кому не нужны по работе. А те, кому нужны, не могли сделать с ними ничего опасного.

Во-первых, система может идти «от пользователя»: запрещать/разрешать просмотр конкретных файлов и папок сотрудникам или группам в зависимости от их полномочий. Например: личные документы сотрудников должны лежать в сетевой папке, с которой работают только пользователи из группы «отдел кадров». Так обеспечивается контроль доступа к местам хранения ПДн.

Во-вторых, FileAuditor защищает документы «по контенту» — по меткам классификации. Тогда сотрудники без необходимых полномочий не смогут открыть файл с ПДн, где бы он ни хранился. Система запрещает доступ для программ, с помощью которых сотрудники обращаются к файлу: это офисное ПО, мессенджеры, почтовые клиенты, браузеры, даже самописные системы. Например, можно запретить открывать клиентские базы в MS Excel, или прикреплять сканы паспортов во вложения в Telegram. Блокировки в DCAP работают так, что программы не смогут получить доступ к документам в файловой системе.

Блокировки не мешают бизнес-процессам — ограничения затрагивают конкретные варианты взаимодействия с данными, в другом ПО с файлами можно работать. То есть «СёрчИнформ FileAuditor» задает такие правила обработки ПДн, что их технически сложно нарушить. Это уникальный функционал, технология запатентована.

РЕЗУЛЬТАТ

DCAP-системы эффективны в защите ПДн и снижении риска их утечек. Организация видит: сколько хранит

ПДн, как происходит их обработка, контролирует соблюдение ее правил — как и предписывает закон. Фокус на данных гарантирует, что критичная информация останется под защитой, несмотря на любые манипуляции с файлом. Система страхует от потери и модификации документов с ПДн. А блокировки помогают ограничить спектр возможных действий с ПДн и круг сотрудников, которым они доступны.

Таким образом, FileAuditor:

- ♦ **Находит ПДн** в содержимом любых файлов, в т.ч. нетекстовых, где бы они ни хранились.

- ♦ **Запрещает доступ** к файлам с ПДн для сотрудников и групп, в чьи обязанности не входит их обработка.

- ♦ **Контролирует все операции с файлом**: создание, изменение, копирование, перенос, удаление.

- ♦ **Блокирует передачу, изменение, чтение** данных на уровне доступа к файлам.

- ♦ **Ведет архив** файлов с ПДн, чтобы восстановить нужную версию в случае их порчи/утраты.

Система высоко автоматизирована, поэтому ее можно внедрить быстро и просто. Функционал обеспечивает базовую защиту данных внутри компании, что снижает риск штрафов за нарушения в сфере обработки ПДн и их утечку. К тому же DCAP усиливают профильные средства защиты от утечек — DLP-системы. Например, FileAuditor бесшовно интегрирован с «СёрчИнформ КИБ» и помогает ему быстрее обнаруживать защищаемые документы.

FileAuditor доступен для бесплатного тестирования в течение 30 дней. Этого хватит, чтобы оценить «фронт работ» по защите ПДн в вашей компании и испытать, как фокус на контенте облегчает эту работу:



КАК НЕ ДОПУСТИТЬ ОБОРОТНЫХ ШТРАФОВ ЗА УТЕЧКУ ПЕРСОНАЛЬНЫХ ДАННЫХ



Денис СУХОВЕЦ
директор
продуктового
направления
защиты данных
компания
«Аладдин Р.Д.»



Анна ГОРШКОВА
product
marketing
manager
компания
«Аладдин Р.Д.»

3 0 ноября 2024 г. Президент Российской Федерации подписал **Федеральный закон № 420 «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»**, который вступит в силу 30 мая 2025 г.

Какие меры предусмотрены для компаний за утечку персональных данных?

С момента вступления в силу изменений компаниям-операторам персональных данных могут быть предъявлены следующие штрафы:

- ♦ **до 300 тыс Р** за несвоевременное уведомление Роскомнадзора о намерении начать обработку персональных данных (далее ПДн);
- ♦ **до 3 млн Р** за каждую просрочку уведомления об утечке и промедление уведомления о результатах внутреннего расследования утечки;
- ♦ **до 500 млн Р** за утечку ПДн;
- ♦ **до 10 лет лишения свободы** за незаконное использование ПДн.

Новые меры за нарушение работы с ПДн очень строгие, срок до вступления изменений в силу короткий. При оценке инцидента и вынесении наказания за утечку законодательство предусматривает смягчающие меры. Но их наличие не освобождает компанию от ответственности. Из всего многообразия ИБ-инструментов сейчас организациям необходимо выбирать защиту непосредственно самих данных.

В чём причины ужесточения наказания за утечку данных?

При общем росте уровня информационной безопасности в крупных российских организациях вопросу непосредственно защиты данных уделяется мало внимания. Все силы сосредоточены на защите инфраструктуры и управлении ИБ-инцидентами — защита периметра, мониторинг событий, управление контролем доступа. Эти меры важны для снижения уровня угроз, но сами данные не защищают. Персональные данные стали современной валютой, при организации целевых атак именно они являются мишенью для злоумышленников. По разным оценкам вероятность успеха атак, целью которых является похищение данных достигает 90 %. Когда злоумышленники доберутся до желаемой цели — лишь вопрос времени. Такой масштаб проблемы побудил государство ужесточить регулирование, давая участникам рынка прямой сигнал — **утечки персональных данных должны прекратиться**. На языке информационной безопасности это означает, что обеспечение конфиденциальности персональных данных является приоритетной задачей защиты информации для любой организации.

Как предотвратить угрозы утечек и обеспечить конфиденциальность персональных данных?

Организации-оператору ПДн необходимо выделить информационные системы, обрабатывающие наибольшие объёмы персональных данных.

Обычно это одна-две системы, данные которых коммерчески привлекательны для злоумышленников. Затем необходимо определиться с мерами защиты конфиденциальности этих систем. Наиболее эффективным методом защиты персональных данных является их обезличивание. Обезличивание позволяет организации использовать важную информацию в своих рабочих процессах, но при этом делает её абсолютно бесполезной для злоумышленников. Инструментом такой защиты является российский программный продукт Кripto БД, механизмы которого основаны на отечественных криптоалгоритмах, соответствующих требованиям ФСБ России к СКЗИ. Селективное прозрачное шифрование является эффективным и, пожалуй, единственно действенным методом предотвращения масштабных утечек данных. Система Кripto БД представляет собой набор важнейших возможностей для ИБ-специалиста:

- ♦ **обезличивание данных выборочным шифрованием таблиц/столбцов базы данных;**
- ♦ **«прозрачность» для пользователей и приложений;**
- ♦ **двухфакторная аутентификация и контроль доступа;**
- ♦ **централизованное управление;**
- ♦ **мониторинг и аудит.**

Введение оборотных штрафов за масштабные утечки персональных данных безусловно изменит приоритеты большинства компаний. Широкое применение продукта Кripto БД показывает, что такой подход к защите информации в СУБД обходится организации существенно дешевле (время, деньги, трудозатраты), чем организация внушительного состава комплексных мероприятий, дающих лишь робкую надежду, что злоумышленник не проберётся через несколько эшелонов периметровой безопасности, до хранилища незащищённых данных.

КАК ARZip ПОМОГАЕТ...

...ИСКЛЮЧИТЬ УТЕЧКИ ДАННЫХ В ЗАПАРОВАННЫХ АРХИВАХ



**Дмитрий
СЛОБОДЕНЮК**
коммерческий
директор
ARinteg

Менеджеры, сотрудники отдела продаж и не только они при отправке архивных файлов из организации предпочитают устанавливать на них пароли. Такое письмо может быть отправлено на общую почту партнёра, а пароль от архива по другому каналу связи получит тот, для кого эта информация предназначена.

Удобно — бесспорно, вот только обычная DLP-система не проконтролирует. Неслучайно защищённые паролем архивы считаются одним из распространённых каналов утечек конфиденциальной информации из компаний.

Это касается и персональных данных (ПДн), штрафы за утечки которых существенно возросли, что заставляет компании усиливать защиту конфиденциальных данных. В этом им помогает уникальный архиватор ARZip, который разработали в ARinteg, чтобы упростить жизнь специалистам по ИБ.

ARZip наделяет DLP способностью автоматически контролировать запарованные архивы и тем самым предупреждает утечки данных через них. Архиватор ARZip включён в реестр российского ПО № 15721.

КАК ARZIP ПОЗВОЛЯЕТ DLP «ВИДЕТЬ» АРХИВЫ НАСКВОЗЬ

Для того чтобы все 100 % запарованных архивов, отправляемых за периметр организации, DLP могла проконтролировать, компания

принимает решение о том, что ARZip становится её единственным корпоративным архиватором.

ARZip интегрируется по API с DLP и позволяет последней автоматизировать проверку запарованных архивов. Когда сотрудник в ARZip создаёт свой архив с паролем, архиватор передаёт ID архива и используемый пароль на сервер паролей — дополнительный сервис, предоставляемый ARinteg. При отправке такого запарованного архива из организации DLP обнаружит его в потоке данных и направит ARZip для распаковки. Получив обратно от ARZip данные, DLP проверит их в соответствии с политиками безопасности. Если архив не содержит конфиденциальных данных, то письмо сразу отправится адресату, в противном случае — попадёт в карантин.

В итоге процесс работы с запарованными архивами автоматизируется, офицерам безопасности не приходится вручную разбирать подобные карантинные файлы, исключается согласование отправки файла с конфиденциальной информацией по ошибке. Служба ИБ может использовать высвободившиеся ресурсы для решения других задач.

Архиватор совместим с основными популярными у российских корпоративных заказчиков ОС: Windows, Astra Linux, РЕД ОС, Alt Linux, Debian, РОСА Хром и др. Обеспечивает эффективность сжатия данных на уровне лучших мировых решений благодаря современным алгоритмам:

- ◆ архивирование ZIP, 7ZIP, TAR.GZ;
- ◆ разархивирование ZIP, RAR, 7ZIP, TAR, TAR.GZ, ARJ, CAB, DEB, ISO.

Архиватор мультиязычен, легко переключается с одного языка на другой: китайский, английский, армянский, арабский, татарский и т.д. При создании архивов в ARZip достаточно выбрать тип данных, которые сжимаются, и ARZip сам подберёт наиболее эффективный метод сжатия.

Широкие функциональные возможности, совместимость со многими распространёнными ОС, а также с популярными архивными форматами, гибкие сценарии интеграции делают ARZip эффективным инструментом, который позволяет усилить кибербезопасность компании и более рационально использовать имеющиеся ресурсы.

ARZip
АРХИВАТОР

Архиватор
ARZip

ВКЛЮЧЕН В РЕЕСТР ОТЕЧЕСТВЕННОГО ПО №15721 от 05.12.2022 г.

**ПРОКАЧАЙ
СВОЮ DLP!**

ЗАЩИТА ДАННЫХ И ПРОТИВОСТОЯНИЕ КИБЕРУГРОЗАМ

КАК ИЗБЕЖАТЬ ФИНАНСОВЫХ И РЕПУТАЦИОННЫХ ПОТЕРЬ



Василий СЕВОСТЬЯНОВ

начальник отдела технического сопровождения продаж компании «Доктор Веб»

Возможность ведения бизнеса с использованием облачных сервисов и аутсорсинга расширила поверхность атаки для злоумышленников, нацеленных на цифровые данные. Для обеспечения конкурентоспособности в киберсреде от служб информационной безопасности требуется комплексная модель защиты данных.

Актуальность темы защиты данных стремительно растёт. Широкое использование облачных сервисов, применение аутсорсинга, практика найма распределённых команд и использование инструментов удалённого доступа получили высокую оценку компаний. Но эти же изменения расширили поверхность атаки для злоумышленников, создавая для них новые «точки входа» для проникновения в инфраструктуру и несанкционированного доступа к данным.

Фишинг, эксплуатация уязвимостей в общедоступных сервисах, атаки на подрядчиков, низкий уровень сегментации сети и массовое применение устаревшего программного обеспечения представляют собой серьёзные угрозы. Классические

подходы защиты периметра уже не справляются с высокой сложностью атак на современные инфраструктуры.

Сегодня от служб информационной безопасности требуется комплексная модель защиты данных, которая включает в себя весь спектр доступных средств защиты информации. Она должна учитывать риск-ориентированные подходы, повышение осведомлённости персонала и активное взаимодействие с внешними источниками информации.

КАКИЕ АСПЕКТЫ УЧИТЫВАТЬ ПРИ ПОСТРОЕНИИ СИСТЕМ ЗАЩИТЫ ДАННЫХ

Как внешние, так и внутренние угрозы могут стать причиной нежелательных для бизнеса событий. Недобросовестные сотрудники или посторонние лица нередко получают доступ к важным данным «изнутри», без лишнего шума.

Жертвами становятся как крупные корпорации так и небольшие компании, где нет полноценного штата ИБ-специалистов. Можно не только «словить» шифровальщик, но и получить «в дополнение» несанкциониро-

ванные публикации на теневых ресурсах, кражу финансовых средств с расчётных счетов, внедрение криптомайнеров и др.

Например, при компрометации инфраструктуры поставщика ИТ-услуг злоумышленник попадает в инфраструктуру клиента. Такая схема особенно опасна, поскольку подрядчики обычно имеют привилегированный доступ для обслуживания системы.

Могут применяться атаки с использованием легитимных средств удалённого доступа и туннелирования. Финансово мотивированные злоумышленники используют AnyDesk, MeshCentral, Ngrok, Localtonet и подобные инструменты для долгосрочного присутствия в инфраструктуре.

Заметно расширилось использование шифровальщиков-вымогателей. Классическая схема с получением выкупа за расшифровку скомпрометированных данных обогатилась за счёт распространения исходных кодов различных вредоносных средств, таких как LockBit, Babuk и прочих.

Деструктивный хактивизм прочно занимает почётное третье место (после финансовой заинтересованности и промышленного шпионажа) по мотивации злонамеренных действий. Если несколько лет назад злоумышленники ограничивались «пропагандистскими» действиями, то сегодня они не чураются отказов в обслуживании, уничтожения данных и порчи инфраструктуры.

Всё чаще используются легитимные инструменты для постэксплуатации. Для скрытной загрузки



ки и запуска других вредоносных модулей активно используются PowerShell, PsExec, CrackMapExec, WMIExec и различные скриптовые интерпретаторы (Python, NodeJS, JavaScript).

Компрометация инфраструктуры может начинаться с утечки учетных данных (пароль, токен, ключ) — с использованием таких инструментов, как Mimikatz, LaZagne, XenArmor All-In-One Password Recovery Pro, а также из сообщений мессенджеров (чаще всего Telegram) и хранилищ браузеров.

Перед массовым шифрованием злоумышленники пытаются найти и удалить резервные копии данных или зашифровать также и резервные хранилища, чтобы оказать более сильное давление на жертву и исключить возможность быстрого восстановления инфраструктуры.

Очевидно, что меры защиты информации должны быть выстроены на опережение действий злоумышленников и учитывать полный жиз-

ненный цикл кибератаки: от разведки и начального проникновения до финального уничтожения, шифрования или кражи данных.

АКТУАЛЬНЫЙ ВЕКТОР АТАКИ. СПОСОБ, МЕТОД И СРЕДСТВО ПРОНИКНОВЕНИЯ В СИСТЕМУ

По мнению исследователей «Доктор Веб», среди векторов атаки на российские организации уверенно лидируют фишинг и социальная инженерия. На них приходится до 60 % атак. Зачастую злоумышленники в письмах представляются сотрудниками государственных организаций, банков, налоговых ведомств или силовых структур. Также набирает популярность практика использования легитимных почтовых ящиков скомпрометированных организаций для дальнейших фишинговых атак.

Источником повышенного риска стало широкое распростране-

ние различного иностранного ПО, лишившегося поддержки и официальных обновлений на российском рынке (такого как Microsoft Exchange, Atlassian Confluence, Oracle WebLogic, Citrix ADC и прочих). Злоумышленники целенаправленно занимаются сканированием открытых сетевых сегментов в поисках таких сервисов и массово пытаются эксплуатировать их известные уязвимости.

Значительная доля успешных атак приходится на доступ в защищаемый периметр инфраструктуры через взлом подрядной организации, имевшей более низкие стандарты безопасности в сравнении со своим нанимателем.

Отдельным значимым вектором атак является нарастающая тенденция на компрометацию с целью скрытого майнинга криптовалют. Такие действия могут оставаться незамеченными в течение продолжительного времени, при этом приводя к снижению быстродей-

Требуется реальная комплексная защита. Мы предлагаем использовать линейку сертифицированных ФСТЭК России продуктов Dr.Web Enterprise Security Suite, которые позволяют защитить и рабочие станции, и серверы, и трафик

ствия систем и прямым убыткам для бизнеса.

Также получили широкое распространение кража учётных данных и внедрение «закладок». Проникновение с использованием перехваченных учётных данных (зачастую с помощью инструментов для дампа LSASS или захвата сохранённых паролей из браузеров), с дальнейшим закреплением в системе с использованием легитимных средств — таких как Ngrok, Localtonet — позволяет сохранять доступ даже после изменения пароля.

НЕОБХОДИМОСТЬ МНОГОУРОВНЕВОЙ СХЕМЫ ПРОТИВОДЕЙСТВИЯ И КОМПЛЕКСНЫХ МЕР

Защита данных — процесс, требующий постоянной адаптации к новым киберугрозам. Опыт «Доктора Веб» показывает, что у злоумышленников не иссякает набор инструментов для получения доступа к корпоративным сетям: социальная инженерия, фишинг, эксплуатация старых уязвимостей, обход систем безопасности через легитимные удалённые приложения и т.д.

«Доктор Веб» также рекомендует организовать комплексный контроль учётных записей, внедрить средства многофакторной аутентификации (MFA) для всех служебных учётных записей и внешних сервисов. Проводить регулярную ревизию всех повышенных привилегий, руководствуясь принципом «минимально необходимого доступа», что сократит масштаб ущерба в случае компрометации.

Обязательно применять средства антивирусной защиты, регулярно обновлять как базы сигнатур, так и сами антивирусные компоненты для противодействия актуальным угрозам. Рекомендовано проводить плановые проверки АРМ и файловых хранилищ для выявления и удаления вредоносного ПО, которое могло скрытно проникнуть в инфраструктуру. Постоянно контролировать результаты антивирусных проверок, фиксировать инциденты в системе учёта, разбирать причины по каждому инциденту и формировать рекомендации по улучшению мер безопасности. Для повышения вероятности выявления вредоносного ПО — применять антивирусы различных вендоров на разных уровнях инфраструктуры (на файловых серверах, почтовых серверах, интернет-шлюзах, рабочих станциях, мобильных устройствах).

Важное значение имеет постоянное выявление уязвимостей с применением средств автоматизации и плановые тесты на проникновение для своевременного выявления уязвимостей на периметре и в общедоступных сервисах. А также установка обновлений для всего применяемого прикладного и системного программного обеспечения, с отслеживанием публикаций о выявлении уязвимостей в пределах защищаемого периметра. Сегментация сети с выделением критических систем в отдельные сетевые сегменты, недоступные извне нужна для затруднения распространения доступа злоумышленников при компрометации систем.

Реализовать концепцию «нулевого доверия» через проверку всех пользователей и устройств, независимо от их положения в сети, а также минимизацию коммуникаций между сегментами. Ограничение до минимально необходимых внешних подключений к СУБД и системам резервного копирования резко снижает риски масштабной компрометации.

Необходимо регулярно (и желательно автоматизированно) проверять целостность резервных копий, а также иметь актуальный отработанный план восстановления инфраструктуры из резервных копий. Сами резервные копии должны храниться в изолированной среде или оффлайн для исключения возможности их уничтожения или шифрования.

Цифровая грамотность персонала поможет минимизировать человеческий фактор в вопросах социальной инженерии и схожих методов). Тренинги, имитационные фишинговые рассылки и простой алгоритм уведомления о подозрительной почте существенно снизят риск реализации данного вектора атаки.

Нужно контролировать доступ к облачным сервисам. Это подразумевает ограничение доступа к API-интерфейсам и применение сильных механизмов аутентификации для защиты облачной инфраструктуры. Необходим регулярный аудит применяемых конфигураций, особенно при использовании автоматических конвейеров сборки (CI/CD).

Следование вышеприведённым рекомендациям и применение современных средств защиты позволят вывести защиту данных в организации за рамки формальных требований регуляторов и превратить её в реальный инструмент предотвращения финансовых и репутационных потерь, обеспечивая устойчивое развитие и конкурентоспособность любой организации в цифровой среде.

ЗАЩИТА ДАННЫХ КАК РАБОТА ОРКЕСТРА

SOAR-РЕШЕНИЯ ОБЪЕДИНЯЮТ АВТОМАТИЗИРОВАННЫЕ ПРОЦЕССЫ В ЕДИНУЮ СИСТЕМУ



**Роман
ДУШКОВ**
Security Vision

Защита данных – это ИБ-процесс, который может включать в себя целые комбинации СЗИ и подходов к обеспечению безопасности. Для начала рассмотрим те технологии, которые применяются для защиты:

◆ С одной стороны, вирусы, шифровальщики, программы-вымогатели и другие типы вредоносного ПО могут повредить файлы и сделать их недоступными для пользователей и процессов. Для обеспечения целостности и доступности данных используются средства резервного копирования и восстановления (Backup), обнаружения (SIEM, IDS) и предотвращения (SIEM, IDS/IPS, AV/EDR)

атак. Сами данные могут быть связаны с конкретными активами (AM/CMDB), что можно учитывать при оценке критичности, а также быть «прикрыты» дополнительными слоями средств защиты, вроде брандмауэров (FW, NGFW), веб-приложений (WAF, anti-DDoS).

◆ С другой стороны, нужно обеспечивать конфиденциальность данных и обеспечивать предотвращение угроз, исходящих как от внешних злоумышленников, так и от внутренних пользователей с доступом. Для этого применяют средства и подходы управления доступом (IAM, MDM), мониторинга возможных утечек (ILD) и проактивной защиты (DLP, CASB). Нужно помнить также, что нарушение конфиденциальности может быть связано и со «случайными» рисками, поэтому пригодятся риск-ориентированный подход и интеграция SGRC-процессов.

Опишем участие этих технологий в процессе защиты на примере хорошо изученного процесса – атаки шифровальщика на корпоративную сеть через спам: пользователь скачивает подозрительный файл из внеш-

него письма, EDR помечает его как потенциально вредоносный, Sandbox запускает дополнительную проверку, SIEM фиксирует аномалии в поведении пользователя. Таким образом, реализуется обнаружение и подтверждение угрозы, далее происходит реакция: FW/NGFW определяет и изолирует IP-адрес, ОС блокирует учётную запись пользователя через каталоги (AD), а при помощи микро-сегментации происходит изоляция заражённого устройства. Далее следуют этапы анализа и восстановления: VS/VM проверяет, не использовал ли шифровальщик известные уязвимости, если обнаружена уязвимость AM/CMDB система автоматически применяет патч, а Backup-система восстанавливает зашифрованные файлы.

Приводя множество примеров СЗИ и описывая одну из атак, мы хотели показать, что защита данных – это многослойный процесс, включающий как усилия специалистов, работающих с этими данными, так и технологии защиты, основанные на различных подходах. Среди приведённых примеров можно встретить системы, развивающиеся «агентские»

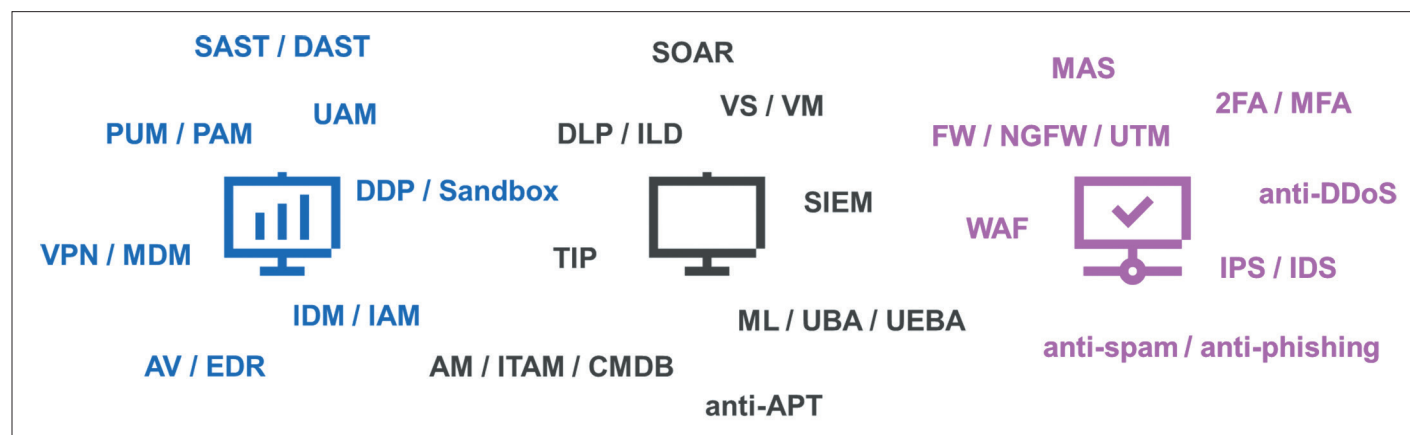


Рисунок 1.

(т.е. имеющие более близкий контакт с данными через программу, установленную на компьютере или сервере), сетевые и смешанные решения. Даже при попытке разделить все продукты на 2 лагеря возникает так много пересечений функционала и возможностей. Если добавить к этому конкуренцию, то с трудом можно разделить их на три блока (см. рис. 1).

Финальным пунктом в обзоре технологий становится тот факт, что для финансовой выгоды и снижения рисков весь процесс защиты данных становится многовендорным, т.е. включает десятки разных поставщиков технологий и тысячи экспертных мнений. Все участники, как различные музыкальные инструменты большого оркестра, пытаются вместе играть общую мелодию. Сам процесс затрудняется не только различиями в подходах, но и необходимостью знать, как играть на каждом инструменте. Переводя на язык технологий — требуется знать интерфейс и уметь пользоваться каждым средством защиты.

Мы рассказали про десятки классов систем, которые могут быть вовлечены в процесс защиты, и указали на определённую сложность этого процесса — все системы должны работать вместе и не просто не мешать друг другу, но обмениваться данными и обладать каким-то единым (или хотя бы похожим друг на друга) интерфейсом. На текущем этапе развития ИТ и ИБ, даже при высочайшем уровне регулирования, это невозможно технически, поэтому для управления «оркестром» используются решения класса SOAR, из названия которого (Security Orchestration, Automation and Response) буквально исходит наше музыкальное сравнение.

Security Vision предлагает модульные решения для набора требуемого функционала. Например, SOAR может быть эффективно дополнен модулями управления активами и уязвимостями (для управления CIA-параметрами, определения SLA и приоритизации всех задач), взаимодействия с регуляторами (для привлечения в процесс защиты данных

центров реагирования ГосСОПКА и ФинЦЕРТ), поведенческого анализа и анализа угроз (UEBA, TI). Сами по себе эти модули не являются средствами защиты информации, но позволяют собрать вместе частички паззла и разрозненные данные, а также облегчить работу аналитикам.

Как мы уже упоминали ранее, бизнесу важно не просто сохранить данные, а учитывать финансовые последствия и другие риски. Например, добавляя в экосистему новые решения, можно основывать выбор на сравнении их стоимости и последствий потери данных и других рисков. В таком случае методы оценки рисков типа Монте-Карло и другие количественные оценки с переводом в финансы позволят собрать для себя подходящую группу продуктов.

Рассмотрим участие различных решений и модулей Security Vision в процессе оркестрации на нескольких простых примерах:

◆ Потенциальная утечка данных: системы контроля доступа IAM и MDM запускают проверки на выполнение политик, DLP-система может автоматически ограничить доступ к файлам и передаёт сведения в единый центр управления SV SOAR. В более сложных ситуациях ILD система и работа экспертов по анализу позволяют обнаружить источник утечки, например, по фотографии в сети, и также при помощи коннекторов передает эту информацию аналитикам.

◆ Реагирование на инциденты: SIEM или другое средство защиты выявляет угрозу, ИТ-специалист устраняет её по заявке от службы ИБ. В более сложной цепочке — больше участников. Например, SV UEBA фиксирует аномалию, аналитик подтверждает её анализом индикаторов компрометации и угроз при помощи SV TIP, далее SV SOAR запускает весь процесс.

◆ Патч-менеджмент: поиск уязвимостей при помощи сканеров (SV VS, SV SPC), интеграция с базами уязвимостей CVE, автоматическое развертывание обновлений на уязвимые системы через средства управления активами (SV AM) и/или создание тикетов в системе управления зада-

чами (SV VM, SD/ITSM) и автоматическое оповещение сотрудников.

Из этих примеров отлично видно, что любой процесс стартует с детектирования средствами защиты, но вовлекает все больше участников, данных и процессов. Поэтому применение зонтичных продуктов на примере модулей платформы Security Vision становится полезнее с ростом инфраструктуры и количества применяемых СЗИ. Более того, среди этих примеров нет ни одной цепочки, которая бы полностью покрывалась решениями одного вендора и имела хотя бы шанс на единый интерфейс и сквозной процесс. Поэтому в каждую из них можно встроить SOAR-решение, которое выполняет функции единого центра управления и оркестрирует всеми средствами защиты. Специальные конструкторы, входящие в состав платформы, позволяют кастомизировать не только внешний вид, но и настроить интеграцию с любыми источниками данных и средствами реагирования.

Оркестрация объединяет несколько автоматизированных процессов в единую систему, позволяя управлять ими централизованно и согласованно. Она важна для координации действий между различными инструментами и системами безопасности, поскольку при наличии десятков систем возможны тысячи комбинаций.

Дополнительно SOAR обеспечивает автоматизацию, например, запускает сценарий реагирования, собирает данные из любых СЗИ в единое окно, отправляет нужные оповещения и связывается с регуляторами по установленным каналам для сбора и отправки нужных сведений.

Это позволяет в общем:

- ◆ Снижать риск ошибок, связанных с человеческим фактором;
- ◆ Ускорять реакцию на угрозы;
- ◆ Оптимизировать использование ресурсов команды ИБ.

Работая как единое целое при помощи оркестратора и коннекторов, продукты любых вендоров могут бесшовно обмениваться данными, упрощая работу специалистов ИБ и ИТ-подразделений.

МЕЖДУ ДОМЕНАМИ

ОДНОНАПРАВЛЕННЫЕ ШЛЮЗЫ ОБЕСПЕЧИВАЮТ ПЕРЕДАЧУ ДАННЫХ ТОЛЬКО В ОДНОМ НАПРАВЛЕНИИ, ЧТО ИСКЛЮЧАЕТ ВОЗМОЖНОСТЬ ОБРАТНОЙ ПЕРЕДАЧИ ДАННЫХ И ФИЗИЧЕСКИ ПРЕДОТВРАЩАЕТ УТЕЧКИ



Вячеслав ПОЛОВИНКО
руководитель
направления
собственных
продуктов
АМТ-ГРУП

Рост объемов информации, циркулирующей между объектами критической инфраструктуры, а также между чувствительными объектами и сегментами и сетями (доменами) различного уровня доверия уже сегодня требует дополнительного контроля для предотвращения утечек защищаемых данных, повышения эффективности применения комплексных решений по защите информации.

Наличие в информационной инфраструктуре действенных инструментов контроля в рамках междоменного взаимодействия крайне важно для достижения следующих ключевых целей:

1. Защита конфиденциальной информации
2. Соблюдение нормативных требований
3. Защита от кибератак
4. Предотвращение утечек в будущем и повышение уровня защищенности

СТРАТЕГИЧЕСКАЯ ЗАДАЧА

Контроль утечек данных из критических сегментов — не только техническая необходимость, но и стратегическая задача для значительного количества современных организа-

ций и предприятий. Однако существующие средства предотвращения утечек достаточно узконаправлены и применяются ограниченно. Несмотря на то, что каждый тип СЗИ может эффективно выполнять свои функции на определенном технологическом участке, совместное гармонизированное использование СЗИ разных типов для предотвращения утечек реализуется достаточно редко, гораздо чаще какая-то одна задача решается одним классом СЗИ, а другие задачи — организационными мерами контроля за персоналом силами внутренних служб безопасности.

ОСНОВНЫЕ ОГРАНИЧЕНИЯ

Рассмотрим некоторые существующие ограничения применения СЗИ на примере их классов, наиболее часто используемых для решения указанных выше задач: межсетевых экранов (firewalls, МСЭ) и DLP (Data Loss Prevention), являющихся важными и значимыми компонентами системы защиты информации. Помимо того, что «в связке» на практике они применяются не так уж часто, их автономное применение, что более важно, существенно ограничивает их возможности, что делает их недостаточными для эффективного контроля за утечками данных в ходе междоменного обмена.

Можно выделить следующие основные проблемы автономного применения межсетевых экранов в контексте междоменного обмена:

♦ **Ограниченность в анализе данных.** Межсетевые экраны предназначены для контроля и фильтрации сетевого трафика на основе правил (например, IP-адресов, портов, протоколов). Они не анализируют

содержимое передаваемых данных, что делает их уязвимыми для утечек, скрытых в разрешенном трафике.

♦ **Отсутствие защиты от инсайдеров.** Межсетевые экраны не могут предотвратить утечки, вызванные действиями авторизованных пользователей, которые имеют доступ к данным и передают их через разрешенные каналы (например, электронную почту, файловый обмен).

♦ **Уязвимости программных решений.** Современные методы атак, такие как туннелирование через разрешенные протоколы (например, DNS, HTTPS), демонстрируют системный и планомерный обход функций защиты межсетевых экранов.

DLP-системы при автономном применении в контексте междоменного обмена также имеют определенные проблемы:

♦ **Большая зависимость от контекста.** DLP-системы анализируют содержимое данных и пытаются выявить конфиденциальную информацию. Однако они могут пропускать утечки, если данные зашифрованы, замаскированы или передаются в нестандартных форматах. Поэтому обмен с применением таких решений должен быть максимально типизирован и не должен организовываться только на уровне организации соединений L3-L5 модели OSI.

♦ **Ложные срабатывания и пропуски.** DLP-системы сталкиваются с проблемой ложных срабатываний (блокировка легитимных данных) и пропусков (необнаружение реальных утечек), особенно, в сложных сценариях передачи данных. Поэтому целесообразно иметь хотя бы базовые дополнительные меры на средствах междоменного обмена (дополнитель-

Однонаправленные шлюзы невозможно обойти с помощью программных методов, так как они работают на аппаратном уровне, что ограничивает эксплуатацию иных протоколов, кроме прямо разрешённых

ные проверки на тип, размер файла, интенсивность обмена, регламентное время передачи), которые могут компенсировать возможные ложные позитивные или негативные срабатывания.

В случае использования интегрированных решений (МСЭ + DLP) полученные схемы междоменного обмена также не будут лишены недостатков:

- ♦ **Отсутствие физической изоляции.** Межсетевые экраны и DLP-системы работают на программном уровне и не обеспечивают физической изоляции сетей. Злоумышленник или вредоносное ПО может обойти эти средства, используя уязвимости в программном обеспечении или неправильно настроенные правила.

- ♦ **Не защищают от обратного трафика.** Межсетевые экраны и DLP-системы не могут полностью исключить возможность обратного подключения к защищенной сети, что делает их уязвимыми к атакам извне, и, в конечном итоге, позволяет организовать атаку на саму DLP-систему в целях ее отключения или компрометации.

- ♦ **Сложность управления в распределенных сетях.** В сложных сетевых инфраструктурах (например, с множеством филиалов или использованием облачных сервисов) обеспечение контроля за всеми каналами передачи данных становится крайне сложной задачей.

ПРЕИМУЩЕСТВА, КОТОРЫЕ МОЖНО ИСПОЛЬЗОВАТЬ

С учетом сказанного выше крайне важно выделить те преимущества, которыми обладают выходящие на рынок междоменные решения на базе однонаправленных шлюзов:

- ♦ **Физическая изоляция.** Однонаправленные шлюзы обеспечивают

передачу данных только в одном направлении, что исключает возможность обратной передачи данных и физически предотвращает утечки.

- ♦ **Усиленная защита от инсайдеров.** Даже если авторизованный пользователь попытается передать данные, однонаправленный шлюз в функциональности междоменного решения (МДР) не позволит этому произойти, если передача нарушает политики безопасности (тип, размер файла, регламент передачи, интенсивность трафика) и передаст информацию об инциденте подразделению ИБ.

- ♦ **Устойчивость к обходу при интеграции с DLP.** Однонаправленные шлюзы невозможно обойти с помощью программных методов, так как они работают на аппаратном уровне, что ограничивает эксплуатацию иных протоколов, кроме прямо разрешенных. В таких решениях однонаправленные шлюзы исключают возможность обратного подключения к защищенной сети, что делает их устойчивыми к атакам извне. Это особенно важно для критически важных инфраструктур, таких как промышленные системы, сети государственных учреждений, финансовых организаций. DLP-системы, интегрированные с такими шлюзами, получают еще один эшелон защиты. МСЭ также могут быть интегрированы с DLP-системами для дополнительного анализа передаваемых данных. Однако общие преимущества решений на базе однонаправленных шлюзов гораздо выше за счет более высокой стойкости получаемой системы к удаленным векторам атак. В частности, реализация удаленного вектора для компрометации DLP, которая находится в закрытом сегменте («перед диодом»), невозможна.

- ♦ **Повышение соответствия требованиям стандартов и законодательства («духу закона, а не только букве»).** Нормативные акты (например, ФЭ-152) требуют строгого контроля за передачей данных. Использование однонаправленных шлюзов в сочетании с DLP-системами помогает организациям более полно соответствовать этим требованиям, обеспечивая контроль как физического, так и логического доступа к данным.

- ♦ **Эффективное управление инцидентами.** DLP-системы, интегрированные с однонаправленными шлюзами, могут оперативно блокировать попытки передачи информации, которые нарушают политики безопасности. Дополнительными преимуществами таких срабатываний являются четкие и лаконичные данные журналирования и отчеты самих DLP-систем. Такие предметные сведения могут быть более системно и оперативно использованы специалистами ИБ для анализа инцидентов и улучшения политик безопасности.

АКТУАЛЬНОСТЬ ДЛЯ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ (ВКЛЮЧАЯ КИИ)

Очевидно, несмотря на то что межсетевые экраны и DLP-системы сами по себе являются важными инструментами защиты, они не обеспечивают полного контроля за утечками данных из-за своих ограничений. Однонаправленные шлюзы дополняют эти средства, обеспечивая изоляцию потока данных на аппаратном уровне и исключая возможность обхода защиты. Интеграция однонаправленных шлюзов с системами предотвращения утечек информации (DLP) предоставляет ряд значительных преимуществ, создавая мощный механизм предотвращения утечек данных, в котором «физическая» изоляция сочетается с продвинутым анализом передаваемого контента. Это особенно актуально для организаций с повышенными требованиями к безопасности, в том числе объектов критической информационной инфраструктуры, в системно-значимых организациях.

ОБ УСИЛЕНИИ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЕ ПОРЯДКА ОБРАБОТКИ ПДн

АРГУМЕНТЫ И ФАКТЫ



**Николай
ПЕРЕМЫШЛЕННИКОВ**
эксперт BIS Journal

ОБ ИЗМЕНЕНИЯХ В ЗАКОНОДАТЕЛЬСТВЕ

30 ноября 2024 года принят Федеральный закон № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (далее — 420-ФЗ), который вступит в силу 30 мая 2025 года, по истечении 180 дней со дня опубликования на официальном интернет-портале правовой информации.

Нововведения в первую очередь направлены на существенное усиление ответственности операторов за нарушения порядка обработки персональных данных, а не только на борьбу с утечками и их последствиями, как позиционировалось на стадии публичного обсуждения соответствующего законопроекта.

В числе прочего частями 11–18 дополнена статья 13.11 Кодекса Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (далее — КоАП РФ) устанавливающая ответственность и размеры налагаемых штрафов.

В зависимости от установленной категории административного правонарушения, предусмотрено наложение штрафа за:

- ◆ невыполнение или несвоевременное выполнение оператором предусмотренной законодательством Российской Федерации в области

персональных данных обязанности по уведомлению уполномоченного органа по защите прав субъектов персональных данных о намерении осуществлять обработку персональных данных, а также в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных;

- ◆ действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей персональные данные (включая специальную категорию персональных данных, а также биометрические персональные данные (за исключением случаев, предусмотренных статьей 13.11.3 КоАП РФ), если такие действия (бездействие) не содержат признаков уголовно наказуемого деяния, а также за совершение соответствующих им повторных правонарушений.

Сведения о принятых изменениях консолидированы в таблице (см. таблицу 1).

Немного предыстории.

С 2018 года в Российской Федерации наблюдается активный ежегодный рост числа совершаемых кибератак, направленных на кражу персональных данных, а также фактов проведения в отношении субъектов

персональных данных мошеннических действий, способы их реализации становятся все более разнообразными. В силу определенного накопительного эффекта это привело законодателей к выводу о неэффективности предпринимаемых мер, направленных на предотвращение подобных атак и на минимизацию последствий их реализации.

Во многом принятые меры — вынужденная альтернатива бездействию. Возникает вопрос, могут ли и при каких условиях эти нововведения переломить негативные тенденции в борьбе с утечками данных в современных реалиях. Однозначно проблема требует рассмотрения отдельных своих аспектов под углом зрения разных субъектов экономики данных. В первую очередь речь пойдет о крупных операторах обработки персональных данных, поскольку утечки их инфраструктуры в следствии масштаба и охвата клиентской базы вносят в статистику наибольший вклад.

Безусловно, в крупных компаниях ужесточение штрафов за совершение правонарушений по работе с персональными данными привлечет внимание высокопоставленных руководителей к вопросам организации и выстраивания эффективной защиты персональных данных. Сыграют свою роль и репутационные риски. Но надо понимать, что это существенно увеличит бюджеты на обеспечение информационной безопасности лишь в компаниях, которые: а) раньше не уделяли этим вопросам должного внимания, б) располагают достаточным объемом средств, чтобы не перенаправлять их с более актуальных бизнес-задач. При этом выделенные бюджеты будут использованы эффективно только при условии, что такие компании кардинально пе-

№ п.п.	Характер нарушения	Категория субъектов применения штрафа	Размер административного штрафа
1	Часть 10. Невыполнение или несвоевременное выполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по уведомлению уполномоченного органа по защите прав субъектов персональных данных о намерении осуществлять обработку персональных данных	Граждане физические лица	от пяти тысяч до десяти тысяч рублей
		Должностные лица	от тридцати тысяч до пятидесяти тысяч рублей
		Юридические лица	от ста тысяч до трехсот тысяч рублей
2	Часть 11. Невыполнение или несвоевременное выполнение оператором предусмотренной законодательством Российской Федерации в области персональных данных обязанности по уведомлению уполномоченного органа по защите прав субъектов персональных данных в случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных	Граждане физические лица	от пятидесяти тысяч до ста тысяч рублей
		Должностные лица	от четырехсот тысяч до восьмисот тысяч рублей
		Юридические лица	от одного миллиона до трех миллионов рублей
3	Действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей персональные данные (если эти действия (бездействие) не содержат признаков уголовно наказуемого деяния):		
3.1	часть 12: от одной тысячи до десяти тысяч субъектов персональных данных и (или) от десяти тысяч до ста тысяч идентификаторов	Граждане физические лица	от ста тысяч до двухсот тысяч рублей
		Должностные лица	от двухсот тысяч до четырехсот тысяч рублей
		Юридические лица	от трех миллионов до пяти миллионов рублей
3.2	часть 13: от десяти тысяч до ста тысяч субъектов персональных данных и (или) от ста тысяч до одного миллиона идентификаторов	Граждане физические лица	от двухсот тысяч до трехсот тысяч рублей
		Должностные лица	от трехсот тысяч до пятисот тысяч рублей
		Юридические лица	от пяти миллионов до десяти миллионов рублей
3.3	часть 14: более ста тысяч субъектов персональных данных и (или) более одного миллиона идентификаторов	Граждане физические лица	от трехсот тысяч до четырехсот тысяч рублей
		Должностные лица	от четырехсот тысяч до шестисот тысяч рублей
		Юридические лица	от десяти миллионов до пятнадцати миллионов рублей

Таблица 1. Сведения о принятых изменениях (продолжение на следующей странице)

рассмотрели применяемые подходы к обеспечению кибербезопасности и сделают ее постоянное совершенствование одной из приоритетных задач развития и поддержания бизнеса. В самом лучшем случае при максимальном вовлечении в процесс квалифицированных сил и ресурсов эффект все равно не будет мгновенным, а за тот год (или два) могут произойти инциденты, если не обесценивающие, то во всяком случае сильно снижающие ценность результата, с которым принято сравнивать затраты на его достижение. А еще следует понимать, что впоследствии все равно никаким инвестированием (вне зависимости от его объема) не будут на сто процентов гарантированы ни отсут-

ствие инцидентов, связанных с утечками данных, ни полное нивелирование последствий таких инцидентов.

Отметим, что на сегодняшний день к финансовым организациям на протяжении многих лет уже применяется множество регуляторных требований, в том числе обязывающих проходить периодические проверки соответствия установленным требованиям безопасности.

Помимо прочего финансовые организации (как минимум, крупные игроки на рынке, конкуренция между которыми достаточно велика) вынуждены принимать в расчет также и репутационные риски, во избежание оттока действующих и снижения темпов привлечения новых клиен-

тов. Они вынужденно, без дополнительных законодательных стимулов заинтересованы в построении и скорейшей реализации адекватной системы защиты информации и поддержании ее на должном уровне. Как следствие, в таких организациях ни расширение классификатора правонарушений, ни ужесточение административных штрафов за них не увеличат объем эффективных инвестиций в информационную безопасность, поскольку этот объем скорее всего уже достиг тех значений, которые позволяют развивать безопасность без ущерба для бизнес-функции организации. Напротив, по факту утечки данных в силу самого факта утечки, даже в случае объектив-

№п.п.	Характер нарушения	Категория субъектов применения штрафа	Размер административного штрафа
4	Часть 15. Совершение административного правонарушения, предусмотренного частями 12–14 настоящей статьи, лицом, подвергнутым административному наказанию за административные правонарушения, предусмотренные частями 12–14, 16–18 настоящей статьи и настоящей частью	Граждане физические лица	от четырехсот тысяч до шестисот тысяч рублей
		Должностные лица	от восьмисот тысяч до одного миллиона двухсот тысяч рублей
		Юридические лица	от 1 до 3 процентов совокупного размера суммы выручки, полученной от реализации всех товаров (работ, услуг), за календарный год, предшествующий году, в котором было выявлено административное правонарушение, либо за предшествующую дате выявления административного правонарушения часть календарного года, в котором было выявлено административное правонарушение, если правонарушитель не осуществлял деятельность по реализации товаров (работ, услуг) в предшествующем календарном году, либо размера собственных средств (капитала) кредитной организации на дату совершения административного правонарушения, но не менее двадцати миллионов рублей и не более пятисот миллионов рублей
5	Часть 16. Действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей специальную категорию персональных данных:	Граждане физические лица	от трехсот тысяч до четырехсот тысяч рублей
		Должностные лица	от одного миллиона до одного миллиона трехсот тысяч рублей
		Юридические лица	от десяти миллионов до пятнадцати миллионов рублей
6	Часть 17. Действия (бездействие) оператора, повлекшие неправомерную передачу (предоставление, распространение, доступ) информации, включающей биометрические персональные данные, за исключением случаев, предусмотренных статьей 13.11.3 настоящего Кодекса	Граждане физические лица	от четырехсот тысяч до пятисот тысяч рублей
		Должностные лица	от одного миллиона трехсот тысяч до одного миллиона пятисот тысяч рублей
		Юридические лица	от пятнадцати миллионов до двадцати миллионов рублей
7	Часть 18. Совершение административного правонарушения, предусмотренного частью 16 или 17 настоящей статьи, лицом, подвергнутым административному наказанию за административные правонарушения, предусмотренные частями 12–17 настоящей статьи и настоящей частью	Граждане физические лица	от пятисот тысяч до восьмисот тысяч рублей
		Должностные лица	от одного миллиона пятисот тысяч до двух миллионов рублей
		Юридические лица	от 1 до 3 процентов совокупного размера суммы выручки, полученной от реализации всех товаров (работ, услуг), за календарный год, предшествующий году, в котором было выявлено административное правонарушение, либо за предшествующую дате выявления административного правонарушения часть календарного года, в котором было выявлено административное правонарушение, если правонарушитель не осуществлял деятельность по реализации товаров (работ, услуг) в предшествующем календарном году, либо размера собственных средств (капитала) кредитной организации на дату совершения административного правонарушения, но не менее двадцати пяти миллионов рублей и не более пятисот миллионов рублей

Таблица 1. Сведения о принятых изменениях (окончание)

ного отсутствия вины компании, ее средства будут вынужденно расходоваться на уплату штрафов (а не на выплаты субъектам персональных

данных, чьи права были нарушены), что может привести к недофинансированию в том числе статей расходов на информационную безопасность.

При этом следует заметить, что далеко не каждая компания, даже в случае ее экономической заинтересованности, сможет себе позволить

бюджетировать и обеспечить полноценное выполнение установленных на регуляторном уровне требований по защите персональных данных, сколько угодно сопоставимых с реализацией системы защиты в крупных организациях. А как известно уровень защиты любой системы определяется уровнем защиты ее наименее защищенного компонента. Возможно, если не прежде, то одновременно с проработкой штрафных санкций следует обратить внимание и на то, что отдельные требования в ряде действующих профильных документов регуляторов не обновлялись в течение весьма продолжительного времени, и как следствие, не адаптированы к применяемым в современных реалиях ИТ-технологиям и не отражают эффективных способов или направлений их защиты. При этом нормативное регулирование осуществляется на уровне нескольких ведомств одновременно (зачастую рассинхронизированно), и многие требования в отношении одних и тех же процессов, и направлений защиты информации излагаются в альтернативных формулировках (а потом проверяются по несколько раз одним ведомством за другим, отвлекая как ресурсы проверяющих, так и проверяемых).

КАК ЕЩЕ МОЖНО ДВИГАТЬСЯ В НАПРАВЛЕНИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПРОТИВОДЕЙСТВИЯ УТЕЧКАМ ДАННЫХ

Прежде всего, понимая количество и объемы фиксируемых утечек данных и динамику этого показателя в современных реалиях, следует уделить особое внимание работе, направленной на повышение раскрываемости киберпреступлений, связанных с кражей и (или) распространением (в том числе неконтролируемым или реализуемым путем продажи) утекших данных, усилиям в отношении выявления и пресечения соответствующей деятельности со стороны незаконных цифровых сообществ, иных подобных им формирований и подконтрольных им лиц, совершающих вышеуказанные

правонарушения (далее — мошеннические сообщества), а также максимального ужесточения наказания виновных за целенаправленное осуществление мошеннической деятельности. Наряду с организацией и выстраиванием межведомственного взаимодействия на различных уровнях, координируемых из единого центра противодействия кибермошенничеству, выполняющего роль центра соответствующих компетенций, целесообразно активнее применять меры подавления мошеннических ресурсов, в том числе реализуемые с использованием проактивных методов «offensive security», например, кибератак на соответствующие ресурсы в Darknet. Реализация таких методов может осуществляться как силовыми ведомствами, так и с привлечением лицензированных организаций. Для повышения раскрываемости киберпреступлений целесообразно также отдельно рассмотреть возможность внедрения в мошеннические сообщества или имитации их деятельности с применением скомпилированных фейковых баз данных с целью выявления их органов управления, сети покрытия, источников распространения, заказчиков поставок и потребителей данных. В ходе расследования киберпреступлений следует предусмотреть реализацию процедур, посредством которых совместно (на уровне различных ведомств) будут проводиться разбирательства по каждому факту утечки данных с выявлением и анализом ее корневых причин и последствий, вырабатываться превентивные меры, направленные на своевременное выявление и нейтрализацию «слабых» мест в реализации защиты применяемых технологий, устанавливаться состав апостериорных мер, прежде всего, направленных на нейтрализацию неконтролируемого распространения утекших данных. Одновременно в виде конкретных требований или решений полезно тиражировать полученные знания и опыт в профильные организации с целью недопущения повторного применения выявленных схем реализации угроз безопасности ин-

формации и нейтрализации используемых ими уязвимостей.

В целях пресечения использования мошенниками информационных поводов, связанных с фактами массовой публикации и таргетированного распространения сведений об утечке данных из конкретной организации, как элемента психологического воздействия при реализации со стороны нарушителей методов социальной инженерии, а также предотвращения обусловленных такими поводами информационного резонанса и необдуманных действий со стороны субъектов персональных данных, публичное (массовое) распространение (включая неконтролируемое тиражирование) соответствующей информации о крупных утечках должно быть исключено до ее проверки и подтверждения компетентными органами. При этом субъекты персональных данных не должны быть поражены в правах на информацию, которая может уберечь их от ошибок и заставит действовать более осторожно.

В свою очередь, в качестве альтернативы некачественным источникам информации предлагается повысить привлекательность получения информации (за счет ее точности, актуальности, оперативности и объективности) от сервисов государственных информационных систем, таких как: «Единый портал государственных и муниципальных услуг (функций)» (gosuslugi.ru), систем электронных опросов, например, «Активный гражданин» или иных государственных справочно-информационных интернет-порталов, в том числе с учетом планов их развития и реализации на их платформе нового функционала. В зависимости от характера предоставляемых сведений такое информирование может осуществляться как персонализировано — посредством доступа к личному кабинету пользователя и размещения сведений, касающихся непосредственно субъекта персональных данных, так и коллективно — путем размещения общедоступной информации. Вышеуказанные сервисы и системы также могут быть

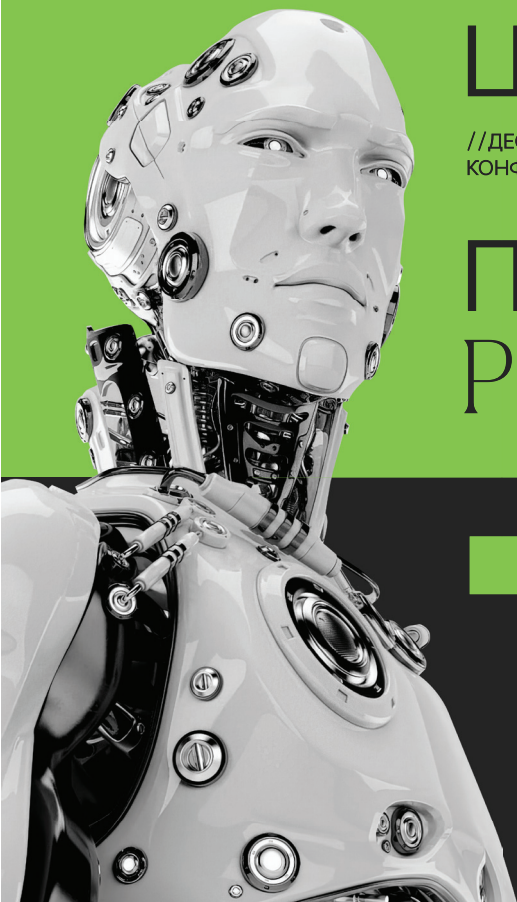
эффективно использованы не только как доверенный источник проверенной информации, но и как ресурсы для повышения киберграмотности населения, а также доведения до целевой аудитории в простой и наглядной форме правил цифровой гигиены для обеспечения личной безопасности в цифровом пространстве, противостояния социальной инженерии. Инструментами вовлечения граждан в данный процесс может служить рассылка коротких уведомлений из рубрики: «Знаете ли Вы, что ...», посредством которых на конкретных примерах будут разъясняться нормы поведения в цифровом пространстве с предложениями пройти экспресс-тестирование на определение своего уровня киберзрелости. Главное в подобных сервисах правильно выставить баланс «полезности — навязчивости» и обеспечить максимально интересный и полезный контент. Мотивацией могут слу-

жить введение рейтингов участников, успешно прошедших максимальное количество тестов за определенный интервал времени (например, за неделю) и поощрений лидеров в виде бонусов или иных вознаграждений, а также предоставления лицам, развившим интерес к кибертематике, доступа (подписок) на получение соответствующих информационных рассылок и дайджестов с актуальными новостями.

При организации работы с персональными данными, в дополнение к обязательным требованиям по минимизации состава атрибутов, собираемых и обрабатываемых данных, важно минимизировать источники централизованного получения доступа к консолидированным наборам персональных данных. В случае выгрузки данных из систем и компонентов систем централизованного хранения и обработки персональных данных применять меры в

целях обеспечения возможности последующего установления источника и объема выгруженных данных, а также субъектов или объектов доступа, осуществивших выгрузку таких данных.

Реализуя инициативу о введении оборотных штрафов для крупного бизнеса (как Quick win для формального достижения цели), следует максимально уточнить критерии оценки утечек данных и их последствий, определить, контролировать и на постоянной основе актуализировать рекомендуемые состав и содержание мер защиты информации по каждому направлению деятельности по защите персональных данных, соответствующие современным технологиям и применяемым техникам для предотвращения кибератак, а также продумать и реализовать компенсирующие меры, статус реализации которых будет учитываться при исчислении размера налагаемого штрафа.



ЦИФРОВАЯ

//ДЕСЯТАЯ ЮБИЛЕЙНАЯ
КОНФЕРЕНЦИЯ ЦИПР

ИНДУСТРИЯ ПРОМЫШЛЕННОЙ РОССИИ

// 3-6 ИЮНЯ, 2025

// РОССИЯ, НИЖНИЙ НОВГОРОД

CIPR.RU



ЦУГЦВАНГ ПО-РОССИЙСКИ

КАК ШТРАФЫ ЗА УТЕЧКИ ПРЕВРАТИЛИ БИЗНЕС В ИГРОКА, КОТОРЫЙ ПРОИГРЫВАЕТ В ЛЮБОМ РАСКЛАДЕ



Андрей
ЖАРКЕВИЧ
эксперт StartX

Представьте, что вы играете в шахматы. Любой ваш ход ухудшит позицию, но не ходить тоже нельзя — проиграете. Это и есть цугцванг. Теперь замените шахматную доску на российский бизнес, а фигуры — на защиту данных и штрафы за их утечки. Вуаля! Добро пожаловать в реальность, где компании, обрабатывающие персональные данные, оказались в роли игрока, которому законодатели предложили головоломку без правильного решения.

Количество утечек данных стремительно растёт. Системного решения проблемы на государственном уровне не нашлось, поэтому задачу делегировали бизнесу, действуя по принципу «больше боли — больше результата». Наказания ужесточили так, что у руководителей компаний начал развиваться нервный тик. Ведь даже предыдущую редакцию штрафов сложно назвать гуманной.

Отраслевые эксперты засуетились, массово выпуская гайды, чек-листы и таблицы с новыми санкциями — всё, чтобы помочь бизнесу не угодить под каток. Но если отбросить суммы штрафов, возникает вопрос: а что, собственно, изменилось? Как это поможет в борьбе с массо-

вой компрометацией конфиденциальной информации? Проблемы-то остались теми же.

ДЕФИЦИТ КВАЛИФИЦИРОВАННЫХ КАДРОВ

Если представить российский рынок ИТ и информационной безопасности как ресторан, то он напоминает заведение с бесконечным потоком гостей, но всего двумя поварами на кухне. Один из них увлечённо жарит яичницу, а второй пытается на колёнке собрать молекулярный десерт. А посетители тем временем стучат вилками и кричат: «Где наш стейк?» Примерно так выглядит ситуация с кадрами: спрос зашкаливает, а предложение едва тлеет.

Прочитирую CNews.

«...в России дичайший дефицит ИБ-специалистов. (...) Все хорошие уже заняты, а вузы выпускают «сырых». Количество резюме сокращается при одновременном росте числа открытых вакансий. На борьбу с дефицитом ИБ-кадров уйдут годы, и даже рост предлагаемых зарплат пока не помогает решить проблему. Все хорошие специалисты уже трудоустроены, а выпускников вузов нужно дообучать».

Почему дефицит стал хроническим?

Теория без практики — как суп без соли. Вузы долгое время готовили специалистов по шаблонам 2000-х: лекции о сетях на примере Windows XP, курсы по защите данных без упоминания облачных технологий. Пока учебные программы проходили согласования, мир уже перешёл на DevOps, AI и Zero Trust.

В итоге выпускники приходят в компании с багажом устаревших

знаний, и работодателям приходится тратить месяцы на их обучение. Многие предпочитают не связываться с новичками без опыта и перекупают готовых специалистов, которых и так не хватает. Получается замкнутый круг. Специалистов мало, новички никому не нужны, потому что ничего толком не умеют, но научиться им негде, потому что их не берут на работу.

ИБ — это сложно, дорого и не так интересно, как показывают в фильмах. Специалисты по безопасности — это «врачи» ИТ-мира: их ценят, только когда случилось что-то серьёзное — взлом, утечка, шифровальщик. Но чтобы влиться в ряды спецов по ИБ, нужно:

- ♦ постоянно учиться: хакеры не спят, а законодатели придумывают новые требования;

- ♦ работать в условиях стресса: один промах — и компания платит миллионные штрафы.

При этом зарплата junior-аналитика ИБ часто меньше, чем у junior-разработчика. И это обидно. А ещё ответственность, куча бумажной работы, от которой никуда не денешься, беспечные пользователи и суровые руководители. И никакой романтики, никаких сражений с коварными хакерами.

Компании экономят на безопасности. Как правило, руководство воспринимает ИБ как статью расходов, а не инвестиций. Зачем платить 150 тыс. руб. специалисту, если можно назначить «ответственным за всё» сисадмина за 80 тысяч? Зачем покупать новое оборудование, если у нас ещё старое не амортизировано (реальный вопрос от главного бухгалтера)? В результате настройка файрвола превращается в

бесконечный квест «как бы не сломать», а проактивная защита остаётся мечтой.

Миф о «всемогущем аутсорсе». Малый и средний бизнес часто нанимает ИБ-специалистов на аутсорсе, экономя бюджет. Но одна компания-подрядчик может обслуживать десятки клиентов, раскидывая ресурсы тоньше папиросной бумаги. Когда случается инцидент, оказывается, что «ваш куратор в отпуске», а резервных специалистов нет. А если и есть, им нужно время, чтобы погрузиться в детали вашей инфраструктуры и понять, что происходит.

Последствия

«Дырявые» системы и штрафы как норма жизни. Без квалифицированных кадров компании внедряют защиту «для галочки». Сертифицированный ФСТЭК шлюз настроен так, что пароль от админки — 123456, а к сетевому оборудованию можно подключиться из интернета через telnet. Результат предсказуем: утечки, штрафы, репутационные потери.

Перегрузка и выгорание. Один квалифицированный специалист тащит на себе три проекта, ночной мониторинг и поддержку SIEM. Рано или поздно он либо увольняется, либо допускает роковую ошибку. По данным опросов, больше половины ИБ-специалистов в РФ жалуются на хроническую усталость.

Рост киберпреступности. Хакеры прекрасно знают о кадровом голоде. Они атакуют малый бизнес и госсектор, где защита слабее всего. По данным Positive Technologies, «в III квартале 2024 года количество инцидентов увеличилось на 15 % по сравнению с III кварталом 2023 и незначительно уменьшилось (на 4 %) по сравнению с предыдущим кварталом. Утечки конфиденциальных данных наблюдались более чем в половине (52 %) случаев успешных атак на организации. Нарушение основной деятельности наблюдалось на 5 % чаще в связи с увеличением активности групп вымогателей».

ИМПОРТОЗАМЕЩЕНИЕ В ИБ: КОГДА «СДЕЛАНО У НАС» НЕ ЗНАЧИТ «СДЕЛАНО ХОРОШО»

Представьте, что вам нужно построить крепость, но вместо бетона и стали вы получили глину, солому и добрые напутствия. Примерно так выглядит попытка защититься от утечек данных с помощью импортозамещённых решений. Сертификаты есть, патристичный логотип и запись в реестре Минсвязи — тоже, но функциональность напоминает швейцарский сыр: дырок больше, чем самой защиты. Почему же «российское — значит надёжное» пока остаётся больше лозунгом, чем реальностью?

Технологическое отставание: не догоним, так хоть согреемся

Большая часть отечественных ИБ-решений, присутствующих в реестре Минцифры, создавались в спешке, под давлением санкций и политики цифрового суверенитета. Результат?

«Копипаст-технологии». Многие продукты представляют собой переупакованный open-source с добавлением пары модулей «для галочки». Например, DLP-системы, которые не умеют анализировать контекст сообщений, а лишь ищут шаблонные фразы вроде «секретно».

Слабая интеграция. Российский SIEM может не «дружить» с корпоративной почтой или CRM, превращая защиту в набор разрозненных инструментов.

По данным ежегодного исследования «СёрчИнформ» за 2024 год, основной трудностью импортозамещения остаются проблемы совместимости решений с текущим софтом и оборудованием и необходимость организации новой ИТ-архитектуры.

Тендеры: где побеждает не качество, а цена

Эту проблему знают все, но никто не придумал, как её решить. Госзакупки выигрывает самое дешёвое предложение. Это может показаться оправданным, поскольку у многих организаций нет денег на дорогие решения, даже если они более эффективны. Но тут появляется риск купить прими-

тивное решение, которое в современных условиях обеспечивает лишь иллюзию защиты. Или получить систему без поддержки.

Обновился — остался без сертификата

Ещё один тонкий момент — сертификация ФСТЭК. Для некоторых организаций использование сертифицированного оборудования и ПО обязательно. Но есть проблема. Сертификация предполагает фиксацию состояния ПО. Любое обновление меняет это состояние.

Таким образом, обновление — риск. Если вендор выпустит патч для закрытия уязвимости, продукт может потерять сертификат. Если не выпустит — систему могут взломать. Компании вынуждены выбирать между безопасностью или законностью.

Сделано в РФ, но... из китайских деталей

Даже «настоящее» импортозамещение часто зависит от иностранных компонентов. Российские серверы и маршрутизаторы собираются на чипах, закупленных через третьи страны. При санкциях поставки останавливаются — и производство встаёт.

Многие «отечественные» решения используют зарубежные библиотеки или фреймворки. Если GitHub или другой репозиторий заблокирует доступ, обновления превратятся в непроходимый лабиринт.

«Мы не умеем этим пользоваться»

Даже идеальное оборудование бесполезно без специалистов. Многие ИБ-специалисты учились на зарубежных продуктах (Cisco, Palo Alto). Переход на российские аналоги требует переподготовки, которую никто не оплачивает.

Но даже самостоятельно изучить не получится: инструкции к отечественному ПО иногда написаны так, будто их переводили с китайского через Google Translate. А изучить тестовую версию «российского ПО» тоже не получится: у большинства вендоров просто нет возможности загрузить пробные версии продуктов.

В итоге получается, что после внедрения российской SIEM сотрудники ЦОД не могут понять, как настроить правила корреляции. И героически сражаются с ложными алертами вместо того, чтобы заниматься действительно полезными вещами.

ЧЕЛОВЕЧЕСКИЙ ФАКТОР КАК ГЛАВНАЯ УГРОЗА ИБ

Ещё одна нерешённая проблема. Представьте: компания потратила миллионы на суперсовременную систему защиты с квантовым шифрованием и встроенным ИИ для анализа аномалий. А потом сотрудница бухгалтерии Нина Ивановна, получив письмо с текстом «Ваш пароль скомпрометирован! Срочно смените его, или будете уволены», вводит учётные данные для входа в корпоративную сеть на фишинговом сайте. И всё — крепость пала, враг проник в инфраструктуру.

Человеческий фактор как дыра в бронежилете: можно купить самую дорогую защиту, но пуля всё равно попадёт в незащищённое место. Люди остаются людьми: доверчивыми, любопытными, ленивыми и... обиженными на начальство.

Инсайдеры

Сотрудники сливают данные не только из-за доверчивости или лени. Причины бывают разными:

- ♦ Корысть. Продать базу клиентов на чёрном рынке, оказывать услуги по платному «пробиву».

- ♦ Шантаж. «Либо ты устанавливаешь нам софт, либо твоей дочери будет плохо».

- ♦ Месть. Перед увольнением сотрудник открывает доступ в корпоративную сеть и публикует логин и пароль на хакерском форуме.

Статистика: по данным «Информзащиты», в период с января по сентябрь 2024 года доля утечек данных из финансовых организаций из-за действий инсайдеров достигла 31 %. Это на 34 % ниже, чем за первые девять месяцев 2023 года, но на 28 % выше, чем в 2022 году. А всего с января по сентябрь 2024 г. в финансовом секторе зафиксировано около 500 случаев утечек данных.

А вот у регулятора другая статистика: Роскомнадзор зафиксировал за 2024 год 135 случаев утечки баз данных, в которых содержались более 710 млн записей о россиянах.

Защита мешает работать

Сотрудники ненавидят сложные пароли, которые надо менять каждые 30 дней, постоянные запросы на подтверждение действий. И уж тем более запрет на вход в личную почту с рабочего компьютера.

Итог: Нина Ивановна пишет пароль на стикере и клеит его на монитор или в секретное место — под клавиатуру. Чтобы не забыть.

Обучение? Нет, не слышали

Многие компании проводят «обучение ИБ» раз в год в формате «посмотрите этот 40-минутный ролик и распишитесь». Или даже просто проходят по кабинетам с бумажным журналом инструктажа и просят расписаться. Да, к сожалению, бывает и такое. Результат обескураживает:

- ♦ сотрудники путают фишинг с рыбалкой;

- ♦ двухфакторная аутентификация воспринимается как личное оскорбление;

- ♦ правило «не подключать флешки неизвестного происхождения» нарушается ровно через день после инструктажа.

Случай из жизни: «Мы проходили это в прошлом году. Зачем повторять? Всё и так понятно!» — говорит сотрудник, который только что ввёл логин-пароль на фишинговом сайте с опечаткой в адресе.

ЗАЩИТА ОТ ПРОВЕРКИ, А НЕ ОТ ВЗЛОМА

Поскольку решить проблему дефицита специалистов по ИБ в ближайшие 3–4 года точно не получится, а что-то сделать, чтобы не получить штраф, нужно до 30 мая, компании строят потёмкинские деревни из сертифицированного оборудования и ПО, нормативов и регламентов.

Внешне всё выглядит красиво: выполнен комплекс «правовых, организационных и технических мер», как того требует закон. Назначены от-

ветственные, выпущены приказы и регламенты, закуплены системы защиты (если хватило бюджета) или задействовано то, что есть (если подходит под требования закона).

Но только вот всё равно получилась бронированная дверь с сертификатом «Пуленепробиваемая!», в которую забыли врезать замок. Регламенты есть, бумаги подписаны, а злоумышленники всё равно гуляют по системе, как по парку. Почему? Потому что безопасность — это не про документы, а про то, как их исполняют.

Сертификация ≠ защита

Сертификат ФСТЭК или Минцифры — это как диплом о высшем образовании: он подтверждает, что продукт теоретически может работать. Но если админ настроил систему по мануалу 2015 года, не адаптируя её под текущие угрозы, поможет это примерно как изучение латыни перед экзаменом по квантовой физике.

Регламенты, которые никто не читал

Компании гордятся толстой папкой «Политик ИБ», но на деле:

- ♦ документы пишутся под копирку, без учёта специфики бизнеса;

- ♦ правила вроде «нельзя передавать пароли» соседствуют с практикой «Нина Ивановна, дайте мне ваш логин, я отчёт быстро заполню»;

- ♦ обновления регламентов откладываются до «после проверки», которая случится через год.

Случай из жизни. Сотрудник внутреннего контроля филиала банка просил сделать ему папку с документами, подписанную фамилией ИТ/ИБ-аудитора из головной организации, и положить туда все документы, которые требуется предъявить проверке, чтобы не было замечаний. Как всё организовано на самом деле, никто не проверял.

Админ-зомби: «Я месяц не спал, мне всё равно»

Бывает, что за настройкой защиты часто стоит перегруженный специалист, который в итоге настраивает SIEM-систему в 3 часа ночи, путая

правила «разрешить» и «запретить», а затем отключает часть функций, потому что «это тормозит систему, а начальник кричит».

Случай из жизни. В банке админ, спасая сервер от перегрузки, отключил проверку подозрительных исходящих подключений. Через неделю хакеры выкачали данные клиентов через тот самый порт.

На тесты нет времени, работать нужно

Многие компании проверяют защиту только в двух случаях: перед проверкой Роскомнадзора («Быстро сгенерируйте отчёт, что всё работает!») и после утечки («Как так вышло? Мы же купили систему защиты!»). Пентесты проводятся редко или никогда, потому что это дорого и нет времени. Да ещё и если найдут проблемы, придётся их устранять.

В итоге получается, что система считается безопасной, пока хакеры не докажут обратное.

Опасная иллюзия: «У нас всё по стандарту»

Следование стандартам и отраслевым практикам — это хорошо. Но когда компания фокусируется только на соответствии, забывая о сути, может получиться та самая бумажная безопасность, когда готовится папка «Для аудита», но работают как получится: резервные копии делаются, но не проверяются на восстановление, шифрование данных есть, но ключи хранятся в файле «passwords.txt» на рабочем столе.

ИТОГ

Ситуация не слишком вдохновляющая. Выполнять требования закона нужно, иначе можно стать жертвой утечки и получить за это суровое наказание. Что конкретно нужно делать — не очень понятно, если говорить о технической части требований закона. Людей, которые знают и могут настроить эффективную защиту от утечек, катастрофически мало. И если крупные компании с большой вероятностью найдут нужных специалистов среди штатных сотрудников, средний



и малый бизнес вынужден будет привлекать аутсорсеров. Которых на всех не хватит.

Непростая ситуация с импортозамещённым оборудованием и ПО — многие продукты из реестра Минцифры (пока?) уступают в функциональности и совместимости западным аналогам. «Отечественные» форки open-source-софта никто толком не умеет обслуживать, кроме их «создателей».

«Защита от проверки» работает до первого инцидента. Чтобы регламенты не стали фикцией, нужно настраивать системы под реальные угрозы, а не под требования бумажек, регулярно тестировать и обновлять защиту, обучать специалистов и беречь их время, не отвлекая бесконечным потоком посторонних задач.

Но даже если все эти проблемы каким-то чудом удастся решить, остаётся ещё одна угроза, которую принимают в расчёт по остаточному принципу, — человеческий фактор. Нейросети, блокчейн и квантовое шифрование не спасут от действий или бездействия людей. Причём речь не только об условной сотруднице

бухгалтерии, но и о суровом админе, который забыл вернуть безопасные настройки файрвола или не установил патч для критической уязвимости.

Сейчас компании, словно игроки в русскую рулетку, крутят барабан (пишут регламенты, издают приказы и назначают ответственных), надеясь, что пуля (читай: утечка или проверка) пролетит мимо. И дело не в том, что бизнес ленив или глуп. Просто очевидно, что даже идеальное следование правилам не гарантирует защиты — только отсрочку до следующего «выстрела».

Сертификаты, гайды, чек-листы, приказы и регламенты — это современные амулеты. Компании надеются, что с их помощью они отпугнут злых духов (Роскомнадзор), но забывают, что на хакеров ритуалы не действуют.

Соответствие формальным требованиям не спасает от хакеров, хотя и создаёт иллюзию контроля. Как говорил Оноре де Бальзак, «закон — это паутина. Крупные мухи сквозь неё прорываются, а мелкие — застревают».

«КИБЕРБЕЗ ПЕРЕСТАЛ БЫТЬ ЧЕМ-ТО КУЛУАРНЫМ И СТАНОВИТСЯ ЧАСТЬЮ ЖИЗНИ»

НА ВОПРОСЫ BIS JOURNAL ОТВЕЧАЕТ USERGATE



Сергей ПЕТРЕНКО

директор по работе с государственными структурами UserGate

— В 2024 году Роскомнадзор зафиксировал 135 случаев утечек баз данных, в которых содержалось более 710 млн записей о россиянах. Чем объясняются, на Ваш взгляд, такие большие объёмы утечек? Видите ли Вы тенденции к улучшению ситуации с безопасностью и целостностью данных?

— Последние годы в целом характеризуются ростом кибератак, которые достигали своих целей и нередко приводили к утечкам. Видимо, это стало отражением глобального тренда, обусловленного сложной геополитической ситуацией. Кроме того, истории с утечками ПДн оказались в фокусе внимания. Их активно стали обсуждать, может быть, в силу изменений в законодательстве или возрастания масштабов явления.

Могу только предположить, что ситуация будет стабилизироваться. Количество утечек ПДн, как минимум, должно перестать расти, по причинам, связанным с ужесточением законодательства и усилением мер защиты. Сами пользователи становятся более информированными и ищут способы себя обезопасить.

— В прошлом году был принят ряд поправок в законодательство, касающихся процесса обработки и защиты персональных данных. Какие из них Вы считаете наиболее важными и полезными?

Станут ли они стимулом для компаний пересмотреть своё отношение к защите данных в лучшую сторону?

— Действительно, наша законодательная ветвь власти подготовила свой ответ на угрозы, который представляется весьма своевременным. Теперь нарушение законодательства в сфере защиты ПДн чревато чувствительными последствиями, вплоть до потери бизнеса. В принципе вся индустрия кибербезопасности восприняла новые законодательные инициативы положительно, поскольку ранее ответственность за нарушения было крайне скромной и не воспринималось всерьёз операторами ПДн и не мотивировала их реально вкладываться в средства защиты.

Из важного безусловно выделю оборотные штрафы. Раньше штрафы не были существенными для физлиц должностных лиц, а штрафы для организаций вообще выглядели ничтожными. По моему личному убеждению, большинство компаний, с точки зрения защиты персональных данных, реализовывало стратегию принятия риска утечки. Сейчас в вопросе оборотных штрафов речь идёт об очень серьёзных суммах — с верхним ограничением на уровне 500 миллионов рублей. Добавим к этому также имиджевые потери. Теперь

операторам видится более целесообразным от стратегии принятия риска перейти к стратегии его минимизации.

Подготовленные законодателями изменения предусматривают как кнут, так и очень условный кончик, но пряник. Если у организации все-таки случится утечка ПДн, то потенциально большой штраф можно существенно сократить при наличии двух смягчающих обстоятельств, которые действуют одновременно. Первое — оператор на протяжении последних трех лет активно инвестировал в защиту ПДн и в целом в укрепление информационной безопасности.

И второе — оператор регулярно проводил аудит на предмет нормального функционирования ИБ. В итоге ситуация тоже должна измениться. Эти оборотные штрафы не самоцель: они должны запустить процесс, когда компании начнут вкладываться в ИБ, она начнет работать, и утечек, по факту, станет меньше.

— Считаете ли Вы достаточными принятые меры регулирования или следует ужесточить их еще больше, в частности в отношении преступников, по вине которых происходят утечки ПДн и неправомерное их использование?

— Помимо административного наказания, вводится уголовная ответственность в отношении злоумышленников (хакеров). Появились статьи за неправомерную обработку, передачу данных и т.д. Злоумышленником может быть и сотрудник оператора связи, но здесь уголовное право применимо исключительно к физлицам, к гражданам, а не к компании.

Так что на уровне законодательства ужесточили требования и к опе-

раторам, и к злоумышленникам, чтобы соблюсти некий баланс. Наверное, на текущий момент принятых мер достаточно: нельзя одномоментно делать очень большие изменения. Надо оценить эффект от принятых мер, прежде чем ужесточать их дальше.

— **Какие технические решения сегодня позволяют обеспечить надежную защиту от утечки данных? Какие возможности есть у компаний для того, чтобы предотвращать эти утечки или производить эффективные действия по минимизации ущерба?**

— В информационном, правовом поле России есть определённые требования по обеспечению безопасности информационных систем персональных данных, выпущенные регулятором в лице ФСТЭК России. Понятно, что есть еще требования отраслевые и так далее, но ФСТЭК России и ФСБ России — это два основных федеральных регулятора.

Уже достаточно давно существует приказ ФСТЭК № 21 о том, как надо защищать персональные данные. С точки зрения правового регулирования, он относится к органам власти, а не к бизнесу. Однако там содержатся требования, которые написаны экспертами, уже много лет существуют и апробированы. И я считаю хорошим подходом со стороны бизнеса брать эти требования за эталон. Естественно, с учетом профиля конкретной компании. Методичная реализация мер защиты из 21-го приказа ФСТЭК однозначно может минимизировать риски реальной утечки.

Понятно, всегда рвётся там, где тонко. И если у вас какая-то мера защиты не реализована, скорее всего, там и пройдет атака. Поэтому нужны комплексный подход, лучшие практики, в том числе следование рекомендациям регулятора.

— **Какие цифровые продукты и решения, способные минимизировать возможный ущерб для оператора ПДн, может предложить клиентам компания UserGate как опытный игрок на**

В итоге ситуация тоже должна измениться. Эти оборотные штрафы не самоцель: они должны запустить процесс, когда компании начнут вкладываться в ИБ, она начнет работать, и утечек, по факту, станет меньше

рынке информационной безопасности?

— Мы, как и, наверное, все российские вендоры, периодически проводим трассировку требований регулятора на функциональность наших средств защиты. Таким образом, у нас всегда есть четкое понимание, какие меры защиты информационных систем персональных данных реализует наш продукт.

Мы занимаемся разработкой и внедрением решений класса NGFW более 15 лет. По большому счету, мы пионер в создании российских NGFW. Это сложный продукт с обширной функциональностью, который реализует большое количество мер защиты из нормативных требований регулятора. И если необходимо начинать построение системы безопасности с нуля, в том числе для защиты персональных данных, считаю эффективным начать строить безопасность с таких метапродуктов.

Когда мы ставим на периметре сети межсетевой экран следующего поколения, то одним этим продуктом закрываем несколько десятков мер защиты из приказа ФСТЭК. Безусловно, это не панацея, потому что есть другие домены безопасности, кроме сетевого. Но межсетевой экран хорош тем, что он находится на границе сети, отделяя её от внешнего агрессивного мира.

— **Какие еще меры необходимы, чтобы произошел психологический перелом в обществе и случаи утечек с использованием личной информации в преступных целях стало чем-то из ряда вон выходящим?**

— В целом, решений было принято достаточно. Стоит дать вре-

мя для их реализации. При этом я бы уже выделил два позитивных аспекта. Во-первых, сейчас кибербезопасность становится доступнее. Возможно, через какое-то время это даст качественное изменение ландшафта. Ведь когда-то эти услуги и решения были очень дорогими и доступными только для крупных корпораций. Сейчас появляются целые линейки решений, рассчитанные на клиентов в диапазоне от малого бизнеса до крупной компании.

Очень многое переходит сейчас в сервисную модель — Managed Security Service Provider, информационную безопасность по подписке. Безопасность становится доступней, как с точки зрения продуктов, которые можно себе позволить, так и возможностей аутсорсинга.

И второй важный аспект — это осознанность. Все-таки со временем появляется больше информации, тема ИБ проникает в различные сферы науки, техники, «народного хозяйства». Люди в это погружаются, начинают больше думать об информационной безопасности, как личной, так и корпоративной.

Так что рано или поздно количество должно перейти в качество. И наступит момент, когда уже не останется людей, не подготовленных к банальным мошенническим схемам. Доступность конкретных решений и услуг, а также информации о защите информации в целом трансформируют сферу кибербезопасности: она перестаёт быть чем-то кулуарным, а становится просто частью нашей жизни.

Вопросы задавал
Усам Оздемиров

WILDBERRIES И RUSS: «ПЕРСОНАЛЬНЫЕ ДАННЫЕ — НЕ ТОВАР»



Кирилл
ЗЮБАНОВ
CDPO
Wildberries
и Russ

В 2024 году Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» (152-ФЗ) исполнилось 18 лет, и на совершеннолетие он обзавелся невиданными прежде инструментами — оборотными штрафами за «утечки» персональных данных и уголовной ответственностью за неправомерную обработку незаконно полученных данных. Это, конечно, не могло пройти незамеченным. О персональных данных говорят еще больше, чем прежде, компании ищут экспертов в сфере приватности или специалистов по организации обработки персональных данных.

В Wildberries и Russ сформирована полноценная функция Data Protection Officer (DPO), ответственная за организацию обработки персональных данных.

КЛЮЧЕВОЕ ТРЕБОВАНИЕ — БЫТЬ В КОНТЕКСТЕ

Мы исходим из того, что в основе всего лежит контекст обработки персональных данных — те обстоятельства, в которых данные были собраны, получены или даже созданы, цель их дальнейшей обработки, ожидания, которые есть у субъекта (например, у покупателя). Если данные оказываются «вырванными из контекста»

(например, каким-то образом попадают в руки злоумышленника, который точно использует их не в тех целях, в которых покупатель предоставил их компании), это является неправомерной обработкой, нарушением закона.

Вырвать данные из контекста может и работник компании, который недостаточно внимательно следит за соблюдением правил обработки данных. Например, взять данные, предоставленные работником при трудоустройстве, и направить с их помощью рекламную рассылку — тоже нарушение, потому что без согласия субъекта меняется цель обработки данных.

Для того, чтобы обеспечивать высокий уровень защиты прав субъектов персональных данных и учитывать интересы всех прямых и косвенных участников обработки данных (субъектов, бизнеса, уполномоченных органов), рекомендуется принимать следующие меры.

ИНТЕГРАЦИЯ

Команда DPO должна быть не просто контролирующей функцией, не страшным «надсмотрщиком», а партнером, доверенным советником, помогающим, как мы говорим, сделать красивое еще и законным, а законное — еще и красивым. Уровень доверия к DPO можно сравнить с уровнем доверия доктору: обоим честно рассказывают, что произошло, спрашивают, насколько это критично, можно ли поправить и как в следующий раз сделать хорошо.

Для этого мы постоянно организуем выступления для всей компании, где рассказываем о развитии законодательства, о базовых понятиях (например, о том, что относится к персональным данным, а что — нет) и правилах работы с данными.

Это позволяет говорить с бизнесом если не на одном языке, то хотя бы на близких диалектах одного языка.

Также большие выступления помогают найти ключевых контрагентов на самых разных уровнях — от исполнителей до топ-менеджмента, и каждый из них каждый день повышает степень покрытия требованиями DPO процессов, проектов и продуктов.

КОНТРОЛЬ

Мы выстраиваем отличные отношения с бизнес-командами, но человеку, как известно, свойственно ошибаться и, следовательно, терять контекст. Тема персональных данных — далеко не самая простая для понимания и использования в работе. Для того, чтобы снизить риск ошибки, мы используем систему двухуровневого контроля.

Первый уровень — операционный контроль, потоковое согласование инициатив, выявление рисков и рекомендации по их устранению. Через этот фильтр, через это «сито» проходят все новые инициативы.

Второй уровень — выражение того, что мы называли shift everywhere privacy (по аналогии с концепцией shift left security, предполагающей проведение технического анализа на как можно более ранней стадии реализации идеи). Наша концепция — про проактивное взаимодействие с уже существующими процессами, проектами и продуктами через разного рода аудиты.

Итого, операционный контроль и аудиты как проекты, охватывающие разные предметные области, — весьма эффективный способ увеличения покрытия функции DPO.

Необходимо отметить, что успех работы функции DPO напрямую за-

висит от того, имеют ли владельцы процессов, проектов и продуктов ответственность за соблюдение требований DPO и понимают ли они эту ответственность. Мы считаем, что коллеги, фактически осуществляющие обработку данных, как и принимающие решения о том, что она будет осуществляться, — одни из самых главных адресатов требований DPO.

ИНФОРМИРОВАНИЕ

Ты можешь быть самым защищенным оператором, но какая разница, если твой субъект плачет? Мы уделяем особое внимание тому, чтобы обработка, которую мы осуществляем, была не только законной, но еще и понятной.

Для внешних пользователей мы подготовили и запустили лендинг (страницу, на которую пользователи попадают («приземляются»), нажав на ссылку — прим. ред.) о бережливом отношении к персональным данным,

призванный рассказать пользователям о том, какие данные могут обрабатываться, для чего и почему об этом надо знать и заботиться (privacy.wildberries.ru). Он доступен всем без ограничения, и любой посетитель сразу видит наше основное кредо: «Персональные данные — не товар».

Кроме того, мы в Wildberries и Russ разработали концепцию киберсознанности — культуры, в которой каждый осознаёт свою ответственность и принимает необходимые действия для защиты данных и денег онлайн. Мы занимаемся системной просветительской работой по теме информационной безопасности среди сотрудников, покупателей, партнёров и продавцов. В частности, недавно был запущен пополняющийся ресурс «Гид по безопасности» (security.wildberries.ru), где собраны основные мошеннические схемы и способы противодействия.

Также мы следуем принципу «интерфейсной прозрачности», кото-

рый подразумевает, что несмотря на то, что вся необходимая по закону информация уже содержится в правовых документах, любой интерфейс должен быть понятен пользователю в том числе без всяких документов. Например, если есть форма сбора данных, из нее должно быть понятно, для чего собираются данные.

Для профессионалов на рынке мы также стараемся быть полезными, делиться опытом и интересными кейсами. Например, недавно мы провели первое в истории компании мероприятие для экспертов в сфере приватности — Wildberries Privacy Day.

Мы продолжим развивать компетенции команды DPO, всегда готовы взаимодействовать с коллегами по профессии, делиться опытом и вместе делать обработку данных, за которую мы отвечаем, законной, безопасной и прозрачной для субъекта, бизнеса и уполномоченных органов.



АССОЦИАЦИЯ
БАНКОВ
РОССИИ

XXV Всероссийская банковская конференция «Банковская система и национальная экономика: новая архитектура взаимодействия для достижения целей 2030»

16 апреля 2025 года

Москва + онлайн

В конференции традиционно принимают участие представители Банка России, Минфина, Минэкономразвития, Госдумы, институтов развития, ведущие кредитные организации и эксперты отрасли. Организатор - Ассоциация банков России.

Программа включает четыре сессии, которые посвящены роли банков и институтов развития в достижении национальных целей 2030, мерам поддержки региональной экономики, перспективам развития банковской и платежной отраслей.

Контакты: +7 (495) 785-29-93, +7 (495) 785-29-88
event@asros.ru, <https://asros.ru>

Подробная
информация



К НЕЗАВИСИМОСТИ БЕЗ ИЗОЛЯЦИИ

НА ВОПРОСЫ BIS JOURNAL ОТВЕЧАЕТ

ПРЕДСЕДАТЕЛЬ НАУЧНОГО СОВЕТА РАН

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ИГОРЬ ШЕРЕМЕТ

Игорь ШЕРЕМЕТ

председатель Научного совета РАН
«Информационная безопасность», доктор
технических наук, профессор, академик РАН

— **Игорь Анатольевич, как формировался состав Научного совета РАН «Информационная безопасность»?**

— Любой научный совет в составе Российской академии наук — это научно-консультативный, координационный, совещательный и экспертный орган. Совет не является юридическим лицом, не имеет бюджета, но представляет собой эффективный инструмент осуществления Академией ее функций по генерации новых знаний и экспертизе предлагаемых научных и технических решений. Наш совет был создан постановлением Президиума РАН № 12 от 16.01.2024 г. по инициативе президента РАН Г. Я. Красникова, который и предложил мою кандидатуру на роль председателя Совета. В этом качестве я представил проект положения о Научном совете «Информационная безопасность» и проект его состава. Они были утверждены еще одним постановлением РАН от 26.03.2024 г. Полный состав Совета — 72 человека — был утвержден решением Президиума РАН от 01.10.2024 г. И 15.10.2024 г. на площадке МИФИ состоялось первое заседание Совета.

— **Кто эти 72 человека, которые входят в состав Совета?**

— Они представляют четыре основных сегмента сферы, за которую отвечает Совет:

- ♦ обе палаты Федерального Собрания РФ (Совет Федерации и Государственная Дума);
- ♦ силовой блок исполнительной власти (Следственный комитет, ФСБ, МВД, ФСТЭК, Роскомнадзор, Росфинмониторинг, Федеральная налоговая служба, Федеральная таможенная служба, Росгвардия, Минобороны);
- ♦ финансово-экономический блок исполнительной власти (Минцифры, Минэконом-

развития, Минэнерго, Минтранс, Минобрнауки, Минздрав и ФМБА) и крупнейшие субъекты экономики РФ — Банк России, Сбербанк, ВТБ, «Ростех», «Ростелеком», «Роснефть», «Транснефть», «Газпром»;

♦ крупнейшие российские центры компетенций в области кибербезопасности (Академия криптографии РФ, Национальный технологический центр цифровой криптографии, Национальная ассоциация международной информационной безопасности, Национальная система платежных карт, «Лаборатория Касперского»).

И, конечно, в состав Совета входят представители практически всех отделений РАН. Все члены Совета, — безусловно, специалисты высочайшей квалификации.

Следует отметить, что тематикой информационной безопасности как таковой сфера деятельности Совета не ограничивается, она шире. В частности, потому что правоохранные ведомства России пришли к пониманию необходимости создания специального экспертного совета по вопросам противодействия криминалу, все активнее использующему киберпространство для совершения преступлений. Учитывая, что методологический, технологический и математический инструментарий, используемый правоохранителями и специалистами по кибербезопасности, практически один и тот же, было решено еще один совет не создавать, а возложить соответствующие функции на наш Совет.

Сегодня мы выделяем пять основных направлений работы Совета:

- ♦ кибербезопасность;
- ♦ информационно-психологическая безопасность;
- ♦ правовое обеспечение информационной безопасности;
- ♦ противодействие криминалу, использующему киберпространство для совершения преступлений;
- ♦ подготовка кадров в сфере информационной безопасности.

ВСЕ ГРАНИ

— Одно только направление кибербезопасности — это целая вселенная. Каким образом Совет подходит к рассмотрению научных исследований в этой сфере?

— Безусловно, любое системное изучение какой-либо области следует начинать с создания ее онтологии, то есть построения базовой системы признаков, позволяющих разумно декомпозировать эту область до уровней, с которых можно формулировать понятные и решаемые научно-технические задачи. В данном случае такими упорядочивающими признаками являются источники угроз, основные объекты их активности, а также преследуемые ими цели. Мы видим четыре основных источника угроз:

- ♦ деятельность государственных структур недружественных стран, в первую очередь их спецслужб;

- ♦ киберпреступники и их сообщества, в просторечии — хакеры;

- ♦ террористические организации различного толка, которые в последнее время весьма активно используют киберпространство;

- ♦ конкурирующие субъекты политики и экономики. Это могут быть политические партии или группировки, а также коммерческие компании, которые пытаются захватывать рынки с помощью не вполне законных методов. Опыт развитых стран однозначно свидетельствует о наличии криминально-информационных технологий, предназначенных для нанесения ущерба бизнесу конкурента. Что касается компрометирующих фейковых сюжетов о политических деятелях, то с появлением нейросетевых имитаторов подобные видеоматериалы стали делом обыденным. В англомире даже появился термин, достаточно точно характеризующий время, в котором мы живем, — Post-Truth Era.

Каждый из упомянутых источников угроз характеризуется, прежде всего, собственными целями и своими доступными ему интеллектуальными, финансовыми, технологическими и информационными ресурсами. Так, у госструктур развитых недружественных стран все эти ресурсы имеются в максимальном объеме. У хакеров они, конечно, поменьше, но у них и цели не столь масштабные. У террористов и политико-экономических конкурентов ресурсы также могут быть относительно небольшими, однако при наличии обширного рынка предложений со стороны киберкриминала, обладающего иногда просто эзотерическими знаниями в области Cyberspace и Cybersecurity, этих ресурсов мо-



жет быть достаточно для оплаты криминальных киберуслуг.

— Как выглядят цели нападений в киберпространстве для разных типов акторов?

— Если мы говорим о спецслужбах недружественных стран, то основные цели их активности в киберпространстве — это критические инфраструктуры России и система государственного и военного управления, которая на них базируется. В первую очередь, мы имеем в виду четыре опорных инфраструктуры: топливно-энергетическую, транспортную, производственную и инфор-

мационную, которая, собственно, обеспечивает их согласованное функционирование, а также работу любых других функциональных инфраструктур, пользующихся услугами энергетики, связи, транспорта и промышленного производства. Понятно, что недружественные страны испытывают интерес к нашим критическим инфраструктурам, чтобы, во-первых, иметь возможности по снижению экономического и военного потенциала Российской Федерации в любой конфликтной ситуации, а, во-вторых, чтобы иметь устойчивый доступ к информации ограниченного распространения, циркулирующей в различных сегментах российской информационной инфраструктуры.

ЗАЩИТИТЬСЯ НЕЛЬЗЯ ИЗОЛИРОВАТЬСЯ

— **Какие подходы положены в основу мероприятий защиты в этой ситуации?**

— Что касается подходов к реализации кибербезопасности, то у нас (и не только у нас, а в любой другой стране — например, в США) с давних пор действует ключевой принцип: наиболее важные объекты и системы управления физически изолируются от глобальной инфосферы, от сети Интернет. И это очень правильный принцип. За три года специальной военной операции мы видели и продолжаем наблюдать, к большому сожалению, атаки беспилотников на объекты критических инфраструктур. Но при этом мы ни разу не слышали, что через киберпространство была осуществлена какая-то серьезная кибератака, оставившая, скажем, без электроэнергии, промышленное предприятие или целый город. Поэтому, с одной стороны, изоляция от глобальной сети остается самым эффективным способом защиты от кибератак (разумеется, этот простейший способ не универсален, ибо существует огромное количество сервисов, принципиально открытых для доступа из Интернета).

С другой стороны, на настоящий момент остаются некоторые источники угроз. Российская информационная инфраструктура по известным причинам перенасыщена программными и аппаратными средствами зарубежного производства, каждое из которых («надейся на лучшее — готовься к худшему») может быть потенциальным носителем встроенных диверсионных дефектов («операционных мин»). Однако благодаря своевременно принятым мерам, развивается целая экосистема обеспечения кибербезопасности. В частности, создана система ГосСОПКА, обеспечивающая, прежде всего, безопасное функционирование госсектора, государствен-

ных систем управления. Под эгидой ФСБ и ФСТЭК разработана хорошая нормативная база, создана система испытательных лабораторий и аттестационных центров. Они обеспечивают достаточно серьезный «входной контроль» того программного обеспечения, которое поступает на эксплуатацию на различные объекты и в госорганизации. Однако проконтролировать весь поток обновлений, патчей и т.п. применительно к функционирующим программным средствам крайне сложно. Поэтому, конечно, некоторые «шероховатости» в этой части время от времени проявляются, но они не перерастают в серьезные инциденты, уходящие в материальную сферу (так называемые киберкинетические воздействия).

На этом же поле действуют террористические организации. Для них киберпространство — это средство получения противоправного доступа к финансовым ресурсам, нелегального сбора информации о возможных объектах их террористической деятельности (организациях и людях), а также средство реализации собственно террористических действий в материальном мире. Например, деструктивное воздействие через киберпространство на какое-нибудь химическое производство может нарушить технологический цикл и привести к тяжелым экологическим последствиям.

Надо сказать, что в этой части наша правоохранительная система абсолютно в курсе всех возможных способов деструктивной деятельности террористов. Мы неоднократно проводили совещания с нашими силовиками на эту тему. Тем не менее, нашли некоторые сегменты, которые до настоящего времени не были охвачены в нужной мере соответствующими научными исследованиями. Благодаря нашему Совету мы выходим на уровень превентивного изучения возможных угроз и проведения предварительных исследований, которые позволят сформировать комплексное описание этих угроз, включая детальные «портреты» потенциальных преступников.

ПРО МОШЕННИКОВ

— **А как обстоят дела с кибермошенниками? До сих пор на этой теме Президент России акцентирует свое личное внимание.**

— Киберпреступники и их сообщества — это отдельный источник угроз. У них задача очень простая — хищение денежных средств. Поэтому объект номер один для их атак — Сбербанк, лакомый кусок — 110 млн клиентов, физических лиц и 3,5 млн юридических

лиц. Сеть Сбербанка включает порядка двух миллионов объектов сетевой инфраструктуры: рабочих станций сотрудников, сетевого и серверного оборудования, банкоматов. Центр киберзащиты Сбербанка ежедневно обрабатывает более 500 млрд событий безопасности от локальных средств защиты (межсетевых экранов, систем обнаружения вторжений и т.п.), фиксируется порядка 20 тыс. попыток кибермошенничества — тех самых звонков от «следователей», «начальников службы безопасности Сбербанка» и проч. И ежедневно этот Центр выявляет порядка сотни АРТ-атак — сложных, плохо предсказуемых и потому наиболее опасных. Вот так выглядят масштабы сражений, которые в настоящее время происходят в киберпространстве.

— **Как Вы оцениваете текущие результаты этих сражений?**

— По моим оценкам, Центр кибербезопасности Сбербанка — это ведущий центр компетенций в данной сфере. Он работает в самых жестких условиях: если то или иное силовое ведомство может при необходимости физически отключить свои системы от Интернета, что позволит сосредоточить внимание на оставшихся угрозах типа злонамеренных инсайдеров, то Сбербанк — это по определению открытая система, которая принципиально не может быть закрыта. И в этих условиях, согласно актуальной статистике, 99,8 % попыток кибермошенничества в настоящее время выявляется и блокируется. Хотя с точки зрения правоохранительных ведомств, раскрываемость киберпреступлений в целом не очень высока — всего лишь около 23 %. Мы видим в качестве одной из основных задач Совета содействие правоохранителям с тем, чтобы эта цифра существенно выросла.

ПРЕВЕНТИВНОЕ ПРОТИВОДЕЙСТВИЕ

— **В каждом ведомстве и крупной компании всегда были и есть собственные планы работ и исследований в области кибербезопасности. Какие новые возможности дает им ваш Совет?**

— Впервые появилась возможность организовать не только междисциплинарные (это было всегда), но и межведомственные исследования и разработки, для которых наш Совет выполняет координационные функции. Дело в том, что, действительно, по некоторым вопросам ведомственные исследования дублируют друг друга, но есть и пустые места, которыми никто не занимается в силу определенной инерции. И сейчас с появле-

нием площадки нашего Совета появилась возможность эту инерцию преодолеть.

Кроме того, четыре основных источника угроз, которые мы перечислили раньше, в реальной жизни не существуют изолированно друг от друга. Так, спецслужбы во всех странах с большим удовольствием используют киберпреступников в качестве, так сказать, рабочей силы. Смычка террористов с киберпреступниками тоже, очевидно, имеется, и она очень опасна. На этой почве вырастает весьма опасный компьютерный андеграунд, борьба с которым — достаточно сложное дело. Поэтому мы поставили перед собой задачу — и уже начинаем ее решать — разработка моделей поведения различного рода преступных сообществ. Тогда, опираясь на информацию о ведущихся ими действиях, разработках, которые они ведут в данное время (это так или иначе всегда проявляется заранее), можно выстраивать эффективную систему противодействия. Других способов нет. Надо очень хорошо понимать, чего ожидать в будущем, какие реальные угрозы могут формироваться в реальном мире.

ЧОП В КИБЕРПРОСТРАНСТВЕ

— **Какие направления таких превентивных исследований Совет ведет уже сегодня?**

— Сегодня мы выделили шесть таких направлений. Первое — это создание экосистем безопасности на основе интегрированных SIEM-систем (Security Information and Event Management), на основе которых функционируют оперативные центры кибербезопасности (Security Operation Center, SOC). Напомню о хорошем опыте Сбербанка, где с 2015 г. функционирует SOC, один из крупнейших в Европе. Именно благодаря работе этого Центра стали возможны упомянутые мною результаты в части противодействия киберпреступности.

В целом, надо сказать, в настоящее время фактически идет осмысление и формирование концепции SIEM-as-a-Service. Мы уже знаем много примеров применения концепции «As-a-Service»: Software-as-a-Service, Infrastructure-as-a-Service, Mobility-as-a-Service и даже Government-as-a-Service. Так вот, SIEM-as-a-Service в киберпространстве — это, по сути, переход к новым системнообразующим принципам защиты. По аналогии с функциями охраны в материальном пространстве, где могут работать либо собственные сотрудники охраны, либо внешний ЧОП, либо организация находится под охраной Росгвардии, для защиты в кибер-

пространстве любая организация или создаст собственное подразделение CyberSecutity или пользуется услугами аутсорсинга в этой сфере. Схема SIEM-as-a-Service, на мой взгляд, станет одной из доминирующих тенденций ближайшего будущего: услуги защиты будут оказывать весьма серьезные и развитые специализированные Центры компетенций. Естественно, они будут иметь лицензии правоохранительных органов (ФСБ, ФСТЭК, МВД) и закрывать по периметру все те области, на которые укажет организация, фактически реализуя ее политику кибербезопасности.

Понятно, что для госструктур есть ГосСОПКА — аналог Росгвардии, только в киберпространстве, а для бизнеса наиболее разумным подходом станет «ЧОП SIEM-as-a-Service». Это очень наукоемкое и высокотехнологичное направление, потому что мало создать систему, которая обеспечит сбор информации от локальных средств защиты. Нужно вести комплексную обработку этого потока, а это, напомним, могут быть миллиарды сообщений в сутки. Значит, здесь не обойтись без искусственного интеллекта (ИИ), точнее, целого спектра технологий, которые обеспечат необходимую комплексную обработку потоков данных о событиях ИБ в жестком реальном времени. Я подчеркну: речь идет не об отложенном режиме обработки — год копили большие данные, потом год их анализируем, а о том, что все события обрабатываются практически в темпе их поступления. И это очень серьезный научно-технологический вызов и важнейшее направление исследований нашего научного Совета, можно сказать, системообразующее.

Здесь мы уделяем серьезное внимание распространению передового опыта Сбербанка в части эксплуатации и развития их SOC-центра и видим большое поле для работы Совета именно как координирующего, консультативного органа, который способствует распространению передовых знаний и технологий на всю страну. Сейчас мы работаем, по сути, по отраслевому принципу, но думаем подключать к этим процессам регионы и выйти через некоторое время на модель киберзащиты региона.

БАЗА ЗНАНИЙ: УМНАЯ, НО ОПАСНАЯ

— **Раз развитие концепции SIEM-as-a-Service требует применения методов ИИ, значит, методы искусственного интеллекта — тоже предмет научных исследований Совета?**

— Да, это еще одно важное направление нашей деятельности. В массовом сознании сегодня понятие «искусственный интеллект» связывается исключительно с нейросетями. Но на самом деле это только одна из широкого спектра современных технологий ИИ. Например, в программе предстоящей в ноябре этого года всемирной конференции по искусственному интеллекту в Осаке, на которую я приглашен, заявлено 17 направлений исследований в области ИИ. Конечно, и нейросетевые системы тоже нуждаются в защите — надо защищать их входы и выходы.

Сегодня считается, что основная угроза — это атаки на обучающие выборки (training datasets): если сеть будет обучена неправильно в результате целенаправленного внешнего воздействия, она будет выдавать неправильные результаты. Правда, с точки зрения кибербезопасности, training datasets ничем не отличаются от любых других datasets. И таким же способом их надлежит защищать. Я не вижу здесь особой новизны. А вот что касается искусственного интеллекта других направлений, в частности, конклюдентного искусственного интеллекта (от слова conclusion — заключение), где есть база знаний и система логического вывода, которая получает на входе некие сообщения и, используя базу знаний, генерирует те или иные осмысленные выводы, цепочки рассуждений и т.д., тут открывается обширное поле для научно-технических разработок.

— В чем здесь новизна с точки зрения технологий защиты?

— Здесь я вижу две проблемы. Одна из них — защита базы знаний, ее входов и выходов, системы логического вывода. Вторая обусловлена тем, что системы конклюдентного ИИ представляют собой объекты относительно нового вида.

Проблема в том, что система логического вывода может и не содержать никаких ошибок, ведь она, как правило, весьма простая и понятная, иначе было бы сложно создавать и обновлять базы знаний. А вот что касается самой базы знаний, то ее структура, технологии ее использования и обновления напрямую зависят от модели представления знаний. Для каждой из них должен быть разработан особый способ или технологии или комплекс средств обнаружения в ней дефектов. Дело это не то чтобы совсем новое, системы конклюдентного ИИ существуют несколько десятков лет. Но по сравнению с тем опытом, который накоплен в части проверки кода традиционного ПО, мы находимся в самом начале пути.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ — КОД, ДА НЕ ТОТ

— Разве нельзя использовать весь тот практический опыт автоматизированной проверки в виде разнообразных технологий статического, динамического анализа кода, фаззинга и т.д.?

— Коль скоро мы заговорили о верификации программных средств, то здесь мы сталкиваемся с серьезными теоретическими ограничениями, связанными с неразрешимостью такого рода задач. Есть известная проблема останова машин Тьюринга, которая алгоритмически неразрешима: не существует машины Тьюринга, которая, получив на вход другую машину Тьюринга с ее входной лентой, в общем случае определила бы, закончит ли упомянутая другая машина свою работу или будет работать вечно. В переводе с языка математической логики это означает: невозможно придумать программу, которая, получив на входе любую другую программу, сказала бы, что в ней нет ошибок. Почему так? Потому что в этом случае она, получив на вход саму себя, должна подтвердить, что в ней ошибок нет.

Эта проблема — один из примеров логических парадоксов, которыми занимается логика как наука. Другой известный пример того же рода — парадокс брадобрея: брадобрей бреет всех, кто не бреет себя сам. Если предположить, что он бреет себя сам, значит, он не бреет себя сам. Если предположить, что он не бреет себя сам, значит, он бреет себя сам.

— Как же можно справиться с теоретической неразрешимостью задачи проверки любого кода в общем виде?

— Народная программистская мудрость гласит: каждая последняя ошибка, найденная в программе, на самом деле является предпоследней. С точки зрения кибербезопасности каждая такая невыявленная разработчиками и отладчиками ПО ошибка, или эксплойт, является источником уязвимости ПО, которая может быть использована для подготовки и осуществления кибератаки. Надо сказать, что конкретно в России сейчас в этой части сложилась весьма серьезная ситуация. Что я имею в виду?

Возьмите корпорацию Microsoft в ее лучшие годы: всю основную продукцию, которая продавалась и приносила огромные прибыли вендору, производили 1800 программистов и 1800 специалистов по отладке ПО. Обратите внимание: на одного программиста приходился один отладчик. И то до сих пор в продуктах Microsoft можно при определенных

условиях обнаружить баги. Я сам, пользуясь Word (казалось бы, что может быть более отлаженным — весь мир им пользуется десятки лет), чуть ли не ежедневно на них попадаю.

А как выглядит сегодня российская программная индустрия? Ее ландшафт составляют, в основном, малые и средние предприятия. Даже среди крупнейших российских программнопроизводящих компаний нет софтверхаусов, близких по масштабам к Microsoft, Oracle, Siemens или SAP. У нас сейчас хватает рабочих рук только для того, чтобы разрабатывать и производить первичную отладку ПО. А в современных российских условиях софтверным компаниям, которые, как правило, кредитозависимы и живут, что называется, от кредита до кредита, невозможно добиться такой прибыли, которая позволила бы выдержать это кредитное давление. И они вынуждены сокращать численность разработчиков... А что в итоге? Решая задачу обретения импортной зависимости, мы, стремясь к уменьшению количества потенциальных диверсионных дефектов, источником которых может быть импортное ПО, одновременно рискуем увеличивать число непреднамеренных дефектов за счет не очень глубокой отладки этого программного обеспечения и практически отсутствующей инфраструктуры сопровождения всего жизненного цикла ПО. Вот это нас очень беспокоит.

СТИЛЬ «КИБЕР» — ЭТО ПРО МОДУ ИЛИ НАВСЕГДА?

— Проблематика ИИ ведет нас, в том числе, в мир робототехники. Там, похоже, тоже скрываются фундаментальные проблемы кибербезопасности?

— Да, все так. Отдельное направление исследований нашего Совета — новые киберсреды: беспилотные системы, киберфизические производства и т.д. — все то, что находится на границе между кибер- и материальным пространством. И отсюда могут исходить очень серьезные угрозы — киберкинетические воздействия. Скажем, беспилотный автомобиль, который едет по дороге, в результате кибератаки меняет направление движения, выезжает на встречную полосу и становится источником аварии, где погибают люди. Или нарушение технологического процесса на химическом производстве в результате кибератаки, приводящее к техногенной и экологической катастрофе. Здесь самое страшное — это так называемые каскадные, или цепные воздействия, когда некоторое первичное воздействие запускает целую лави-

ну вторичных воздействий, те, в свою очередь, — воздействия третьего уровня и т.д.

Здесь огромное поле для исследований и систематизации мало или совсем не изученных явлений. Хороший опыт эксплуатации накоплен, пожалуй, только в области АСУ ТП. Но, как я сказал ранее, очень много технических решений этого класса завязано сегодня на глобальную информационную инфраструктуру, и велики риски их дефектоносных обновлений со стороны зарубежного производителя.

Есть еще один вариант новой киберсреды — то, что сегодня называется англоязычным термином *ubiquitous computing* и переводится как «вездесущие» или «повсеместные» вычисления. Речь идет о том, что современный человек погружен в киберсреду, состоящую из множества различных вычислительных устройств. Этой концепции стало уделяться особое внимание, в том числе, в связи с появлением майнинга криптовалют и подобных технологий. Скрытый майнинг, то есть использование чужих вычислительных ресурсов для решения задач производства криптовалютных единиц, также требует определенного противодействия.

Еще одно проявление глобализации информационной инфраструктуры — новые среды коллективного доступа, прежде всего, облачные ресурсы. Их популярность объяснима: бизнес уже привык использовать большие данные, но поддерживать и наращивать собственное хранилище данных оказывается слишком накладно. Очень удобно оставить сотрудникам только терминалы, используемые исключительно как точки доступа к ресурсам, размещенным в облаках. Не подвергая сомнению квалификацию и благие намерения владельца этих ресурсов, тем не менее, мы считаем не нулевой вероятностью того, что злоумышленники смогут получить доступ к этому ЦОДу и нанести ущерб большому количеству пользователей облачного хранилища.

— **Если пофантазировать и представить ситуацию, что все облачные хранилища, обслуживающие всех российских клиентов, встроены в Гособлако?**

— Гособлако, действительно, считается абсолютно защищенной конструкцией, которая исключает саму возможность проникновения со стороны кого бы то ни было к его ресурсам. Но надо принять во внимание несколько соображений. Во-первых, необходимое масштабирование технического решения потребует совершенно новых способов организации коммуникационной инфраструкту-

ры такого мега-облака. Представьте только, какова должна быть производительность такого ЦОДа, куда круглосуточно обращается 150 млн физлиц и 3 млн юридических лиц. Тут точно возникает вопрос экономики такого проекта.

Во-вторых, пусть даже мы создали такой экономически выгодный гигантский супер-параллельный суперкомпьютер. Ясное дело, что в условиях вооруженных конфликтов такого рода ЦОДы будут объектом номер один после электростанций. А воздействие на критические инфраструктуры отличается тем, что помимо ущерба в самой нулевой точке, возникают упомянутые каскадные эффекты, генерирующие волны аварий и разрушений.

В-третьих, в мире с начала нынешнего века идут активные научные исследования по вопросам создания максимально надежных катастрофоустойчивых систем. Сегодня считается доказанным, что такую систему можно построить на базе нескольких (на практике трех-четырех) «зеркал» (полных резервных копий основного хранилища), причем, быстроедействие современных каналов связи позволяет синхронизировать эти копии в глобальном масштабе. Но финансовые затраты на реализацию таких проектов представляются весьма значительными.

КВАНТОВЫЙ КОМПЬЮТЕР: УГРОЗЫ И РЕШЕНИЯ

— **Говоря о перспективных исследованиях в области ИБ, нельзя обойти вниманием угрозу квантового компьютера, который способен, по крайней мере, теоретически разрушать все известные ныне криптосистемы.**

— Конечно, одно из важнейших направлений деятельности нашего Совета — исследование того, на базе каких архитектурных, системных и т.д. подходов и технологических решений можно обеспечить защиту от таких компьютеров в случае их реального появления. В течение ряда лет отечественные ученые работают над технологиями и решениями квантовой и постквантовой криптографии. Главным центром компетенций в этой части выступает Академия криптографии РФ. Она работает по своим планам и, насколько я понимаю, успешно их реализует.

Однако для противодействия этой новой потенциальной угрозе крипто- и имитостойкости современных телекоммуникационных систем могут использоваться механизмы, усиливающие системы собственно шифрования. Например, в условиях, когда вдруг оказалось, что не все криптосистемы столь

надежны, как предполагалось ранее, специалисты придумали стеганографию. Напомню, что эта технология позволяет скрывать защищаемые данные в массивах и потоках открытой информации таким образом, что непосвященный пользователь вообще не понимает, что там что-то скрыто. Образно говоря, если традиционная криптография работает в парадигме одного канала передачи данных (и если он оказался скомпрометированным, значит, мы проиграли), то стеганография — в парадигме всего киберпространства, и злоумышленник не знает, где искать то сообщение, в котором в закрытом виде находится интересующая его информация. Упомянутое сообщение — это «контейнер» (например, графический или мультимедийный файл), в который записывается передаваемая криптограмма. Но для того чтобы направить на ее взлом ресурсы квантового компьютера, нужно вначале, по сути, перехватить весь трафик Интернета и попытаться найти тот «контейнер» (а в общем случае их может быть несколько), в котором скрыта криптограмма.

Стеганография — это хорошая иллюстрация того, какого рода методы, способы, технологии могут быть применены для противодействия квантовым компьютерам и новым возможностям по разрушению известных криптосистем.

ОТ РЫНКА ИБ К ОТРАСЛИ ПРОИЗВОДСТВА ПО

— **Расскажите, пожалуйста, о механизме, который должен доводить результаты научных исследований, идущих под эгидой Научного совета РАН «Информационная безопасность», до уровня практического функционирования киберзащищенной, киберустойчивой цифровой экономики России?**

— Акцентирую Ваше внимание на том, что мы не являемся юридическим лицом, научно-исследовательским институтом, который выполняет такого рода задания. Но мы способны сформировать хорошо проработанный паспорт программы РАН, обеспечить постановку задачи и довести этот паспорт до исполнителей, научных организаций. У нас есть поручение Президиума РАН, сформулированное по итогам Общего собрания РАН 10.12.2024 г. Согласно этому поручению, мы должны представить к 01.06.2025 г. дополнение к Программе фундаментальных научных исследований до 2030 г. в части кибербезопасности. До сих пор тема кибербезопасности там практически не была представлена, и

Обязательно придется создавать отечественную софтверную индустрию. Не рынок, а именно настоящую отрасль экономики — промышленность производства программных средств — суверенную, независимую от внешнего мира

мы сейчас работаем над описаниями перспективных теоретических исследований в русле тех шести направлений, о которых я рассказывал.

После того, как это новое направление появится в Программе фундаментальных научных исследований, будем оказывать содействие государственным заказчикам в постановке соответствующих работ, привлекать наиболее серьезные и активные российские центры компетенций к их выполнению, мониторингу результатов работ, участию в приемке и определению направлений дальнейших исследований.

Важно понимать, что эта научная активность развивается на специфическом системном фоне. Выделю его основные особенности: устойчивый рост сложности и результативности кибератак, недостаточность интеллектуального и технологического ресурса для надежного противодействия тому валу киберпреступности, который имеется в настоящее время, и сохраняющаяся импортозависимость многих сегментов нашей инфосферы. При этом будущее страны связано с появлением и развитием новых отраслей экономики, что приведет к появлению новых решений в области информационных технологий. А это означает, что обязательно придется создавать отечественную софтверную индустрию. Не рынок, а именно настоящую отрасль экономики — промышленность производства программных средств — суверенную, независимую от внешнего мира. Независимость здесь понимается не как изоляция, а как возможность использовать все полезное, что есть в других странах, но в случае необходимости функционировать практически автономно. Это означает способность самостоятельно производить все, что необходимо для цифровой поддержки экономики: от трансляторов с языков программирования до прикладных интеллектуальных систем по всем необходимым направлениям.

Вопросы задавала
Елена Покатаева,
обозреватель
BIS Journal

BIS JOURNAL — «ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ»: ДИАЛОГ ДРУЗЕЙ



Алексей МАРКОВ
главный редактор
журнала «Вопросы
кибербезопасности»,
лауреат премии
Правительства РФ
в области науки и техники,
почетный работник науки
и высоких технологий РФ,
доктор технических наук

Расширяя информационное поле темы ИБ, BIS Journal планирует знакомить читателей с родственными изданиями, а в дальнейшем публиковать дайджест из их наиболее интересных материалов. Сегодня предлагаем познакомиться с журналом «Вопросы кибербезопасности», тем более что герой нашего «Интервью номера» Игорь Анатольевич Шеремет является председателем его редакционного совета.

Рецензируемый научно-методический журнал «Вопросы кибербезопасности» (ISSN 2311-3456) был создан в 2013 г. в период обсуждения проекта «Стратегии по кибербезопасности РФ» по инициативе Минюста России, чем было определено название. С этого времени журнал занимает ведущие позиции

в области публикации научных результатов по тематике безопасности информации по специальностям: ВАК РФ 2.3.6 «Методы и системы защиты информации, информационная безопасность» и 1.2.4 «Кибербезопасность». В настоящее время журнал аккредитован по специальностям 1.2.4, 2.2.15, 2.3.1, 2.3.5, 2.3.6.

Журнал имеет наивысший уровень категории журналов ВАК РФ — К1 и входит в российский научный сегмент WoS — RCSI. Журнал также входит в Белый список. Каждый номер имеет международный идентификатор DOI. Журнал выходит 6 раз в год. Всего журнал

выпустил 65 выпусков (около 700 публикаций).

За последние годы на журнал «Вопросы кибербезопасности» подписались библиотеки, вузы и научные организации из 13 стран: Великобритании, Германии, Израиля, Китая, США и др.

За неполные два года (2023 г. — III кв. 2024 г.) со стороны мирового ученого сообщества, не считая России, была оформлена 241 подписка на журнал. Журнал «Вопросы кибербезопасности» наиболее читаем в США — за два неполных года было оформлено целых 117 подписок.

Цель создания журнала состоит в поддержке в первую очередь молодых ученых России. Поэтому он является бесплатным и все статьи находятся в открытом доступе в полнотекстовом виде.

В состав редколлегии журнала входят ведущие ученые страны в области безопасности информации: два академика РАН, член-корреспондент РАН, 14 докторов наук и 4 кандидата наук.

В журнале неоднократно печатались академики и члены РАН (Аветисян А. И., Бородакий Ю. В., Воропай Н. И., Зегжда П. Д., Шеремет И. А. и др.), руководители тематических научных школ (доктора наук Баранов А. П., Костогрызов А. И., Язов Ю. К., Петренко С. А. и др.), публиковали интервью известные российские государственные деятели, например, начальник Главного управления инновационного развития Министерства обороны РФ, начальник Восьмого управления ГШ ВС РФ, бывший Первый заместитель Секретаря Совета Безопасности Российской Федерации, бывший начальник 8 Центра ФСБ России, начальники академий и военных училищ, ректора вузов.

Журнал имеет высокие наукометрические показатели. Среди всех журналов по тематикам РИНЦ: 81.93.29 (Информационная безопасность), 49.33.35 (Надежность сетей связи и защита информации), 50.37.23 (Защита от несанкционированного доступа) журнал занимает первое место в стране по ряду показателей.

Портал журнала: <https://cyberrus.info/>





КОМПЛЕКСНАЯ ЗАЩИТА БИЗНЕСА

от внутренних угроз

DLP

- ✓ Защита от утечек
- ✓ Выявление мошенничества
- ✓ Контроль дисциплины

DCAP

- ✓ Аудит файловых хранилищ
- ✓ Контроль доступа к файлам
- ✓ Защита от пересылки по любым каналам

SIEM

- ✓ Сбор и анализ событий безопасности
- ✓ Обнаружение угроз по связке событий
- ✓ Сканирование сети и поиск уязвимостей
- ✓ Управление инцидентами и реагирование на них

АУТСОРСИНГ ИБ

- ✓ Комплексная защита по подписке
- ✓ Опытный ИБ-аналитик, рекомендации по усилению защиты
- ✓ Еженедельные отчеты и оперативная реакция на инциденты



searchinform.ru

**Сохранность
вашей информации
зависит от вас!**

«РАБОТАЕМ НАД ТЕМ, ЧТОБЫ СДЕЛАТЬ ЭФФЕКТИВНЕЕ БОРЬБУ С КИБЕРПРЕСТУПНИКАМИ И ТЕЛЕФОННЫМИ МОШЕННИКАМИ»



Василий ПИСКАРЁВ
председатель Комитета
Государственной Думы
по безопасности и противодействию
коррупции

18 марта Государственная Дума рассматривала в первом чтении законопроект¹ о противодействии киберпреступлениям, над которым работал и наш комитет. Примечательно, что именно в этот момент с известным телеведущим, а ныне депутатом Госдумы Евгением Ревенко, который находился в зале пленарных заседаний, вышли на связь мошенники. В популярном мессенджере они обратились к нему от имени Заместителя Председателя Госдумы Петра Толстого. Коллега Ревенко, в итоге распознав фейковый аккаунт, прекратил общение.

Признаюсь, я и сам сталкивался с ситуациями, когда с фейковых аккаунтов с моей фотографией на аватарке пытались обмануть моих коллег и знакомых. Приходилось всем напоминать, что я не делаю в соцсетях никаких рассылок и тем более не обращаюсь с материальными просьбами.

Но далеко не всем удастся вовремя понять, что их собеседник совсем не тот, за кого себя выдает. Доля киберпреступлений в общем массиве совершаемых преступных деяний достигла почти 40 процентов. Несмотря на принимаемые меры, ущерб от деятельности злоумышленников в этой сфере достигает порядка 200 млрд рублей ежегодно. По данным МВД России, только в прошлом году зафиксировано 486 тысяч случаев онлайн-мошенничества, и пятую часть среди них составляют кражи с банковского счета. При этом не единичны случаи, когда жертв обмана склоняют к совершению диверсий и терактов (а это поджоги банкоматов, вышек связи, рейльных шкафов, а также военкоматов и избирательных участков).

¹ <https://sozd.duma.gov.ru/bill/842276-8> Проект федерального закона № 842276-8 «О создании государственных информационных систем по противодействию правонарушениям (преступлениям), совершаемым с использованием информационно-телекоммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации».

Несколько слов о законопроекте, который должен сузить возможности мошенников, придумывающих все новые способы, как технические, так и манипулятивные, для выманивания денег у россиян.

Создаются две государственные информационные системы, оператором которых будет Минцифры России. Госорганы, банки и цифровые платформы в режиме онлайн смогут обмениваться информацией для выявления подозрительных действий и их блокировки, что способствует оперативному реагированию на них правоохранительных органов.

При этом образцы голосов мошенников и абонентские номера, с которых они совершают противоправные действия, будут аккумулированы в специальную базу данных. Это создаст дополнительные возможности для поиска преступников.

Сотрудники кредитных организаций, Банка России и операторов связи больше не смогут обращаться к клиентам с использованием зарубежных мессенджеров. Не секрет, что очень часто именно мессенджеры используют злоумышленники для введения в заблуждение наших граждан.

Другие важные нововведения, которые предусматривает законопроект.

Во-первых, будет запрещено передавать sim-карты третьим лицам, при этом абонент сможет установить самозапрет на оформление нового договора без личного присутствия в офисе оператора и отказаться от получения рекламы в форме массового обзвона.

Во-вторых, оформить удаленно кредит в микрофинансовой организации можно будет только в случае использования единой системы идентификации и аутентификации и проверки биометрии. Чужой паспорт с переклеенной фотографией или бледная его ксерокопия уже не помогут.

Законопроект предусматривает и еще целый ряд требований и ограничений, которые расставляют красные флажки, зайти за которые злоумышленникам станет труднее.

Расскажу и еще об одной законодательной инициативе², в разработке которой я принимал непосредственное участие. Законопроект предусматривает возможность проводить предварительное расследование преступлений в том месте, где находится большинство потерпевших. Хищения имущества, совершаемые дистанционно, а

² <https://sozd.duma.gov.ru/bill/792475-8> Проект федерального закона № 792475-8 «О внесении изменений в статью 152 Уголовно-процессуального кодекса Российской Федерации».



Рабочее совещание в Комитете ГД по безопасности и противодействию коррупции о законодательном противодействии телефонному мошенничеству и мошенничеству с использованием информационно-телекоммуникационной сети «Интернет»

речь как раз идет преимущественно о кибермошенничестве, как правило, связаны с большим числом потерпевших. Количество эпизодов при этом может исчисляться десятками, а то и сотнями. В то же время потерпевшие могут находиться как в одном, так и в нескольких регионах, а злоумышленники — в тех же либо в других регионах или даже за пределами Российской Федерации. Полагаю, что реализация этого законопроекта позволит вести расследования более оперативно и будет способствовать всесторонней защите и обеспечению прав потерпевших, а также возмещению ущерба.

Вместе с уже принятым недавно законом, которым введен так называемый «период охлаждения» при получении кредитов, предложенные поправки помогут оздоровить ситуацию.

Председателем Государственной Думы В. В. Володиным в том числе и Комитету по безопасности и

противодействию коррупции поручено совместно с профильными министерствами и ведомствами проработать дополнительные меры по совершенствованию законодательства в сфере противодействия телефонному мошенничеству и мошенничеству с использованием информационно-коммуникационной сети Интернет.

Учитывая специфику нашего комитета, рассматриваем возможность внесения дополнительных поправок в Уголовный и Уголовно-процессуальный кодексы РФ, а также в Кодекс РФ об административных правонарушениях.

Очень важно, как бы изобретательны ни были киберпреступники, максимально сузить для них возможности для обмана наших граждан, и создать условия для того, чтобы наказание для них было действительно неотвратимым.

КВАРТАЛЬНЫЙ ОТЧЕТ

О НОРМАТИВНОМ РЕГУЛИРОВАНИИ В СФЕРЕ ИБ В I КВАРТАЛЕ 2025 ГОДА



**Екатерина
РАЧКОВА**
обозреватель
BIS Journal

ПЕРСОНАЛЬНЫЕ ДАННЫЕ (ПДН)

I квартал 2025 года продолжил обогащение правового поля новациями в области персональных данных (подробный разбор, а также дискуссионные аспекты законодательства об оборотных штрафах для операторов за нарушение порядка обработки персональных данных — в статье Н. Перемышленникова на стр. 25, наглядная инфографика и смягчающие обстоятельства по данному вопросу — в статье И. Башкирова на стр. 4 — прим. ред.).

24.01.2025 было опубликовано и вступило в силу постановление Правительства Российской Федерации от 18.01.2025 № 15 «О внесении изменений в постановление Правительства Российской Федерации от 15.06.2022 № 1067 «О случаях и сроках использования биометрических персональных данных, размещенных физическими лицами в единой биометрической системе с использованием мобильного приложения единой биометрической системы». Были внесены изменения в правила использования биометрических персональных данных (ПДн), размещенных гражданами в единой биометрической системе с использованием мобильного приложения. В числе прочего, при наличии сведений в ЕСИА биометрические ПДн можно будет использовать для дополнительной аутентификации на портале Госуслуг без подтверждения личности с помощью биометрического загранпаспорта.

14.02.2025 Правительство Российской Федерации опубликовало проект постановления «Об утверждении правил проверки соответствия пользователей государственной информационной системы, определенной в соответствии с частью 2 статьи 131 Федерального закона «О персональных данных», требованиям, указанным в части 7 статьи 131 Федерального закона «О персональных данных», и о внесении изменений в некоторые акты Правительства Российской Федерации». Данный проект определяет процедуру проверки соответствия пользователей государственных информационных систем (ГИС) обезличенных данных — граждан и юридических лиц — требованиям к пользователям системы, а также устанавливает 13-дневный срок рассмотрения запросов пользо-

вателей системы о проведении проверки соответствия, в том числе посредством запроса информации у различных федеральных органов исполнительной власти.

Также 14.02.2025 Правительством Российской Федерации был опубликован проект постановления «О государственной информационной системе, предназначенной для обработки персональных данных, полученных в результате обезличивания персональных данных, и внесении изменений в постановление Правительства Российской Федерации от 14 мая 2021 № 733». Проект уточняет цели и задачи единой информационной платформы, а также предполагает создание новой подсистемы — подсистемы обработки обезличенных данных, а также вводит новые роли участников единой информационной платформы: поставщиков подсистемы обработки обезличенных данных единой информационной платформы и пользователей подсистемы обработки обезличенных данных единой информационной платформы.

21.02.2025 было опубликовано еще два проекта.

Первый — постановление Правительства Российской Федерации «Об установлении Правил взаимодействия федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, с операторами, обрабатывающими персональные данные, в целях формирования составов персональных данных, полученных в результате обезличивания персональных данных, сгруппированных по определенному признаку, при условии, что последующая обработка таких данных не позволит определить принадлежность таких данных конкретному субъекту персональных данных» — предлагает описание организационной стороны вопроса, без указания методов обезличивания ПДн, которые должны быть определены отдельно правительством по согласованию с ФСБ России.

Второй — постановление Правительства Российской Федерации «Об определении случаев формирования составов персональных данных, полученных в результате обезличивания персональных данных, сгруппированных по определенному признаку, при условии, что последующая обработка таких данных не позволит определить принадлежность таких данных конкретному субъекту персональных данных». Случаи формирования составов данных определены в нем с учетом высокой значимости ситуаций для государства и общества (чрезвычайные ситуации, противодействие терроризму, распространение инфекционных заболеваний, экономические, социальные, статистические исследования).

24.02.2025 опубликован проект Федерального закона «О внесении изменений в Федеральный закон «Об

электронной подписи»». Законопроектом предусматривается, что создание и выдача квалифицированных сертификатов ключа проверки электронной подписи государственных органов, не имеющих основного государственного регистрационного номера, будет осуществляться Казначейством России. Также предусматривается возможность передоверия полномочий в электронной форме при использовании квалифицированной электронной подписи и расширение субъектного состава финансовых организаций, которым удостоверяющий центр Банка России выдаёт сертификат ключа проверки электронной подписи.

28.02.2025 опубликован Федеральный закон от 28.02.2025 № 23-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и отдельные законодательные акты Российской Федерации». Изменения вводят особый порядок обработки ПДн работников так называемых «силовых» ведомств.

ПРЕЗИДЕНТ И ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

09.01.2025 была опубликована утвержденная 30.12.2024 распоряжением Правительства Российской Федерации № 4154-р «Концепция государственной системы противодействия преступлениям, совершаемым с помощью информационно-коммуникационных технологий».

17.01.2025 Правительство Российской Федерации опубликовало проект постановления «О внесении изменений в постановление Правительства Российской Федерации от 29.06.2021 № 1046». Предлагаемые изменения коснулись порядка осуществления федерального государственного контроля (надзора) за обработкой ПДн, в том числе действий в отношении оператора ПДн при выявлении нарушений в его деятельности.

18.01.2025 было опубликовано постановление Правительства Российской Федерации от 18.01.2025 № 12 «О внесении изменения в постановление Правительства Российской Федерации от 15.09.2008 № 687», устанавливающее срок действия постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» до 01.09.2030.

17.02.2025 в Госдуму был внесен проект федерального закона № 842276-8 «О создании государственных информационных систем по противодействию правонарушениям (преступлениям), совершаемым с использованием информационно-телекоммуникационных технологий, и о внесении изменений в отдельные законодательные



акты Российской Федерации». Законопроект предполагает введение следующих мер:

- ♦ обязательная идентификация клиентов и пользователей в различных сферах;
- ♦ запрет банковским работникам, работникам маркетплейсов и госорганов использовать определенные зарубежные мессенджеры в служебных целях;
- ♦ обязательная маркировка звонков от юридических лиц или массовых вызовов;
- ♦ меры против похищения СМС-сообщений об изменении пароля от Госуслуг;
- ♦ информирование абонентов о том, что принятый ими вызов шел из-за рубежа;
- ♦ возможность самозапрета на заключение новых договоров оказания связи.

ФСТЭК РОССИИ

10.02.2025 ФСТЭК России обновил «План проведения плановых проверок по вопросам лицензионного контроля на 2025 год».

17.02.2025 опубликовано информационное сообщение ФСТЭК России от 06.02.2025 № 240/11/589 «О формах представления сведений о кадровом обеспечении подразделений специалистами по защите информации». Перечень респондентов для представления сведений приведен в приложении к данному сообщению.

24.02.2025 ФСТЭК России опубликован проект национального стандарта «Защита информации. Системы с конструктивной информационной безопасностью. Методология разработки». Стандарт определяет конструктивную информационную безопасность как подход, при котором система с момента её создания проектируется с учётом требований безопасности, и описывает методологию разработки систем с конструктивной

информационной безопасностью, которая включает процессы планирования, анализа, проектирования, реализации, тестирования и сопровождения систем. Особое внимание уделяется синхронизации требований безопасности с основным функционалом системы. Предлагается использовать шаблоны проектирования, которые помогают решать типовые задачи разработки безопасных систем.

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

28.01.2025 были опубликованы «Методические рекомендации Банка России по проведению тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры организаций финансового рынка» от 22.01.2025 № 2-МР.

Документ формализует подход к проведению работ по тестированию на проникновение и анализу уязвимостей информационной безопасности (ИБ), и устанавливает рекомендации по планированию и проведению тестирования на проникновение и анализа уязвимостей самостоятельно и с привлечением подрядных организаций, рекомендации по формированию отчета о проделанной работе, а также указан порядок информирования Банка России о результатах работ.

ОТРАСЛЕВЫЕ ДОКУМЕНТЫ

13.01.2025 опубликован принятый 28.12.2024 ГОСТ Р 71223–2024 «Вычислительная техника. Термины и определения». Стандарт вступит в силу 01.06.2025.

28.01.2025 опубликован приказ Министерства просвещения Российской Федерации от 24.12.2024 № 1025 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.13 «Интеграция решений с применением технологий искусственного интеллекта»».

03.03.2025 был принят национальный стандарт ГОСТ Р 59999–2025 «Цифровой документооборот организации. Требования к эталонной модели». Стандарт вступает в силу 01.12.2025.

11.03.2025 были приняты национальные стандарты, вступающие в силу 31.03.2025:

♦ ГОСТ Р 59453.3–2025 «Защита информации. Формальная модель управления доступом. Часть 3. Рекомендации по разработке»;

♦ ГОСТ Р 59453.4–2025 «Защита информации. Формальная модель управления доступом. Часть 4. Рекомендации по верификации средства защиты информации, реализующего политики управления доступом, на основе формализованных описаний модели управления доступом».



18-й Межотраслевой форум директоров
по информационной безопасности

CISO FORUM 2025

10 апреля 2025
Loft Hall, Москва



infosecurity-forum.ru

18+

1 000+
гостей
форума

>50%
CISO
в программе

2 лофта
для контента
и крутой экспо-зоны

Реклама

Это школа Соломона Пляра
Школа бальных танцев, Вам говорят.
Две шага направо, две шага налево,
Шаг вперед и две назад.
И. С. Руденков

ШКОЛА БАЛЬНЫХ ТАНЦЕВ, ВАМ ГОВОРЯТ...

РАЗМЫШЛЕНИЯ НАД ПРОЕКТОМ НОВЫХ ТРЕБОВАНИЙ
ФСТЭК РОССИИ ВЗАМЕН ТРЕБОВАНИЙ ДЛЯ ГИС,
УСТАНОВЛЕННЫХ ПРИКАЗОМ ФСТЭК РОССИИ № 17



Сергей ВИХОРЕВ
советник Генерального директора
ООО «Умные решения»

В декабре 2024 года был опубликован проект «Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», которые идут на смену знаменитому приказу ФСТЭК России № 17, устанавливавшему требования по защите информации в ГИС. Планируется, что они вступят в силу в 2026 году. Отрадно, что ФСТЭК России проводит большую работу по совершенствованию защиты информации в государственных информационных системах. Главное, чтобы этот процесс шел не по крылатой фразе В. С. Черномырдина: «Хотели как лучше, а получилось как всегда». Вопросов к новому документу много. Наверное, в дальнейшем будут дополнительные разъяснения, как его применять. Но хотелось бы сделать так, чтобы лишних вопросов, требующих дополнительных комментариев, было меньше. Вот поэтому я и хочу задать несколько вопросов заранее. Может быть, это поможет немного «подрихтовать» такой нужный документ.

ОХ, УЖ ЭТОТ ВЕЛИКИЙ МОГУЧИЙ РУССКИЙ ЯЗЫК

Полтора века назад Иван Сергеевич Тургенев сказал: «Во дни сомнений, во дни тягостных раздумий о судьбах моей родины, — ты один мне поддержка и опора, о великий,

могучий, правдивый и свободный русский язык!»¹. Вот и я сейчас в сомнениях. Конечно, классик вряд ли мог себе представить, что к XXI веку язык пополнится новыми выдуманными словами, заимствованиями и многим другим. Это я о названии нового документа. Очень режет слух: «Требования о защите информации...» Я уж подумал, что, наверное, отстал от норм русского языка. (Правда, и в законах можно найти такое выражение, но насколько это правильно? В наших законах можно еще и не такое увидеть, но это не делает им чести.) Но все-таки, в официальном документе должны, на мой взгляд, использоваться устоявшиеся и узаконенные термины. Оказывается, что я был недалеко от истины. Достаточно было глянуть в действующий ГОСТ Р 50922 «Защита информации. Основные термины и определения»: требование по защите информации — установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации². Так что лучше прислушиваться к ГОСТу и не выдумывать новые сущности. Ну, это не главное, это так, записки на полях...

АНАЛОГИИ ИЗ ПРОШЛОГО: ЗАЧЕМ ДВА РАЗА НАСТУПАТЬ НА ГРАБЛИ?

Хочу вспомнить историю появления ГОСТ ИСО/МЭК 15408, известного как «Общие критерии», его первую реинкарнацию начала 2000-х годов. Первоначально предполагалось, что владельцы информационных систем могут выбрать из каталога оцененных профилей защиты наиболее подходящий по условиям использования своих информационных систем (именно систем, а не средств защиты) или разработать свой профиль защиты. Такой подход грозил лавинообразным ростом количества профилей, что, естественно, могло бы существенно затруднить не только сертификацию средств защиты, но и зна-

¹ И. С. Тургенев, заметка «Русский язык», 1882 г.

² ГОСТ Р 50922-2006: Защита информации. Основные термины и определения, п. 2.9.2

чительно удорожало сам процесс защиты информации³. Слава Богу, этого не произошло. Объяснялось это с одной стороны трудностями при разработке профилей — требовалось наличие высококлассных специалистов, что было не по карману многим владельцам информационных систем, а с другой стороны — отсутствием самого депозитария готовых профилей.

Зато весь процесс разработки профилей вошел в нужное русло: профили стали разрабатывать под эгидой ФСТЭК России, профили стали разрабатывать для определенных классов средств защиты (например, межсетевые экраны, операционные системы и т.д.). И при этом, для каждого класса средств защиты были определены различные типы таких средств защиты (например, тип А, Б, В и т.д.). А самое главное, требования, изложенные в этих профилях, были детализированы относительно классов защиты информационных систем. То есть, был разработан не один профиль, а семейство профилей для каждого типа средств защиты. Ну, и надо заметить, что все требования в этих профилях были проверены и имели определенный уровень доверия. И теперь, владельцу информационной системы, знающему требуемый класс защищенности своей системы, даже не имея высококлассных специалистов (читай дорогих), было легко выбрать требуемое средство защиты, покрывающее его потребности по степени защиты информации (нейтрализации указанных в профиле угроз безопасности информации) и уровню доверия к реализации функций безопасности. И это хорошо!

СПАСЕНИЕ УТОПАЮЩИХ — ДЕЛО РУК САМИХ УТОПАЮЩИХ

А что в новых требованиях? Именно оператор должен разработать внутренние стандарты по защите информации, устанавливающие требования к реализации мер по защите информации⁴. При этом, сами мероприятия по реализации в информационных системах мер по их защите и содержащейся в них информации должны включать реализацию базового набора мер защиты информационных систем и содержащейся в них информации соответствующих классов защищенности⁵. То есть, говоря простым языком, Оператор сам должен сформировать требования по защите информации. А сможет ли он это сделать⁶? А есть ли у него достаточное количество квалифицированных специалистов для формирования таких требований? Это же практически разработка профиля защиты для своей информационной системы. По-большому, это требует применения математических (формальных) моделей угроз, которые позволяют провести обоснование требований и выбор нужных мер защиты с оценкой достигаемой эффективности защиты ин-

формации, с решением задач оптимизации построения системы защиты в информационной системе⁷.

И мы, вольно или невольно, возвращаемся к ситуации начала 2000-х годов со всеми теми трудностями, которые описаны выше. Такой подход приведет к удорожанию системы защиты информации при сомнительном доверии к ее качеству. Ведь принимаемые меры по защите информации должны быть направлены на блокирование (нейтрализацию) актуальных угроз безопасности информации⁸. К сожалению, требования, приведенные в самом документе⁹, в этой ситуации не помогут, потому что они не детализированы по классам защищенности информационных систем (о привязке к угрозам — будет ниже). Да и что такое «базовый набор мер», который надо адаптировать и верифицировать¹⁰, не ясно. Учтем также и тот факт, что методический документ, определяющий меры защиты информации¹¹, который помогал правильно сформировать требования к информационной системе, автоматически прекращает свое действие с отменой приказа ФСТЭК России № 17.

А какие проблемы будут при аттестации информационных систем! На что аттестовывать? На требования, которые придумал оператор? Не получится ли здесь как в басне И. А. Крылова¹²? Ведь оператор, как лицо заинтересованное, придумает не те меры, которые требуются для определенного уровня защиты, а те, что попроще, подешевле. Кто может гарантировать достаточность принимаемых оператором мер защиты? Вопрос открытый.

Мне возразят, мол, можно использовать требования профилей защиты для средств защиты соответствующего класса защищенности информационной системы. Вроде бы так, но, к сожалению, существующие семейства профилей не перекрывают весь спектр мер, предусмотренных новыми требованиями¹³, следовательно, это и не реально. Вот и получается, что оператор брошен в бурный поток защиты информации, а выплывет он или нет — это сугубо его дело.

ЧТО В ЛОБ, ЧТО ПОЛЕЗУ

Сейчас требования к мерам по защите информации не привязаны к угрозам. В новых требованиях угрозы не привязаны к требованиям. Об этом мы говорим уже не первый раз и не первый год¹⁴. В требованиях, введенных приказом ФСТЭК России № 17, есть абзац: «Требования к системе защиты информации информационной системы определяются в зависимости от класса защищен-

³ Я уже как-то писал об этом, см. BIS JOURNAL № 1 / 2020, С. Вихорев, «Перемен! — требуют наши сердца»

⁴ П. 23 проекта Требований

⁵ П. 53 проекта Требований

⁶ См. также BIS JOURNAL № 1 / 2020, Ю. Язов, «Вершина айсберга во тьме».

⁷ См. BIS JOURNAL № 2 / 2021, Ю. Язов, «Нищета... знаний о БДУ»

⁸ П. 30 проекта Требований

⁹ Раздел III проекта Требований

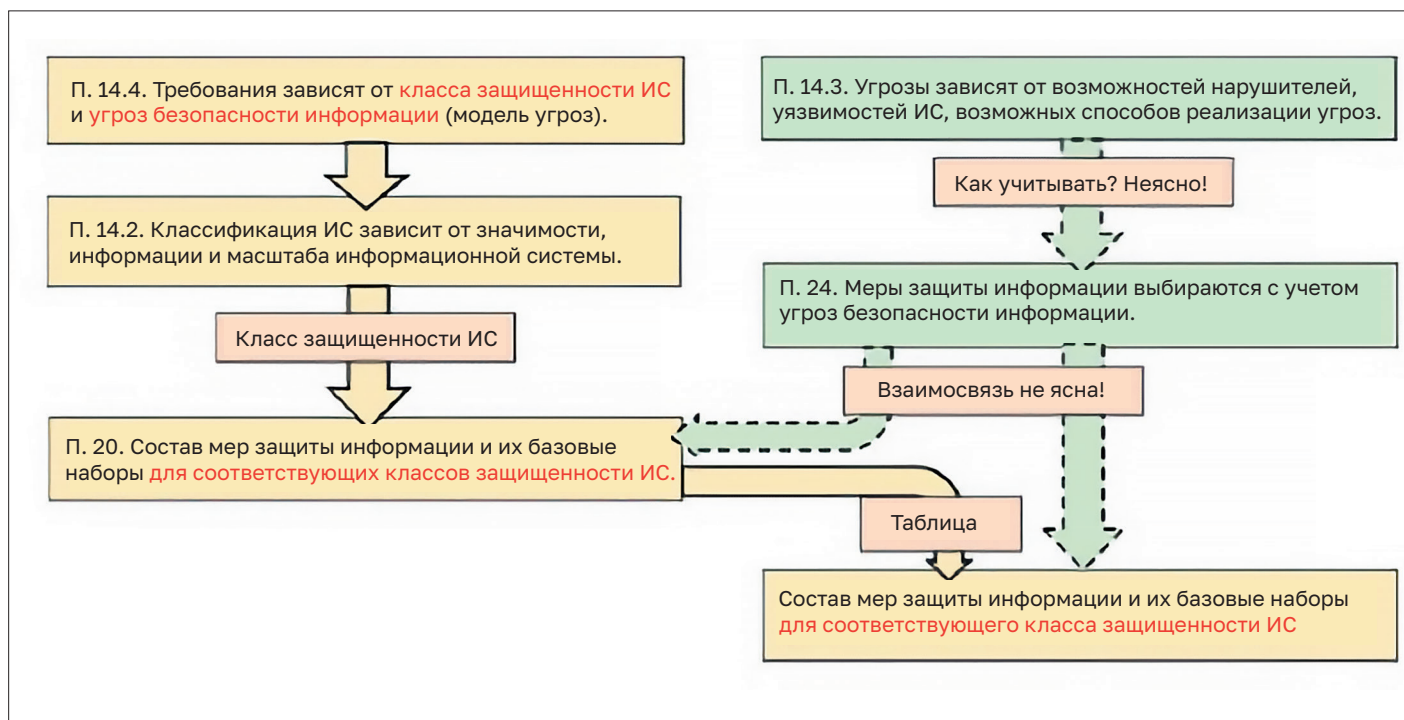
¹⁰ П. 53 проекта Требований

¹¹ «Методический документ. Меры защиты информации в государственных информационных системах», утв. ФСТЭК России 11.02.2014

¹² И. А. Крылов, басня «Медведь у пчел», 1818

¹³ Раздел III проекта Требований

¹⁴ Например, дискуссия в журнале BIS JOURNAL № 2 / 2021 С. Вихорев, «Блеск и нищета... БДУ», А. Калашников, «Главное — ущерб», В. Окулесский, «Тусклый блеск... почти науки», Ю. Язов, «Нищета знаний ... о БДУ»



ности информационной системы и угроз безопасности информации, включенных в модель угроз безопасности информации¹⁵. И далее: «В качестве исходных данных для определения угроз безопасности информации должен использоваться банк данных угроз безопасности информации» (bdu.fstec.ru). Но это только декларация! На самом деле меры защиты выбираются исходя из класса защищенности информационной системы, который, определяется совсем по другим критериям, но никак не отталкиваясь от угроз. Ну здесь хотя бы есть альтернатива: если не от угроз, то хоть от класса защищенности информационной системы.

Да и сам банк данных угроз, на который дается ссылка, никак не говорит какую угрозу каким методом можно устранить или ослабить. Нет взаимосвязи между самими угрозами и теми мерами, которые позволяют их нейтрализовать. Получается, что в данном случае угрозы, вернее модель угроз, построенная на их основе, выступает в качестве некоего «сферического коня в вакууме».

Правда, на просторах интернета можно найти некие таблицы, где сопоставляются угрозы безопасности информации мерам защиты, изложенным в приказах ФСТЭК России¹⁶, но это, к сожалению, только личное мнение блогера (хотя и правильное и вполне разумное).

В новых же требованиях вообще нет альтернативы: «Модель угроз безопасности информации ... должна использоваться в качестве исходных данных для разработки и внедрения мер по защите информации, а также для выбора средств защиты информации и их функци-

ональных возможностей в ходе создания (развития) подсистем защиты информации информационных систем¹⁷. Здесь нигде ничего не сказано о классах защищенности информационных систем, да и привычной таблицы мер тоже нет.

Безусловно, сама идея — использовать модель угроз при выборе мер защиты — абсолютно верная. Однако, не отрицая важности самого процесса оценки угроз безопасности информации при выборе адекватных мер защиты, такая идея действительно будет работать, если каждой угрозе будет сопоставлена соответствующая мера или совокупность мер защиты информации с обязательной оценкой доверия к ее эффективности (и вряд ли это под силу специалистам оператора, ответственным за формирование требований по защите информации для своих информационных систем). А пока этого нет — подход, изложенный в новых Требованиях, вряд ли можно реализовать. Ну, точно как у дедушки Крылова: «Вертит Очками так и сяк: То к темю их прижмёт, то их на хвост нанижет, То их понюхает, то их полижет; Очки не действуют никак¹⁸». И происходит это по банальной причине: нет связи между угрозами и мерами.

И еще, по поводу использования модели для выбора средств защиты и их функциональных возможностей. Эх, эти бы слова, да Богу в уши...

Р.С. Я, конечно, не ретроград, но все же золотое правило IT-шников: «работает — не трогай!» бывает справедливым...

¹⁵ «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утв. Пр. ФСТЭК от 11.02.2013 № 17, п. 14.4

¹⁶ Например, в блоге Сергея Борисова про ИБ https://sborisov.blogspot.com/p/blog-page_13.html

¹⁷ п. 35 проекта новых Требованияй

¹⁸ И. А. Крылов, басня «Мартышка и очки»

ПОД ШКВАЛОМ ЯРОСТНЫХ DDoS

КАК БАНКИ ПРОТИВОСТОЯТ КИБЕРУГРОЗАМ



**Вероника
ГОРЯЧЕВА**
корреспондент
BIS Journal

О б успешных DDoS-атаках на кредитные организации, которые привели к многочасовой недоступности сервисов, сообщали СМИ и в 2025 году, и в 2024-м. Однако главная волна подобных атак на финсектор началась в феврале 2022 года, когда банки были вынуждены пересмотреть свой взгляд на информационную безопасность.

В 2024 году Международный валютный фонд в «Докладе по вопросам глобальной финансовой стабильности» особое внимание обращал на возросшие киберриски для банков, следствием которых является и угроза финансовой стабильности многих стран. В частности, в докладе указывается на двукратный рост числа киберинцидентов почти с допандемийных времён. По данным опроса ЕУ, результаты которого были опубликованы в начале 2024 года, 82 % главных директоров по рискам (CRO) европейских банков назвали киберриски главными из рисков, причём 71 % CRO говорили об атаках хактивистов как главном из киберрисков.

Это утверждение актуально и нашей страны. «Большое количество атак на российские компании начиная с 2022 года обусловлено геополитической ситуацией», — подтверждает в своём исследовании «Актуальные киберугрозы в странах СНГ 2023–2024» компания Positive Technologies.

И здесь банки являются одной из наиболее популярных мишеней хактивистов. «Ещё три года назад и более DDoS-атаки на финансовый сектор носили единичный характер, скажу больше — специалисты по информационной безопасности даже не рассматривали их как действительно серьёзную угрозу, так как к длительной недоступности сервисов они не приводили, — рассказывает директор по продуктам Servicepipe Михаил Хлебунов. — Однако напряжённая геополитическая обстановка и активизация хактивистов изменили отношение кредитных организаций к этому типу киберугроз».

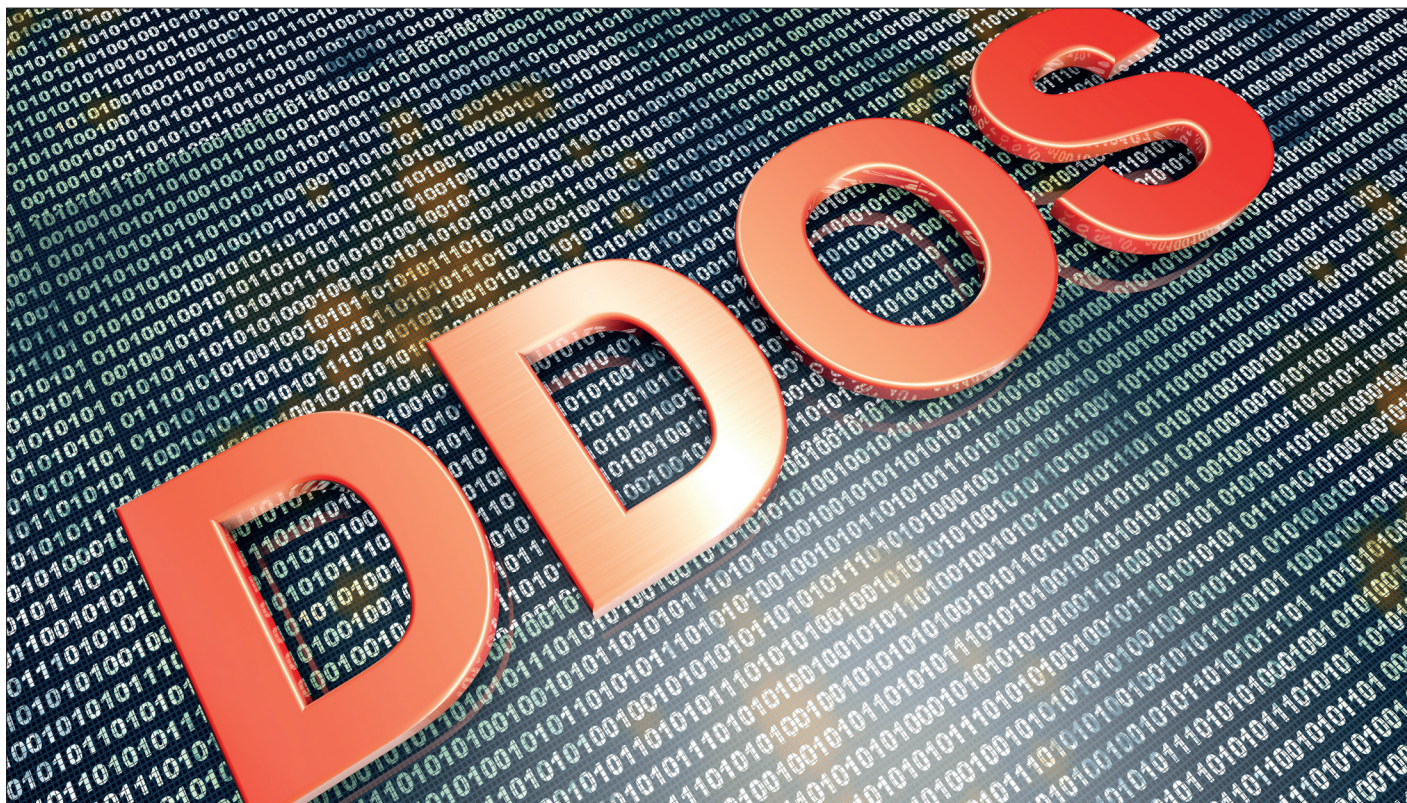
Действительно, до 2022 года DDoS-атаки на кредитные организации «были относительно редкими», подтверждает в интервью CNews директор департамента информационной безопасности Московского кредитного банка (МКБ) Вячеслав Касимов. Да и цели таких атак были иными: «Тогда не было стремления сделать атаку резонансной, не было желания опубликовать информацию о том, что какой-то банк недоступен и его клиенты испытывают неудобства. DDoS-атаки в основном носили коммерческий характер».

Но в феврале 2024 года всё изменилось: атаки хактивистов с каждым годом становились всё изощрённее. «Например, летом 2024 года на отрасль обрушились многовекторные ковровые атаки, когда вредоносный трафик направлялся по большому количеству IP-адресов, — указывает Михаил Хлебунов. — Если в начале 2024 года злоумышленники атаковали в среднем 10–15 % IP-адресов финансовой организации, то в июне в среднем — 98,5 % IP-адресов одновременно. Мы видели «ковры» площадью более чем 400 IP-адресов», — резюмировал эксперт. При этом мощность атак во II квартале 2024 года выросла на четверть.

Как ранее в интервью snews.ru отмечал Вячеслав Касимов, МКБ также подвергался ковровым атакам. Например, последняя, произошедшая в сентябре прошлого года, была рекордной по мощности: 300 Гбит/с, а на пике — 310 Гбит/с. Не обошли стороной хактивисты и другие российские банки. В частности, крупнейшая отечественная кредитная организация пережила мощнейшую в её истории DDoS-атаку в конце июля 2024 года, рассказывал в интервью «РИА Новостям» заместитель председателя правления «Сбера» Станислав Кузнецов. Она длилась 13 часов, и её мощность, по его словам, составляла 500 Гбит/с. Подобные новости об атаках поступали и от многих других российских банков.

Проблема роста количества и мощности кибератак на российские банки соседствует с другой. Как ранее отмечал Вячеслав Касимов, «до определённого времени Россия использовала в основном западные решения для защиты от DDoS-атак». Однако в настоящее время они стали менее доступны. Когда западные вендоры покинули отечественный рынок, возникла дилемма: «либо платить повышенную премию для организации параллельного импорта, либо искать альтернативные варианты», рассказывал топ-менеджер.

К счастью, на рынке уже были зрелые решения. По словам директора по продажам ИТ-интегратора «Телеком биржа» Василия Полькина, сложнейшие DDoS-атаки, обрушившиеся на отечественный бизнес и госкомпанию после событий 2022 года, стали определённой школой жизни для отечественных вендоров. На сегодняшний день можно уже говорить, что российские решения вышли на уровень топовых западных вендоров, являясь достойной альтернативой для решения поставленных задач, резюмировал он.



Как ранее сообщал Forbes, к 2023 году уже лишь 10 % крупнейших российских компаний использовали зарубежные решения для защиты от DDoS-атак. К 2024 году эта цифра ещё больше сократилась — до 6,5 %, приводит издание IT Channel News.

По словам Василия Полькина, изменение регуляторных требований в отношении субъектов критической инфраструктуры способствовало активному переходу на российские решения. Кредитные организации имеют особый статус в законодательстве о КИИ, потому для них это особенно актуально.

По пути применения отечественных решений пошёл, в частности, и МКБ. «В нашем случае это, в частности, решения российского вендора Serviceripe, которые мы внедрили с помощью ИТ-интегратора „Телеком биржа“, — рассказывает Вячеслав Касимов. По его словам, в том числе благодаря совместной работе вендора и интегратора банку удалось успешно справиться с сентябрьской DDoS-атакой.

По словам Василия Полькина, при этом финансовые игроки в первую очередь интересуются решениями on-premise, которые удовлетворяют

всем регуляторным требованиям и обеспечат кредитной организации желаемый контроль над трафиком.

Вячеслав Касимов также подтвердил, что банкам нужен именно ПАК (программно-аппаратный комплекс). «Мне кажется, что утверждения о том, что ПАК не нужен, исходят либо от людей, не совсем понимающих все риски, либо от тех, кто не придаёт значения конфиденциальности данных своих клиентов и фактически передаёт эту информацию третьим сторонам — сервис-провайдерам, — пояснял он в интервью CNews. — Когда трафик не идёт напрямую в организацию, а проходит через сервис-провайдера, то он имеет доступ ко всей информации, которая передаётся: от финансовых данных до личных данных клиентов, и только после этого трафик поступает в организацию». Это, конечно, создаёт дополнительные риски для безопасности и конфиденциальности данных, — резюмировал он.

При этом эксперт подчеркнул, что «одной «чудо-железки», то есть программно-аппаратного комплекса, при серьёзной атаке может быть недостаточно — её нужно будет масштабировать». Поэтому МКБ использует гибридные схемы, которые включают

как ПАК, так и возможность подключения облачного сервиса для защиты, а именно — решения российского вендора Serviceripe, которые банк внедрил с помощью ИТ-интегратора «Телеком биржа».

Атаки на банки, отмечает в своём блоге МВФ, могут «даже поставить под угрозу платёжеспособность» финансовых организаций, не говоря уже о репутационных издержках, которые сложно оценить в денежном выражении.

«Если раньше при коммерциализированных атаках основной целью было просто украсть деньги, при этом не нанося серьёзного ущерба, то сейчас хактивисты преследуют множество целей, — рассказывает Вячеслав Касимов. — Если есть возможность украсть деньги, они это сделают, если можно эксплуатировать конфиденциальную информацию или передать её третьим лицам, они, безусловно, это сделают». Если же ни первое, ни второе невозможно, то они наверняка постараются разрушить инфраструктуру, указывает эксперт, и сетевые угрозы в этом году никуда не денутся, хотя принципиальных изменений в формах DDoS-атак ожидать, скорее всего, не стоит.

ЕСЛИ НЕ КОНТРОЛИРОВАТЬ СВОЙ ПЕРИМЕТР, ЕГО БУДУТ КОНТРОЛИРОВАТЬ ДРУГИЕ

ПИЛОТНЫЕ ПРОЕКТЫ РЕШЕНИЯ F6 ASM КАЖДЫЙ РАЗ ВЫЯВЛЯЮТ ПРОБЛЕМЫ НА ПЕРИМЕТРЕ, О НАЛИЧИИ КОТОРЫХ НИКТО НЕ ДОГАДЫВАЛСЯ



Николай СТЕПАНОВ
технический
руководитель
F6 Attack
Surface
Management



Владимир СОЛОВЬЕВ
руководитель
группы
внедрения
систем
защиты от атак
АО «ДиалогНаука»

Бурный рост компаний, слияния-поглощения, текучка кадров, а иногда банальное безразличие к контролю своего внешнего периметра приводят к появлению множества «мёртвых», так называемых теневого активов. А поскольку любая хакерская атака начинается с разведки, киберпреступники в первую очередь ищут оставленное без присмотра сетевое оборудование — то, которое уже устарело, не контролируется, но всё же обладает доступом к корпоративной сети, или уязвимые сервисы, которые также не обновлялись длительное время, но всё ещё имеют принадлежность к корпоративной сети.

Довольно часто заказчики приходят с вопросом: как усилить свою кибербезопасность без значительных затрат времени и средств? Рекомендация одна — начать с внедрения системы управления поверхностью атаки (Attack Surface Management, ASM). В этой статье мы поговорим о том, что такое ASM, и на примере одного из лидеров отечественного рынка выясним, какие задачи решают системы класса ASM

и куда вообще движется рынок решений данного класса.

ЗНАКОМСТВО С ASM

Понимание того, что именно надо защищать и какие элементы уязвимы, — первый шаг на пути к последовательной и эффективной стратегии защиты.

F6 Attack Surface Management (F6 ASM) — это комплексное информационно-аналитическое SaaS-решение, предназначенное для оценки поверхности атаки компании. Оно позволяет отслеживать незащищённые участки внешнего периметра, потенциальные уязвимости, теновые активы и некорректно настроенные элементы сети, которые потенциально могут быть использованы злоумышленниками в кибератаках (рис. 1).

Система позволяет выявить активы с высоким уровнем риска, выделить слабые места организации и соответствующим образом исправить ситуацию с целью предотвращения атак.

Достигается это путём применения множества различных сканеров (как с открытым кодом, так и самописных), которые позволяют обнаруживать забытые активы, устаревшее и уязвимое ПО, открытые порты

и т.д. А глубокая интеграция с системой киберразведки — F6 Threat Intelligence (F6 TI) — позволяет подсвечивать упоминания в дарквебе и активность ВПО, направленного на периметр компании.

F6 ASM — это полностью отечественная разработка. Хранение данных клиентов F6 осуществляется исключительно на территории России. Установка не требуется, система настраивается в несколько кликов.

Как появился данный продукт? Из «графа».

НАСЛЕДНИК ГРАФА

История F6 ASM уходит корнями к другой разработке компании — графу сетевой инфраструктуры. Это запатентованная технология системы киберразведки — F6 TI, которая позволяет визуализировать связи между доменами, IP, сервер-сертификатами, злоумышленниками и сообщениями в дарквебе (рис. 2).

Изначально граф создавался для проведения расследований — это крайне полезный инструмент, чтобы распутать сложную атаку, деанонимизировать злоумышленника или найти инфраструктуру злоумышленников. Именно так он и использовался, пока не было замечено, что пользователи решения ищут не IP-адреса преступников, а заносят свои, чтобы найти связи.

Поэтому вопрос «если мы и так сканируем весь интернет и строим связи, почему бы нам не помочь клиентам держать их внешнюю инфраструктуру под контролем?» оказался для разработчиков F6 ASM абсолютно логичным.

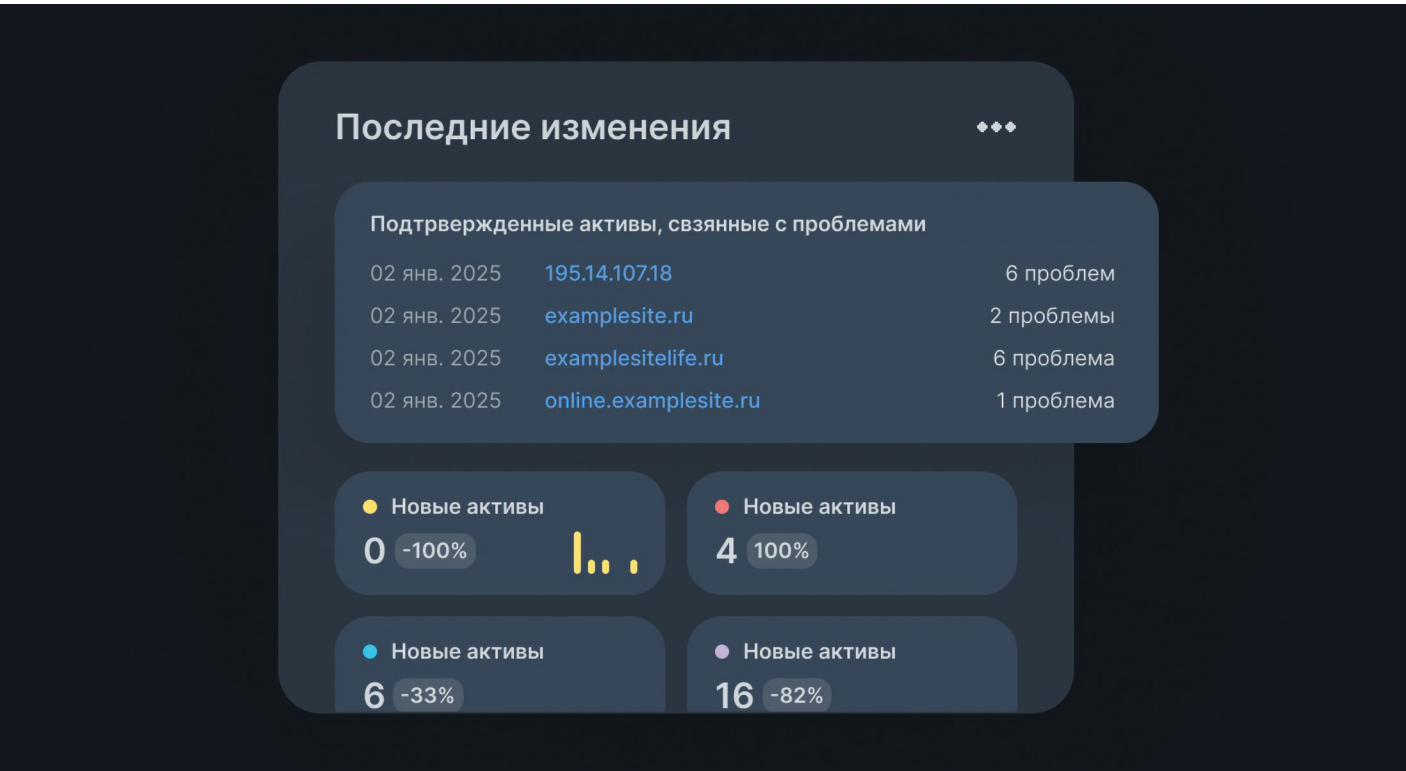


Рисунок 1. Обнаружение используемых и забытых теневых активов

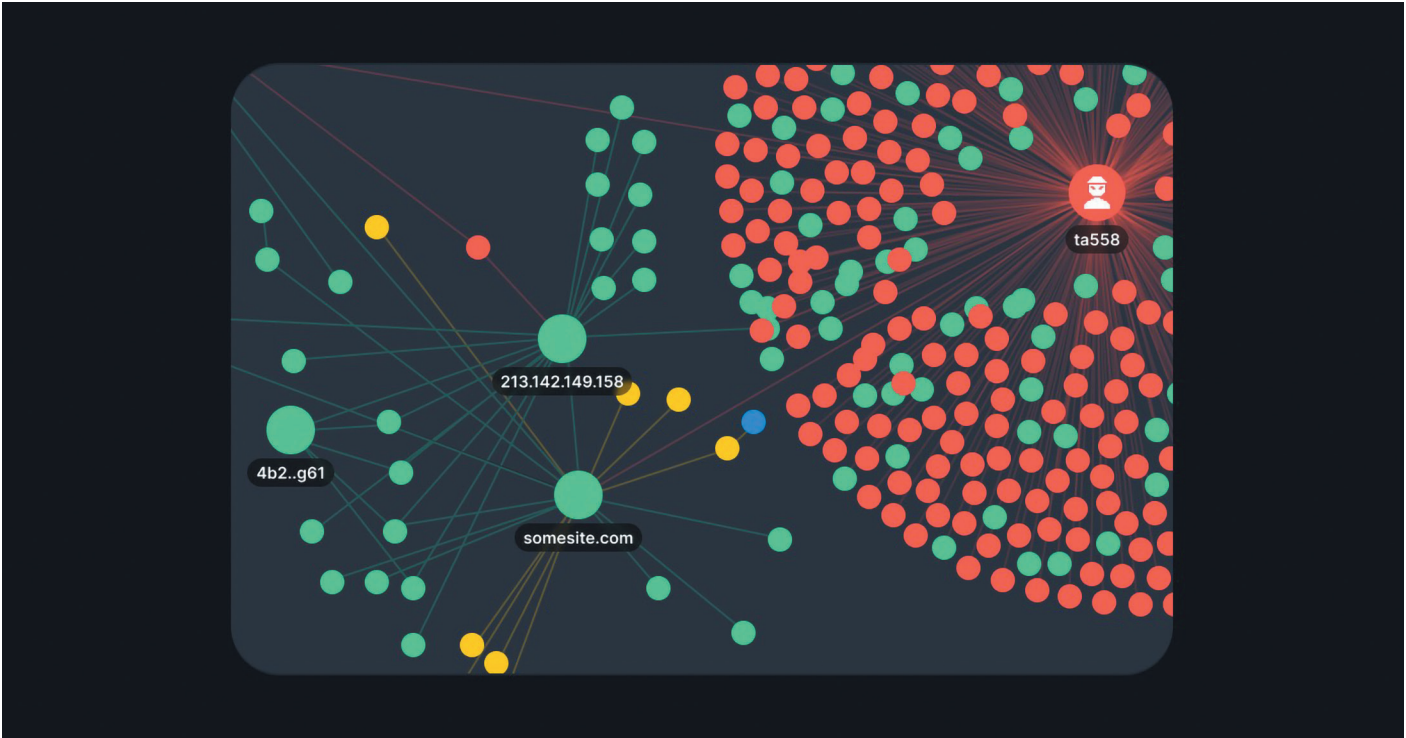


Рисунок 2. Графовый анализ сетевой инфраструктуры

АВТОМАТИЗАЦИЯ ЗАЩИТЫ ПЕРИМЕТРА

Со временем продукт технически развивался, но его суть оставалась неизменной. F6 ASM имеет восемь категорий, по которым проводит ежедневные проверки. Каждый

день эксперты F6 сканируют всю сеть Интернет и находят домены, IP-адреса, SSL-сертификаты, которые могут быть связаны с клиентом. После этого происходит проверка всех доменов и IP-адресов на предмет уязвимого ПО,

сопоставляя версии ПО и известные уязвимости, открытые порты, небезопасные заголовки на сайтах и почтовые записи (Dmarc, SPF). Также происходит обогащение данными киберразведки от системы F6 TI, чтобы найти упо-

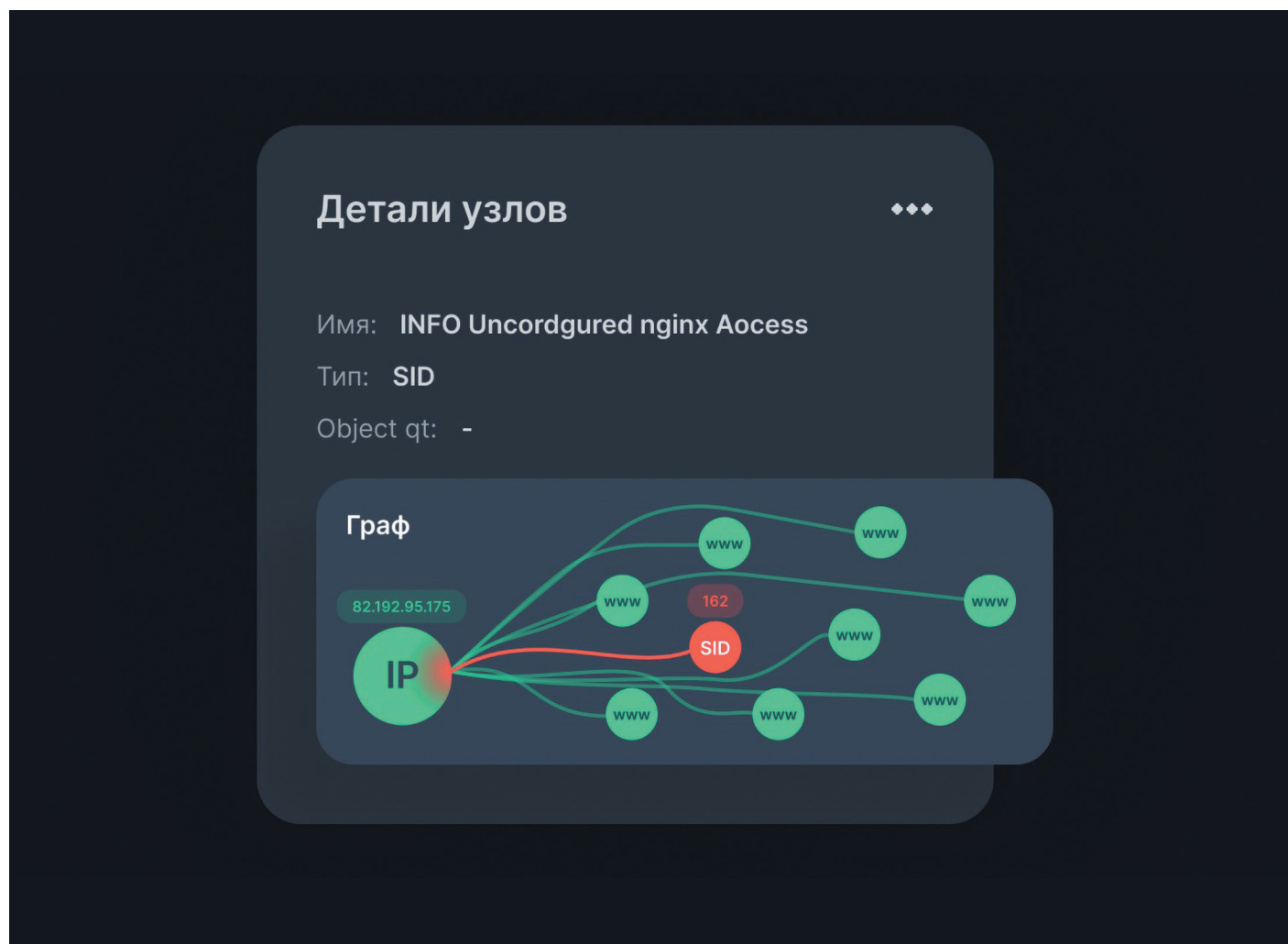


Рисунок 3. Непрерывный мониторинг всех изменений во внешней поверхности атаки

минание доменов или IP на хакерских форумах или внутри конфигов ВПО (рис. 3).

Улучшая стабильность и скорость работы, эксперты F6 не переставали учитывать пожелания клиентов. Многие использовали F6 ASM для того, чтобы автоматизировать свою защиту периметра. Исходя из этого, к системе стали привлекаться аналитики Центра кибербезопасности (CDC), чтобы оперативно помогать клиентам устранять проблемы на периметре. Для тех, кто не хочет, чтобы кто-то, кроме их сотрудников, изучал проблемные точки компании, F6 выпустили обучающие курсы.

Наша основная цель — автоматизация защиты периметра. Когда от клиента требуется провести только определённую работу, а он уже знает, где проблема, что это за проблема, что нужно сделать, чтобы её решить.

ПЕРСПЕКТИВЫ ASM

Исходя из текущих запросов рынка, F6 начали готовиться к релизу активного сканирования. Сейчас F6 ASM работает таким образом, чтобы не «нагружать систему». Эксперты заметили высокий спрос на «активное сканирование», когда система автоматически пытается эксплуатировать известную CVE. Данную потребность доработали, и тем самым в системе появится возможность вносить собственный код, который будет автоматически обрабатывать по всем активам клиента.

Также на текущий момент имеется огромный спрос на on-prem решения. Для этого решение F6 ASM пересобрали таким образом, чтобы оно могло быть запущено на серверах клиента и только клиент мог получить доступ к своим просканированным данным. Это позволяет обезопасить клиента от передачи

внутренней информации за пределы компании.

Подводя итоги, суммируем: решения класса Attack Surface Management, в частности решение F6 ASM, обеспечивают полный мониторинг всех известных и неизвестных активов клиента, доступных извне, и позволяют эффективно реагировать на новые уязвимости и атаки до того, как они приведут к серьёзным последствиям. Для запуска от пользователя системы требуется лишь указать цели сканирования и далее только ожидать результата.

Пилотные проекты решения F6 ASM у наших заказчиков каждый раз выявляют проблемы на периметре, о наличии которых никто не догадывался. Поэтому необходимо постоянно контролировать внешний периметр и эффективно его защищать перед современными киберугрозами.

КОНСТРУКТОР-У

МОДЕЛЬ УГРОЗ И НИКАКИХ ОБЛАКОВ



Дмитрий СЛОБОДЕНЮК
коммерческий директор
ARinteg

Выстроить эффективную систему защиты информации невозможно без «Модели угроз и нарушителя безопасности информации» – документа, наличие которого будет интересовать представителей Роскомнадзора и ФСТЭК России, когда те придут с проверкой в компанию.

Вы же работаете с персональными данными (ПДн)? А для каждой информационной системы (ИС), персональных данных согласно 152-ФЗ, требуется «Модель угроз». Наличие такого документа – обязательное требование регуляторов и в отношении объектов КИИ (187-ФЗ), ГИС (Приказ № 17 ФСТЭК России).

Наши аудиторы подсчитали, что в среднем одной компании необходимо разработать от пяти «Моделей угроз». Работа это небыстрая и кропотливая.

И здесь на выручку им придет Конструктор-У – новый продукт компании ARinteg. Он позволяет за короткий срок разработать «Модель угроз», оперативно ее скорректировать при любых изменениях в инфраструктуре ИС. Для работы с Конструктор-У достаточно базовых знаний в области ИБ. И если у вас недостаточно опыта для разработки подобного документа или вам важно оптимизировать, упростить процесс его создания – этот продукт для вас.

С подготовленными при помощи Конструктор-У «Моделями угроз» вы сможете построить эффективную систему информационной безопасности. Напомним, что, например, согласно ст. 274.1 УК РФ, нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ РФ, грозит сроком от 5 до 10 лет. А с 30 мая 2025 года ужесточаются наказания за утечки персональных данных, вводятся оборотные штрафы до 3 % совокупного размера суммы выручки.

КАК РАБОТАЕТ КОНСТРУКТОР-У

При формировании «Модели угроз» Конструктор-У использует нормативную базу ФСТЭК России и лучшие практики в области ИБ. В ходе моделирования анализируются 222 угрозы из Банка данных угроз ФСТЭК России. Таким образом, Конструктор-У создаст для вас документ в соответствии с «Методикой оценки угроз безопасности информации» ФСТЭК России от 5 февраля 2021 г.

В качестве первичных исходных данных в Конструктор-У используются тип и архитектура информационных систем. Предварительно, конечно, эти данные собираются с IT-подразделений организации по готовому унифицированному опроснику. Обработав исходные данные, Конструктор-У оперативно представит вам «Модель угроз», разработанную для конкретной ИС, на 80–100 листах.

ДРУГИЕ ПРЕИМУЩЕСТВА РЕШЕНИЯ

Конструктор-У работает на операционных системах Windows и отечественных Linux-платформах, а также внутри закрытого контура (без доступа к интернету).

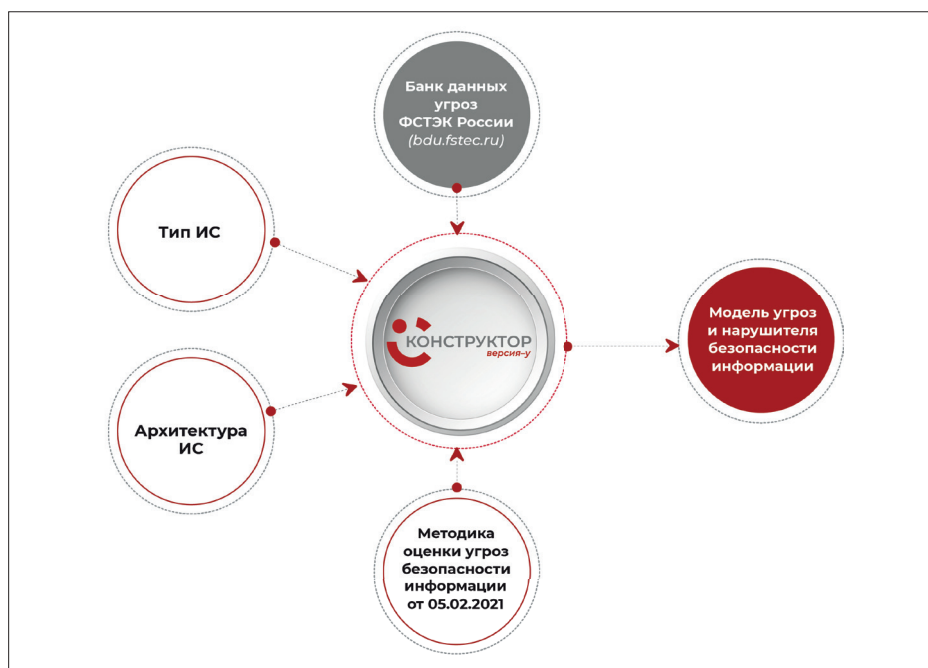
С Конструктор-У:

- ♦ можно вносить экспертные мнения специалистов в автоматизированный процесс создания документа, т.е. весь ваш опыт в нем может быть учтен;

- ♦ при изменении регуляторной базы пользователи ПО получают бесплатные обновления в рамках техподдержки.

И ещё важный момент: при разработке «Моделей угроз» исключено использование облаков, тем самым минимизированы угрозы ее дискредитации.

Конструктор-У от ARinteg в начале 2025 года прошел тестирование в ряде компаний и скоро поступит в активные продажи.



«МЫ СОЗДАЕМ ПРОДУКТ, КОТОРЫЙ ОТВЕЧАЕТ ВЫЗОВАМ ВРЕМЕНИ»



**Михаил
ИВАНОВ**
генеральный
директор
компании
«С-Терра
СиЭсПи»

Компания С-Терра, работая на рынке информационной безопасности более 20 лет, ставит перед собой ключевые цели — обеспечение комплексной защиты критически важной инфраструктуры, государственных и коммерческих организаций от современных киберугроз. За этот период нам удалось создать широкий спектр решений, соответствующих высоким стандартам качества и надежности.

ДОСТИЖЕНИЯ

Среди наиболее значимых достижений компании можно назвать следующие:

- ♦ Разработаны и внедрены решения для обеспечения безопасности сетей, в том числе межсетевые экраны нового поколения, обеспечивающие высокий уровень защиты.
- ♦ Произведена успешная интеграция наших продуктов в государственные и корпоративные информационные системы. — Обеспечено соответствие требованиям регуляторов, таких как ФСБ и ФСТЭК России.
- ♦ Осуществлено развитие экосистемы партнеров и создание собственной сети технической поддержки для бесперебойной работы наших продуктов.

УНИКАЛЬНЫЕ ВОЗМОЖНОСТИ

Требования по импортозамещению создают определённые вызовы, однако также предоставляют уникальные возможности для развития отечественных технологий. Наша компания активно участвует в процессе замещения иностранных решений на российском рынке, разрабатывая собственные продукты, которые не уступают зарубежным аналогам. Благодаря этому мы можем предложить заказчикам полноценные российские решения, соответствующие строгим стандартам информационной безопасности. Мы адаптировали наши разработки таким образом, чтобы соответствовать новым условиям и предлагать клиентам конкурентоспособные решения, отвечающие всем необходимым нормативным требованиям. Этот процесс помогает нам укреплять позиции на рынке и обеспечивать технологический суверенитет страны. Продукты нашей компании, особенно VPN шлюзы и межсетевые экраны, получили широкое признание среди российских заказчиков. Они применяются в различных отраслях, включая государственное управление, финансовый сектор, энергетику и телекоммуникации. Эти решения отличаются высокой степенью надежности и функциональностью, обеспечивая защиту от широкого спектра угроз.

МЕЖСЕТЕВЫЕ ЭКРАНЫ

Идея производить межсетевые экраны у компании возникла еще в 2020 году. Вначале изучали продукты, которые уже присутствовали на рынке. Когда появились тре-

бования регулятора, специалистам компании стало понятно, что нам по силам создать комплементарный продукт. В короткий срок было создано подразделение, которое «с нуля» начало разработку многофункционального МЭ. Данный пример показывает, что компании несложно создать именно то, что отвечает вызовам времени, и начать поддерживать и развивать продукт сразу с правильной позиции.

Многофункциональный межсетевой экран С-Терра — Экран-М разработан с учётом всех актуальных стандартов и требований ФСТЭК России. Наше решение обладает широким функционалом, включая фильтрацию трафика, контроль приложений, предотвращение вторжений и многое другое. По своим характеристикам и возможностям наш межсетевой экран сопоставим с лучшими иностранными аналогами. Более того, он обладает дополнительными преимуществами, такими как глубокая интеграция с отечественными стандартами шифрования и защиты от специфичных для российского рынка угроз. Одним из ключевых преимуществ является сертификация наших продуктов, что подтверждает их соответствие высоким стандартам безопасности. Заказчики доверяют нашим решениям, зная, что они обеспечивают необходимую защиту в условиях постоянно меняющейся киберугрозы.

РЕАГИРОВАТЬ НА ИЗМЕНЕНИЯ ЛАНДШАФТА

Угрозы кибербезопасности становятся всё более сложными и разнообразными, что требует постоянного

совершенствования наших продуктов и подходов к защите. Мы оперативно реагируем на изменения в ландшафте угроз, внедряем новейшие технологии и методы анализа для противодействия современным атакам.

Наши решения регулярно обновляются, чтобы учитывать актуальные тренды и тенденции в области информационной безопасности. Это включает интеграцию методов машинного обучения, поведенческого анализа и других передовых технологий для выявления и предотвращения атак на ранних стадиях.

ПРОДУКТОВАЯ ЛИНЕЙКА

Приведём примеры некоторых продуктов компании, пользующихся заслуженно высокой репутацией у клиентов. Продуктовая линейка компании «С-Терра СиЭсПи» позволяет защитить информационную систему любого масштаба: от небольшой локальной сети до инфраструктуры федерального уровня. Так, С-Терра Клиент, С-Терра Клиент А — это программные комплексы для защиты и фильтрации трафика с контролем состояния сессий для пользовательских устройств с ОС Windows и ОС Astra Linux.

Программно-аппаратный комплекс С-Терра Шлюз служит для обеспечения сетевой безопасности корпоративной сети любой топологии, с любым количеством туннелей. С-Терра Виртуальный Шлюз представляет собой VPN-шлюз в виде виртуальной машины, предназначенный как для защиты доступа к элементам виртуальной среды, так и для защиты взаимодействия между территориально-распределёнными компонентами сети. С-Терра СОВ служит для выявления компьютерных атак на основе анализа сетевого трафика. Продукты С-Терра позволяют решить любые задачи по защите взаимодействия сегментов корпоративной сети, выстраивая через недоверенную сеть защищённый IPsec-туннель. В результате все передаваемые данные оказываются под надёжной защитой: злоумышленник не может ни прочитать, ни изменить защищённые сообщения.

Продуктовая линейка компании «С-Терра СиЭсПи» позволяет защитить информационную систему любого масштаба: от небольшой локальной сети до инфраструктуры федерального уровня

СЕРТИФИКАЦИЯ

Продукты С-Терра, сертифицированные ФСБ России и ФСТЭК России, позволяют обеспечить защиту персональных данных (ПДн) в информационной системе (ИС ПДн) любого уровня защищённости, во исполнение ФЗ № 152 от 27.07.2006 «О персональных данных». Шлюзы безопасности С-Терра Шлюз, сертифицированные в качестве СКЗИ по классу КСЗ, входят в перечень оборудования, рекомендованного для организации защищённого взаимодействия с ГосСОПКА.

НОВЫЕ РЕШЕНИЯ

На текущий момент у нас в разработке несколько новых решений для клиентов. Особое внимание хочется обратить на квантовые технологии и нашу интеграцию с компанией «СМАРТС-Кванттелеком». Сопряжение оборудования С-Терры с квантовыми криптографическими системами выработки и распределения ключей СМАРТС-Кванттелеком позволяет обеспечить защиту информации пользователей на уровне квантовой физики. Система КВАЛИОН, разработанная нашими партнёрами, предназначена для выработки симметричных криптографических ключей, посредством передачи квантовых состояний между двумя модулями — Отправителем и Получателем. В основе работы лежит уникальный отечественный протокол квантового распределения ключей на боковых частотах (КРКБЧ), придуманный сотрудниками Университета ИТМО. Для построения разветвлённых квантовых сетей обеспечивается сопряжение одного СКЗИ сразу с несколькими модулями ККС ВРК, входящими в состав разных систем. Обеспечивается возможность реа-

лизации квантового канала по атмосферной линии связи при сопряжении с телескопической системой (дальность атмосферного канала до 50 м). Модули ККС ВРК конструктивно выполнены в отдельном корпусе, что позволяет обеспечить сопряжение с внешними СКЗИ по специализированному защищённому интерфейсу для обновления ключей в СКЗИ. Сопрягаемые СКЗИ обеспечивают защиту каналов связи в сетях произвольной топологии с производительностью от 100 Мбит/с до 100 Гбит/с с использованием квантовых или квантовозащищённых ключей.

УЧЕБНЫЕ ЦЕНТРЫ

Компания организовала авторизованные курсы в своих Учебных центрах. Преподаватели, обученные в компании «С-Терра СиЭсПи», на лекционных и практических занятиях знакомят слушателей с продуктами и решениями С-Терра, особенностями их применения, а также с правовыми основами в области защиты информации. Собственный обучающий семинар «Защита сетевой инфраструктуры на основе продуктов С-Терра» имеет длительность 2 дня. От практикующих инженеров компании слушатели узнают самую актуальную информацию о продуктах С-Терра, а также получают практические навыки реализации решений С-Терра.

Основным девизом для нашей компании является технологическое преимущество. Именно это мы ставим во главу своего развития, ведь наш продукт — в первую очередь высокотехнологичный.

ЛОКАЛЬНАЯ ЗАЩИТА ОТ БОТОВ — РЕАЛЬНОСТЬ ИЛИ УТОПИЯ?

КОЕ-ЧТО, ЧТО РАБОТАЕТ ЭФФЕКТИВНЕЙ ПРИВЫЧНОЙ КОРОБКИ



**Сергей
АНДРИЕНКО**
менеджер
продуктов веб-
защиты компании
Servicepipe

Много раз слышал от CISO и CIO крупных компаний, в особенности финансовых организаций, что для защиты от DDoS-атак на уровне приложений, а также от ботовых атак на бизнес-логику сайтов нужно исключительно локальное решение (on-premise). Только оно обеспечит полный контроль над трафиком и позволит соблюсти регуляторные требования. И до 2022 года иностранные коробочные решения активно использовались в большинстве кредитных организаций с этой целью. Кое-кто из банков использует эти on-premise и сейчас, хотя вендоры заветных «железок» ещё три года назад ушли из России. При этом существует мнение, что подходящих on-premise российского производства на рынке ещё нет. Но так ли это? Предлагаю разобраться, как обстоят дела на самом деле.

Главным аргументом организации в пользу on-premise является выполнение требований PCI DSS (международный стандарт безопасной обработки платёжных данных). И сложности в связи с этим документом заключаются в передаче SSL-сертификатов. Стандарт PCI-DSS

(Payment Card Industry Data Security Standard) не запрещает напрямую передачу SSL-сертификатов¹ сторонним компаниям. Однако он устанавливает строгие требования к защите данных, включая конфиденциальность и целостность информации, связанной с обработкой платёжных карт.

Если SSL-сертификат используется для безопасной обработки данных, соответствующей требованиям PCI-DSS (например, данных карт), то передача сертификата третьей стороне должна осуществляться с учётом следующих принципов:

1. Конфиденциальность. SSL-сертификаты содержат закрытые ключи, которые должны храниться в секрете. Передача закрытого ключа третьей стороне может создать риски утечки данных, если не обеспечены должные меры безопасности.

2. Минимизация данных. PCI-DSS требует минимизировать объём передаваемых данных, особенно если они связаны с платёжными картами. Если передача SSL-сертификата не связана с обработкой данных карт, это не нарушает стандарт, но всё равно требует осторожности.

3. Контроль доступа. Если третья сторона получает доступ к SSL-сертификату, необходимо убедиться, что у неё есть соответствующие меры безопасности для защиты данных.

4. Соглашения с третьими сторонами. Если вы передаёте SSL-сертификат или связанные данные третьей стороне, необходимо заклю-

чить соглашение, которое обязывает их соблюдать требования PCI-DSS и обеспечивать защиту данных.

5. Аудит и мониторинг. Передача SSL-сертификата должна быть задокументирована, а действия третьей стороны должны контролироваться для обеспечения соответствия стандарту.

Таким образом, передача этих ключей шифрования сторонней компании не запрещена, но должна осуществляться с учётом всех требований PCI-DSS к защите данных и минимизации рисков. Что делает передачу SSL-сертификата сильно осложнённой, практически нереализуемой. Отечественные нормативные акты содержат схожие нормы со стандартом.

И есть устойчивое заблуждение на рынке, что только on-premise решения по защите от атак на уровне приложений, то есть, по сути, стоящие во внутреннем контуре под полным контролем штатных сотрудников, как раз и могут обеспечить защиту без раскрытия SSL-сертификатов. Но только ли они?

Давайте вспомним одного из крупнейших вендоров решений по защите от различных веб-угроз — американскую компанию Cloudflare. У него нет решений on-premise, однако этот вендор предоставляет защиту от DDoS-атак как на сетевом уровне (L3–L4), так и на уровне приложений (L7), а также от ботов. И облачные продукты Cloudflare имеют сертификацию согласно стандарту PCI-DSS. Это означает, что не только on-premise позволяет выполнить требования стандарта, но и сервисная модель вполне может это обеспечить. Иностранцы с облачной моделью

¹ Цифровой сертификат, который удостоверяет подлинность веб-сайта и позволяет использовать зашифрованное соединение, содержит цифровую подпись издателя, ключ и имя владельца сертификата, называемую центром сертификации (прим. ред.).

защиты и сертифицированными по стандарту решениями также ушли с рынка. Российские провайдеры же в большинстве своём могут защищать от тех же DDoS-атак без раскрытия SSL-сертификатов, но не от ботов. В большинстве, но не все.

Есть и другие причины, побуждающие отечественные банки выбирать on-premise. Одна из них – внутренние протоколы безопасности, которые писались ещё во времена присутствия на российском рынке F5, Imperva, Radware, Fortinet и других иностранцев. В то время и с той сложностью атак на прикладном уровне казалось, что стоящая в инфраструктуре «железка» – это оптимальное решение. Выбор формы поставки решения также зависит от того, удобнее ли относить затраты на приобретение решений защиты к капитальным или же к операционным расходам. И расходы на покупку on-premise часто именно CAPEX (хотя и бывают разные варианты). Ну и, наконец, для многих специалистов по информационной безопасности важен максимальный контроль за всеми процессами в ИТ и ИБ при обеспечении подхода Zero Trust в компании, что также возможно с on-premise.

В идеальной картине мира банки хотели бы иметь on-premise-решение для защиты от DDoS-атак как на сетевом уровне, так и на уровне приложений, включая защиту от ботов. С сетевыми DDoS-атаками (L3–L4) и атаками на уровне приложений (L7) всё относительно просто: на рынке есть необходимые решения от разных вендоров. Мы также активно внедряем свою on-premise-защиту в банках. А вот с защитой от атак продвинутых ботов всё иначе. Допускаю, что ещё несколько лет назад можно было реально поставить внутрь инфраструктуры иностранное коробочное решение и быть уверенным, что боты не пройдут. Сейчас же мы видим, что всё чаще в ход идут фулстек-боты, которые умеют имитировать человеческие действия, адаптироваться под профиль трафика, эмулировать действия браузера, менять IP-адреса и идентификаторы устройств. Чтобы эффективно бороться с такими веб-угрозами, антибот-решения должны



обладать мощными алгоритмами машинного обучения, анализировать десятки параметров поведения пользователей, собирать информацию о глобальных базах ботнетов. И даже если организация наймёт лучших на рынке аналитиков, которые будут обучать алгоритмы локального решения бороться с новыми ботами, то обучение это будет происходить всё равно на данных трафика лишь одной организации. Вендор же имеет возможность обучать свой продукт на основании анализа трафика сразу пула веб-ресурсов своих клиентов или даже целых отраслей и выявлять закономерности для повышения точности алгоритмов фильтрации. Такое решение будет априори эффективнее.

Означает ли это, что на российском рынке не может быть никогда готовых on-premise по защите от атак фулстек-ботов? Тоже нет – возможно в этом мире практически всё что угодно, пока не доказано обратное. Но в моей картине мира действенным эффективным средством защиты от ботовых атак не должно быть условно изолированной коробкой во внутреннем контуре. Для качественной защиты необходим гибрид. Пример

такого подхода – использование локального компонента платформы фильтрации, который выполняет детекцию и фильтрацию трафика в инфраструктуре компании, но при этом в реальном времени получает актуальные сигнатуры и модели угроз из облака вендора.

Есть ли такие решения на рынке? Есть и уже активно тестируются в российских банках. Для повышения эффективности защиты они встраиваются в эшелонированную архитектуру ИБ, состоящую из защищённых каналов связи, различных firewall, ПАК по защите от сетевых и сессионных атак, и передают данные об инцидентах в SIEM/SOC (а где-то интегрируются с антифрод-системами).

Так что можно упорно хранить заветную иностранную «железку», надеясь на полный контроль над трафиком и отсутствие атак интеллектуальных фулстек-ботов в обозримом будущем. А можно оглянуться вокруг, изучить внимательно предложения отечественных вендоров и найти свой идеальный on-premise, получающий с регулярным обновлением сигнатуры и модели угроз от вендора. И работающий эффективнее привычной коробки.

ПРОДУКТ, ПОНЯТНЫЙ И НУЖНЫЙ РЫНКУ

КАК ПРАВИЛЬНО ВЫСТРОИТЬ ПРОДАЖИ



Татьяна БЕЛЕЙ
генеральный директор
S&B Group



Елена ШЕДОВА
управляющий партнёр
S&B Group

На ИБ-конференции CIO крупной компании сказал: «Ко мне каждую неделю приходят представители разных ИТ/ИБ-стартапов и уже известных вендоров. Предлагают свои продукты, свои идеи. Но ни разу никто не пришёл и не спросил: какие боли есть у нас?»

Ушедший 2024 год показал хорошие цифры роста ИБ-рынка, но не такие большие, как многие ожидали. За последние три года появилось много новых решений как от известных вендоров, так и от новых игроков. Но практика показывает, что у крупных клиентов многие базовые направления уже закрыты, то есть решения выбраны и внедрены. Но... атаки стали сложнее, их количество значительно увеличилось, и, исходя из всего этого, стали востребованы и другие классы решений, которые позволяют усилить ИБ-контур. Поэтому прогнозируется рост продаж решений разных классов. Но почему некоторые продукты в итоге не продаются? Как правильно выстроить продажи?

Начнём с методологий продаж, которые проверены годами, компаниями и большими деньгами. Успешные директора по продажам скажут: есть методология и ей надо следовать, тогда это позволит структурировать процесс, сделать чёт-

кой воронку с критериями, квалифицировать лиды, следовать по этапам воронки и т.д. И это совершенно верно.

В B2B-ПРОДАЖАХ ВАЖНО ВЫБРАТЬ ПРАВИЛЬНУЮ МЕТОДОЛОГИЮ ПРОДАЖ

Solution Selling — методология продажи решений на зрелом рынке. Здесь нужно понять, есть ли у клиента осознанная проблема и желание её решить (Pain), установить контакт с лицом, принимающим решения, убедиться в наличии у него бюджета (Power) и оценить возможность влиять на процесс продаж (Control). Клиент должен понимать суть продукта и его ценность, увидеть выгоду от использования (Vision и Value). **Какая выгода от использования ваших продуктов?**

Insight Selling — экспертные продажи инноваций, консалтинга, upsales продуктов. Этот подход основан на глубоком понимании и исследовании потребностей клиентов. Ключевую роль играет информация о задачах заказчика, приоритетных бизнес-проектах, особенностях инфраструктуры и уже внедрённых решениях. Основываясь на этих данных, можно предлагать инновационные продукты или услуги. **Вы собираете подобную информацию о своих клиентах, чтобы предложить им что-то новое?**

MEDDIC — ведение сложных сделок в крупных комплексных проектах, где предполагается работа с большим количеством информации: метрики, цифры, обоснования. Вы должны чётко понимать, кто принимает решения, как будет происходить выбор, кто участвует в тендере, как проходит процесс закупки, как продукт влияет на ключевые бизнес-показатели клиента и т.д. **У вас есть расчёт стоимости продукта за Гб обрабатываемой информации или стоимость владения в перспективе использования 1–3 года?**

Поэтому в B2B-продажах маркетинг совсем другой. Маркетологи должны быть экспертами в технологиях и рынке, понимать задачи заказчиков. Всё больше акцент смещается в сторону продуктового маркетинга — правильное позиционирование, понятные смыслы, оценка потребностей и более аудитории, JTBD. И это не только у крупных вендоров, где такой подход уже давно стараются внедрить, но и в стартапах.

ДРУГОЙ ПОДХОД

В B2B-маркетинге нужен другой подход: он должен быть не лидоцентричным, а аккаунт-центричным. Это позволит снизить количество мусорных пресейлов и повысить эффективность продаж. Важно чётко сформулировать и понимать, кто ваш клиент, его потребности и особенности, предпочтения, в чём уникальная ценность предложения для каждого типа клиента. Сделать сегментацию клиентов на категории А, В, С, D и разработать план работы с каждой категорией, а для самых ценных клиентов внедрить АВМ-подход (Account Based Marketing). Важна совместная работа продаж и маркетинга: перекрёстные KPI,

распределение зон ответственности, чёткие требования от продаж к лидам и т.д.

То есть важно не количество заявок с сайта, а конверсия каждого конкретного обращения в сделку. Каждый клиент — это отдельный проект, который нужно прорабатывать и маркетингом, и продажами, и техническими экспертами. Совместно! Сделайте эту трансформацию внутри вашей компании, поскольку без неё продажи могут долго не превратиться в прибыль от сделки.

Если посмотреть на два первых уровня пирамиды ценностей BAIN — функциональные ценности и обязательные условия, то раньше, в начале становления рынка ИТ и ИБ, все производители предполагали, что закрыть эти два уровня — это уже успех. Рынок стал очень конкурентным, и теперь многие обращают внимание на верхние уровни пирамиды — упрощение работы, индивидуальные ценности и цели ИТ/ИБ-директоров.

СМЕНА ПАРАДИГМЫ

Сейчас происходит смена парадигмы, и в крупных корпорациях в выборе ИБ-решений активное участие принимают ИТ-директора. Особенно если это касается сетевых решений — там ЛПРами становятся и ИТшники, и сетевики, и ИБшники. Стало очевидно, что при внедрении любой системы в столь сложные инфраструктуры, какими они сейчас являются, надо договариваться. Решать вместе! Всё больше применяется риск-ориентированный подход, на выбор влияют особенности реализуемых бизнес-проектов, производительность, отказоустойчивость и совместимость уже внедрённых ИТ/ИБ-продуктов. Ключевые приоритеты — упрощение процессов и инструментов, повышение эффективности управления командами и демонстрация ценности ИТ и ИБ для бизнеса. Так, в KPI у CISO теперь не только защита данных и инфраструктуры, но и бизнес-показатели, в частности, снижение финансовых потерь от кибератак.

Поэтому продукты надо рассматривать с разных сторон — не только раз- вивать функциональные возможно-

Условия в 2025 году сильно изменились, и рынок уже это почувствовал как со стороны заказчиков, так и со стороны вендоров. Поэтому сейчас главное — связать R&D, маркетинг и продажи с ключевыми задачами и болями клиентов

сти, но и добавлять другие ценности для всех ЛПР. Пирамида BAIN очень хорошо сочетается с CJM (Customer Journey Map). Ведь CJM как раз и есть путь, как клиент выбирает продукт или решение. И если в CJM-исследовании посмотреть на все этапы пирамиды, то может получиться отличный продукт, востребованный рынком и заказчиками. **Какие ценности включены в ваш road-map?**

CustDev и CJM помогут выявить причины поиска и выбора ИБ/ИТ-решений, а самое главное, узнать, почему не покупают ваш продукт, и определить основной драйвер в продажах.

ПРИЧИНЫ ПОИСКА И ВЫБОРА РЕШЕНИЙ — КАКИЕ ОНИ?

В первую очередь — высокие требования к производительности в связи с появлением критических бизнес-сервисов, ростом использования услуг провайдеров, облачных инфраструктур, для которых требуется повышенная пропускная способность и надёжность. Важны правила обмена трафиком и скорость обработки и анализа передаваемой информации. Критичными являются задержки, которые продукт вносит в работу сети и бизнес-сервисов, особенно это важно в межЦОДовом взаимодействии. Важны ограничения по эксплуатации и правилам пользования, в частности, процесс перехода на новую версию, перенесутся ли настройки и наработки, какое необходимо количество перезагрузок в неделю/месяц/год, за какое время решение «поднимается» после сбоя, атаки или обновления. В приоритете — сценарии использования и совместимость с отечественными

платформами (виртуализации, контейнеризации и т.д.), уровень сертификации продуктов и, конечно, важна стоимость решения.

Условия в 2025 году сильно изменились, и рынок уже это почувствовал как со стороны заказчиков, так и со стороны вендоров. Поэтому сейчас главное — связать R&D, маркетинг и продажи с ключевыми задачами и болями клиентов.

«СЛЕПЫЕ ЗОНЫ»

Путь привлечения клиента в B2B-продажах не такой сложный. Основной приток клиентов: сарафанное радио, прямые продажи и активный пресейл, собственные связи, мероприятия, партнёры. Но есть «слепые зоны», которым стоит уделить должное внимание. Вот несколько из них:

- ♦ нет информационного поля вокруг компании и продукта, клиенты не знают о решении, узнают случайным образом;
 - ♦ нет информации о развитии, а road-map сейчас важен не только для решений от стартапов, но и для всех вендоров;
 - ♦ нет обоснования и аргументации для покупки;
 - ♦ нет требований от регуляторов, продукта нет в Росреестре...
- Этот список можно продолжить. **Что именно мешает вашим продажам и что на самом деле клиенты думают про ваш продукт?** Давайте их спросим?

S&Bi Group — помогаем построить путь от ИТ-продукта к клиенту. Предлагаем пройти этот путь вместе!

«ЦИФРОВАЯ УСТОЙЧИВОСТЬ ПРОМЫШЛЕННЫХ СИСТЕМ — 2025»

ДОГОНЯТЬ ВНЕШНИЙ РЫНОК ИЛИ СОСРЕДОТОЧИТЬСЯ НА СВОЁМ?

Усам ОЗДЕМИРОВ
корреспондент BIS Journal

В Москве, в Центре событий РБК, прошла конференция, посвящённая цифровой устойчивости промышленных систем. В ней приняли участие представители министерств и ведомств, большого числа компаний-заказчиков и вендоров из разных регионов страны, вносящих свой вклад в цифровую трансформацию и обеспечение информационной безопасности на всех этапах деятельности.

РАЗМИНКА

Перед началом пленарной сессии выступили научный редактор

BIS Journal Сергей Пазизин и заместитель генерального директора компании «ИнфоТеКс» Дмитрий Гусев, проведя содержательный превью-диалог на тему киберустойчивости и различных её аспектов.

Информационная безопасность выражается в способности системы противостоять угрозам, реагировать на них и восстанавливаться после нанесённого ущерба. При этом цифровая устойчивость фокусируется на способности организации адаптироваться, реагировать и восстанавливаться после кибератак или разрушительных инцидентов, сохраняя при этом непрерывность бизнеса. Если говорить о промышленных системах, то тут есть своя специфика, заметил Сергей Пазизин. Они насыщены различными устройствами, датчиками, приборами, механизмами. Там при-

сутствует промышленный интернет вещей. И если брать классическую триаду ИБ — конфиденциальность, целостность и доступность, то последняя категория наиболее важна при автоматизации промышленной системы.

Дмитрий Гусев посетовал, что отдельные представители предприятий-заказчиков просят выстроить для них информационную безопасность «по-быстрому, чтобы удовлетворить требованиям 250-го указа и далее по списку требованиям ФСТЭК России и ФСБ». В промышленных системах присутствуют специализированные протоколы и оборудование. Уже сейчас на уровне нормативных требований появляются отдельные пункты в отношении промышленных межсетевых экранов.

Надо отметить, что мы одновременно находимся в нескольких параллельных процессах, констатировал Гусев. В частности, это касается импортозамещения, вместе с которым возникает очень много задач. Надо с ходу заместить промышленное оборудование, при этом обеспечить требования информационной безопасности. Как всё это сделать быстро и надёжно, учитывая временные и финансовые ограничения? Здесь возникает много вопросов, которые требуют комплексного подхода. Дискуссии на конференции должны помочь специалистам в области АСУ повысить своё понимание задач цифровой устойчивости. Советы приглашённых экспертов позволят участникам сформировать своё ви-



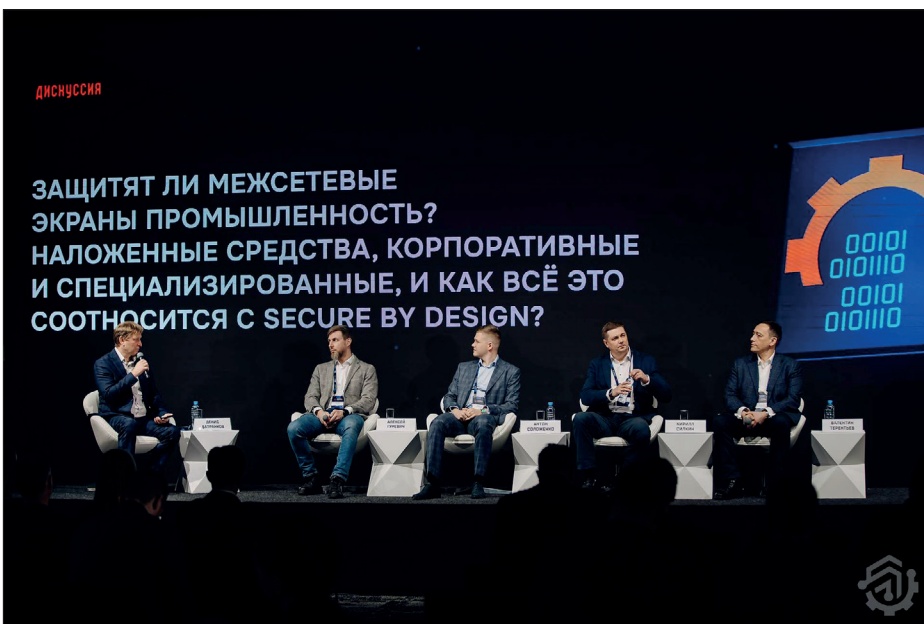
дение того, как двигаться в области развития современных цифровых систем управления производством с учётом требований информационной безопасности, чтобы завтра не сожалеть о возможных негативных последствиях, заключил Дмитрий Гусев.

ПЛЕНАРКА

Выступивший в ходе пленарной сессии заместитель министра промышленности и торговли РФ Василий Шпак акцентировал внимание аудитории на нормативном регулировании, которое ставит в определённые рамки предприятия, являющиеся субъектами критической информационной инфраструктуры. С 2022 года по декабрь 2024-го специалистами центра информационной безопасности министерства промониторено 2700 субъектов КИИ. Они посещали не только предприятия со значимыми объектами, но и предприятия, владеющие объектами КИИ, которым категория значимости не была присвоена. В результате стало понятно, что очень много организаций не спешат с заявлениями о категорировании таких объектов.

По общему результату только 20 % субъектов КИИ выполнили все установленные требования по её защите. И это вызывает удивление, учитывая законодательные требования в области ИБ и динамику роста количества компьютерных атак. Как отметил Шпак, от выполнения действующих требований (причём, как правило, это достаточно простые меры) зависит зачастую функционирование всего производства, так как существуют риски возникновения в том числе и техногенных последствий, остановки этих производств.

Между тем должно быть всем ясно, что нам необходимо и дальше двигаться в сторону импортонезависимости и технологического суверенитета. Это вопрос нашего выживания как государства. По словам Василия Шпака, промышленность играет большую роль в укреплении курса страны на обретение технологической, экономической и политической независимости. Он призвал представителей всех компаний и промышленных предприятий к совместной



работе в формате открытых архитектур, чтобы была взаимозаменяемость всех решений, в формулировании общих технических требований к тем решениям, которые позволили бы улучшить их конкурентоспособность.

ДИСКУССИЯ

В ходе дискуссии, посвящённой использованию межсетевых экранов в промышленности и принципу защиты АСУ ТП secure by design, в роли ведущего выступил директор по продуктам информационной безопасности компании «ИКС

Холдинг» Денис Батранков. Он попросил участников высказаться по таким проблемам, как отсутствие совместимости наложенных средств защиты с системами промышленной автоматизации, несогласованность между ИБ, службой эксплуатации и руководством бизнеса, а также соответствие требованиям безопасности и стандартам.

Информационная безопасность, которая была несколько лет назад, и та, что сейчас, — это две большие разницы, заметил Кирилл Силкин, первый заместитель генерального директора компании «Атомик Софт». С момента



требований. Но есть также вендоры, которые отказываются дорабатывать свои технические решения по тем или иным причинам. Это может быть отсутствие инвестиций в R&D или кадровый дефицит. Потребность бизнеса в новых кадрах ИБ только растёт. На этой «поляне» работают и заказчики, и представители вендора, а также интеграторы, тогда как рынок не успевает выпустить такое количество кадров.

В МЕЖДУНАРОДНОМ КОНТЕКСТЕ

Бизнес сегодня больше озабочен решением проблем настоящего момента, а не инвестициями в ИБ. Получается, что те инвестиции, которые делают вендоры в развитие своих продуктов, не возвращаются должным образом. По словам Гуревича, с 2014 года нашу экспертизу на уровне ИБ начали потихоньку отрезать от мировой. Все эти иностранные решения — Cisco и Check Point... — они ушли. За эти десять лет уровень качества экспертизы и возможностей средств межсетевого экранирования у них вырос. Мы не понимаем, куда технологии в мире развиваются. Соответственно, вендоры смотрят на рынок изнутри и не понимают, как догонять внешний рынок, заключил эксперт.

С предыдущим оратором взялся поспорить директор по развитию бизнеса, направление промышленной и корпоративной кибербезопасности ГК InfoWatch Антон Соложенко. Он напомнил о наших технологических возможностях. Если взять условный «Эльбрус», то разогнать на нём межсетевой экран на 100 гигабит невозможно. Сегодня народ уже понял, что не будет иностранных решений — пора брать российские межсетевые экраны и подгонять их под себя. Да и вендоры промышленных и межсетевых экранов, присутствующие на рынке, тоже это осознали. Они пришли к выводу, что есть определённый набор функционалов, который должен выполнять каждый. Наши вендоры стремятся к тому, чтобы выполнить именно требования заказчика и сделать это максимально корректно и надёжно с точки зрения работы системы, резюмировал спикер.

ужесточения требований к построению безопасности компании приходится возвращать у себя экспертизу и подстраиваться под обновлённые требования как заказчика, так и законодательства. Возникают необходимость в кадрах и дополнительная функциональность — вокруг двух этих моментов постоянно приходится лавировать. По мнению Силкина, рынку не хватает глубоких возможностей для простой удобной интеграции.

«Надо не драться, не толкаться локтями, а работать параллельно в направлении своих компетенций, — обратился к присутствующим Кирилл Силкин. —

Максимальных компетенций. Это позволит как раз вычленив время и ресурсы на то развитие, которое мы себе предполагаем. Нам не придётся заниматься несвойственными нам вещами. Будем развивать свои продукты».

К обсуждению поднятой темы подключился также заместитель начальника управления развития и контроля ИБ компании «Сибинтек» Алексей Гуревич. Как показали некоторые исследования на рынке информационной безопасности в части межсетевых экранов, у нас есть вендоры, которые готовы выполнять набор функционально-технических

22–24 мая
Москва, «Лужники»



**PHDAYS
FEST**
от positive technologies

Международный киберфестиваль Positive Hack Days

Хотите стать частью крупнейшего технологического события страны в 2025 году? Присоединяйтесь к международному киберфестивалю Positive Hack Days. Это масштабное мероприятие, которое объединит представителей министерств и ведомств, лидеров высокотехнологичных индустрий, экспертов в области ИТ и ИБ, а также всех тех, кто неравнодушен к технологиям и хочет классно провести время.

PHDays — это

Открытый диалог государства, бизнеса и населения на одной площадке.

Самая масштабная кибербитва России — Standoff 15.

Сотни выступлений спикеров, воркшопы и интерактивы для всех желающих.

Концерт под открытым небом со звездными хедлайнерами.



Больше подробностей —
на официальном сайте фестиваля

ИСПЫТАНИЯ СТАТИЧЕСКИХ АНАЛИЗАТОРОВ



Дмитрий ПОНОМАРЕВ

заместитель генерального директора — директор департамента внедрения и развития практик РБПО ООО НТЦ «Фобос-НТ», сотрудник ИСП РАН, преподаватель МГТУ им. Н.Э.Баумана

Испытания открытых и коммерческих статических анализаторов исходных кодов компилируемых и динамических языков программирования под патронажем ФСТЭК России [1] — это уникальное для отечественного рынка событие, свидетельствующее как о растущем уровне зрелости рынка и требований [2], так и о востребованности технологии статического анализа для организации процессов разработки безопасного и качественного ПО (далее — РБПО).

Особый интерес к испытаниям вызван формулировкой их целей (см. ниже) и антицелей. Во главу угла ставятся именно технологические возможности «движков» инструментов, определяемые и регламентируемые ГОСТ Р 71207-2024 [3].

Разумеется, конечного пользователя при выборе инструмента могут интересовать и иные критерии — наличие интеграционного функционала, наличие детекторов на актуальные «мисконфиги» (под этим термином понимается класс уязвимостей, связанных с неправильной настройкой ПО, напри-

мер, установленные в настройках «по умолчанию» слабые режимы шифрования трафика веб-сервера), и даже наличие понятной маркетинговой стратегии разработчика инструмента. Естественно и желание увидеть некую совокупную метрику, сочетающую в себе «тёплое с мягким умноженное на цветочные предпочтения» — аналог точки в знаменитом «Гартнеровском квадрате».

Тем не менее ФСТЭК России сознательно фокусируется именно на испытаниях возможностей «движков» инструментов. Поиск различных актуальных «мисконфигов», в том числе снижающих защищенность системы, бесспорно одна из важных задач при обеспечении реальной безопасности. Качественно реализованный функционал интеграции с иными корпоративными сервисами и вспомогательным инструментами — такими как службы домена, корреляторы ошибок и багтрекеры — это практически безальтернативное свойство любого анализатора, планирующегося к применению в крупной организации. Наличие понятных обучающих и маркетинговых материалов, рав-

но как и собственной «школы» внедренцев и последователей, разумеется, также способствует комфорту конечного пользователя. Однако реализация всего вышеуказанного, как правило, представляет собой всё-таки «задачи», а не «проблемы». Число инженеров и иных специалистов, умеющих решать данные задачи, в России и Море бесспорно многократно выше, чем число узкопрофильных специалистов, умеющих создавать, развивать и поддерживать «сердца» инструментов статического анализа.

Именно поэтому в фокусе испытаний именно «движки» инструментов — как отечественных, так и подмножества «открытых» — это должно подчеркнуть важность создания и развития соответствующих отечественных «школ», способных в том числе составлять конкуренцию на мировом рынке. А одной из важнейших целей испытаний является выработка методики оценки возможностей движков, которая в дальнейшем может быть использована не только для оценки возможностей инструментов, но и в качестве актуализируемого обобщенного Технического Задания, на которое смогут ориентироваться начинающие коллективы, желающие попробовать свои силы в создании и развитии статических анализаторов.

[1] <https://ib-bank.ru/bisjournal/news/21667>

[2] https://ib-bank.ru/rbpo_pubs

[3] <https://clck.ru/3HsNTZ>

КРАТКАЯ
ХАРАКТЕРИСТИКА
ИСПЫТАНИЙ

Цели испытаний

- ♦ оценка технологических возможностей отечественных и открытых статических анализаторов исходного кода
- ♦ формирование публичных методик оценки и критериев применимости анализаторов в различных видах исследований и испытаний

Критерии оценки

- ♦ соответствие требованиям ГОСТ Р 71207–2024 в части:

- полноты обнаружения критичных дефектов
- избыточности ложных обнаружений дефектов
- поддерживаемых методов анализа
- ресурсозатратности анализа
- ♦ соответствие дополнительным критериям, вырабатываемым жюри

Предметная область испытаний

- ♦ компилируемые языки программирования (Си / Си++ / Java / Go / C#)
- ♦ интерпретируемые языки программирования с динамической типизацией (Python / JavaScript)

Не войдут в критерии оценки

- ♦ наличие сертификатов тех или иных регуляторов или добровольных сертификаций
- ♦ интеграционный функционал и возможности инструментов по встраиванию, взаимодействию с иными видами анализаторов
- ♦ факты использования технологий искусственного интеллекта «в движении», либо «для приоритизации»
- ♦ функционал, требующий запуска ПО и его анализа в динамическом режиме
- ♦ активность маркетологов и рекламщиков; число статей и выступлений на коммерческих конференциях.

ПЛАН ИСПЫТАНИЙ

№	Шаг	Дата начала	Дата окончания	Ответственные
1	Анонс испытаний на Открытой конференции ИСП РАН	11.12.24	12.12.24	ФСТЭК России
2	Формирование жюри и установочная встреча	10.01.25	10.02.25	ФСТЭК России
3	Повторный анонс на ТБ Форум	12.02.25	13.02.25	ФСТЭК России
4	Подбор компонентов с открытым исходным кодом и разработка комплекта тестов для основного этапа испытаний	10.04.25	01.07.25	ФСТЭК России, жюри
5	Разработка комплекта тестов «Домашнее задание»	01.01.25	25.03.25	ИСП РАН, разработчики СА, жюри
6	Согласование комплекта тестов «Домашнее задание»	25.03.25	10.04.25	ФСТЭК России, жюри
7	Проведение этапа «Домашнее задание»	10.04.25	15.05.25	разработчики СА
8	Подготовка декларативных отчётов по результатам этапа «Домашнее задание»	15.05.25	25.05.25	разработчики СА
9	Подготовка и публикация пресс релиза по результатам этапа «Домашнее задание»	25.05.25	01.06.25	ФСТЭК России, Медиа Группа «Авангард»
10	Подготовка инфраструктуры основного этапа испытаний	01.03.25	01.07.25	МГТУ им. Н. Э. Баумана, разработчики СА, жюри
11	Выполнение анализа в подготовленной инфраструктуре в ходе основного этапа испытаний	01.07.25	08.07.25	МГТУ им. Н. Э. Баумана, жюри
12	Разметка результатов выполненного анализа	08.07.25	01.11.25	жюри, разработчики СА, дополнительно привлечённые организации-эксперты
13	Кроссверификация результатов выполненного анализа	08.07.25	01.11.25	жюри, дополнительно привлечённые организации-эксперты
14	Подготовка технического отчета по результатам основного этапа испытаний	01.10.25	01.11.25	жюри
15	Подготовка итогового отчета о результатах испытаний	01.11.25	01.12.25	жюри, ФСТЭК России
16	Выступление ФСТЭК России, посвященное результатам испытаний		до 15.12.25, открытая конференция ИСП РАН	ФСТЭК России

КРИТЕРИИ ОЦЕНКИ НА ЭТАПЕ «ДОМАШНЕЕ ЗАДАНИЕ»

Комплект тестов этапа «Домашнее задание» доступен всем участникам испытаний, а оценка результатов будет носить декларативный характер. Каждая организация-участник, получив комплект тестов и, проведя испытания самостоятельно, также самостоятельно заполнит типовую

анкету зафиксировав там результаты, полученные в ходе анализа комплекта тестов. Данные результаты будут переданы жюри и организаторам испытаний без какой-либо дополнительной верификации — цель данного этапа это не только верхнеуровневая оценка возможностей инструментов, но и выравнивание позиций и восприятия коллективами участников и жюри.

В критерии оценки этапа «Домашнее задание» войдут количественные показатели обнаружения заложенных в атомарные тесты дефектов кода, а также некоторые качественные характеристики инструментов, такие как маппинг детекторов на «пункты» ГОСТ 71207–2024, наличие документации по всем типам ошибок и выдача результатов разметки в открытых форматах.

КОММЕНТАРИИ ОТ ОРГАНИЗАЦИЙ- УЧАСТНИКОВ ИСПЫТАНИЙ

ИСП РАН (участник испытаний)

Испытания статанализаторов — важная инициатива регулятора, которая решает сразу несколько задач. Во-первых, раскрывает сильные и слабые стороны анализаторов на едином наборе тестов как для пользователей-вендоров, так и для разработчиков самих анализаторов. Во-вторых, «обкатывает» положения недавно принятого ГОСТ 71207 в отношении к уровню технологий анализа и классам критических ошибок на ряде популярных языков программирования. Можно ожидать, что по итогам испытаний будут, кроме прочего, сформированы предложения по развитию требований ГОСТ. Наконец, методика испытаний в дальнейшем сможет стать основой для оценки и других инструментов, в частности, динамических анализаторов. Также важно, что все ведущие российские разработчики анализаторов откликнулись на предложение ФСТЭК. Совместно с коллегами приятно работать и обмениваться опытом, и мы уверены, что результаты испытаний будут интересны и полезны для всего сообщества.

ПВС (участник испытаний)

Благодаря инициативе ФСТЭК у разработчиков ПО и сертификационных лабораторий появится единая

методика оценки инструментов при их выборе.

В ГОСТ Р 71207–2024 (раздел 7 и 8) перечислены требования, предъявляемые к инструментам СА. Однако пользователям затруднительно самостоятельно проверить, насколько им соответствует анализатор. Нужен большой набор синтетических (малых) и реальных (больших) тестов, проверяющих, что выявляются все типы критических ошибок (п. 6.7). Более того, тесты должны проверить, что детекторы СА реализованы на должном уровне и обеспечивают глубокий анализ кода. Имеется в виду, что тесты следует делать разносторонними и иногда сложными, чтобы убедиться, что в инструменте реализованы методы анализа, перечисленные в п. 7.4., например анализ потока данных.

Всё это возможно, но ресурсозатратно. Дополнительная сложность, что пользователи инструментов просто не обладают такой же экспертизой, какая есть у команд, разрабатывающих СА. Непонятно, как убедиться, что разработанные тесты действительно проверяют все важные аспекты.

Поэтому очень важно, что ФСТЭК привлёк к созданию методики сами команды, разрабатывающие инструменты анализа. Благодаря совместным усилиям можно подготовить хорошие наборы тестов и провести их кросс-верификацию.

Ценность разрабатываемой методики в том, что затем можно

взять любой инструмент и достаточно быстро, надёжно и единообразно оценить, насколько он соответствует требованиям ГОСТ Р 71207–2024.

Существование публичной методики испытаний будет стимулировать вендоров адаптировать инструменты к особенностям стандарта, что в итоге поможет пользователям. Например, для испытаний требуется готовый набор детекторов для выявления критических ошибок. Сложно внедрять СА в процесс РБПО, если такого набора нет и пользователям самим предстоит его составлять, рискуя ошибиться.

Базальт СПО (жюри и участник испытаний)

В ходе испытаний будут выработаны материалы и способы сравнения статических анализаторов, проявятся их преимущества и ограничения. Это позволит разработчикам, в том числе в «Базальт СПО», обоснованно выбирать инструменты в зависимости от конкретных задач.

«Базальт СПО» предложила внести в программу испытаний свободные статические анализаторы Clang Static Analyzer и CppCheck, нагрузку по сопровождению которых полностью возьмут на себя специалисты компании.

Мы также готовы способствовать открытой публикации тестов, материалов и техники тестирования не только для участников испытаний, но и для всего мирового сообщества.

SVACE



Андрей БЕЛЕВАНЦЕВ

руководитель направления анализа и оптимизации программ ИСП РАН, доктор физико-математических наук, профессор РАН

Svace – семейство статических анализаторов, разрабатываемых в ИСП РАН с 2003 года. Мы гордимся, что:

- ◆ прошли путь от фундаментальных исследований по анализу до внедрений в крупнейшие российские и зарубежные компании;

- ◆ в рамках совместной лаборатории с компанией Samsung показали, как инновационные технологии могут быть «заточены» под специфику конкретных заказчиков;

- ◆ добились результатов, которые помогли определить мировой уровень развития анализа, на который ориентируются у нас и за рубежом при создании регуляtorики;

- ◆ внесли определяющий вклад в формирование научной специальности «Кибербезопасность» в России.

Svace сегодня – это:

- ◆ 10 языков, более 70 классов критических ошибок и более 1300 детекторов

- ◆ передовой уровень технологий – анализ всей программы целиком (межпроцедурность), отдельный анализ путей выполнения (символьное выполнение), анализ чувствительных данных, анализ статистики, точное построение графа вызовов (де-виртуализация). И это далеко не все!

- ◆ работа с результатами анализа через графический интерфейс Svacer, в котором можно изучить код и разметить предупреждения небольшой программы, а можно вести десятки проектов различных команд с регулярным проведением анализа, переносом разметки между версиями, пользовательскими фильтрами и статистикой. Именно Svacer поддерживает работу Центра исследо-

ваний безопасности системного ПО, объединяющего десятки компаний

- ◆ программный интерфейс для создания пользовательских детекторов-плагинов, который в простой декларативной манере дает доступ к части анализов из основного «движка». В итоге создание детектора для поиска несложных, специфичных для проекта ошибок сравнимо по трудоемкости с простыми шаблонами запросов для анализаторов уровня синтаксического дерева, но при этом дает значительно более точный результат. Пользователи также могут делиться своими детекторами друг с другом на площадке Svace, получать консультацию разработчиков и предоставлять свои плагины в качестве образцов (подробнее в нашем блоге)

- ◆ AI-ассистент для разметки предупреждений анализатора, позволяющий оценивать вероятность истинности предупреждения на основе машинного обучения, управляемого историей разметки (для языков C, C++, C#, Java). Базовыми признаками для оценки служат метрики исходного кода программы, которые дополнительно собираются в ходе анализа. Наилучшая точность предсказания достигается при учете данных прошлой пользовательской разметки. Если результаты анализа загружаются на сервер с такими данными, то дообучение модели для предсказания происходит автоматически (подробнее в нашем блоге).

Svace активно развивается: мы внедряем результаты научных исследований и реализуем необходимый функционал. Новые версии Svace выходят ежегодно, а обновления

текущей стабильной версии выпускаются каждые два-три месяца. Среди примеров изменений двух последних лет:

- ◆ поддержка последних версий языков (C++20, Java 21, Go 1.24, Kotlin 2.0, C# 12)

- ◆ инфраструктура универсального синтаксического дерева (UAST), которая унифицирует простые детекторы между языками и позволяет в ускоренном темпе добавлять новые. В 2024 году на ее основе добавлен язык JavaScript

- ◆ улучшение анализа чувствительных данных и расширение возможностей по пользовательским спецификациям источников и стоков

- ◆ работа с предупреждениями через комментарии в коде

- ◆ роли пользователей, гибкие фильтры предупреждений, статистика разметки, глобальный полнотекстовый поиск в интерфейсе Svacer

Svace – результат многолетних исследований научной школы системного программирования ИСП РАН, реализованных в инновационном продукте благодаря обратным связям от российской и зарубежной индустрии. Svace внедрен более чем в 200 компаниях, среди которых – ключевые игроки в области ИТ и кибербезопасности, крупнейшие финансовые организации (в том числе ведущие банки России), а также предприятия телекоммуникационного сектора. Вместе мы обеспечиваем технологическую независимость российского бизнеса и всей страны.

Будем рады видеть вас в числе наших заказчиков!

**Инструменты
анализа
ИСП РАН**



Блог Svace



СТАТИЧЕСКИЕ АНАЛИЗАТОРЫ В КОММЕРЧЕСКОЙ РАЗРАБОТКЕ

ОДНА ГОЛОВА ХОРОШО, А НЕСКОЛЬКО — ЛУЧШЕ



Дмитрий Шмойлов
Head of Software Security,
Kaspersky

Любая компания, которая начинает внедрять процессы безопасной разработки, в первую очередь задумывается об инструменте статического анализа. С него, как правило, начинается «пробный период» по внедрению практик безопасной разработки. Статические анализаторы являются пилотом и первой ласточкой в коммуникации зарождающейся роли Application Security (подразделения, ответственного за развитие безопасной разработки) с командой разработки ПО.

Это вполне объяснимо, так как данный инструмент ближе программисту. Команды разработки так или иначе всегда использовали инструментарий статического анализа (начиная с IDE плагинов и простых линтеров) самостоятельно, без запроса со стороны Application Security. Уже позже развитие отношений между Application Security и разработкой перейдёт на новый уровень доверия — использование динамических анализаторов, проведение обучений по тематике безопасной разработки, SCA и т.д., а некоторые даже попробуют фаззинг... Но оставим их и вернёмся к «статике».

Статические анализаторы существуют давно и в большом разнообразии представлены на рынке, как в open-source, так и среди коммерческих решений. При выборе подходящего решения компаниям приходит-

ся ответить на множество вопросов: что лучше, что удобнее, что эффективнее? И самое главное — как это применить к нашим реалиям, процессам, процедурам сборки (пайплайнам)?

Поразмыслив ещё, они понимают: «Не мы первые, кто задаётся таким вопросом». А что у «коллег по цеху»?

Думаем, что регулятор инициировал сравнение инструментов статического анализа (SAST), в том числе с намерением ответить и на этот вопрос.

Мы в «Лаборатории Касперского» работаем с SAST каждый день, на большом объёме кода, знаем и понимаем данную практику, ежедневно видим пользу от её применения. В нашей практике встречались случаи, когда разные инструменты находили одни и те же баги, а также когда ни один из используемых SAST не находил ошибку, которая должна обнаруживаться подобными решениями.

Использование статических анализаторов в ходе разработки наших продуктов — обязательное требование для всех коммерческих проектов, это естественная процедура, как помыть руки перед едой.

В ряде критичных проектов используют несколько анализаторов последовательно. Часто эксперты пишут свои дополнительные правила для инструментов, чтобы расширить их детектирующие возможности, адаптируя их под специфику нашего кода.

Там, где это возможно, инструменты работают в блокирующем режиме: любое срабатывание останавливает заливку кода в мастер-ветку, пока срабатывание не будет обработано.

Да, специфика работы SAST подразумевает, что предупреждения инструмента содержат немало ложноположительных срабатываний, это неизбежно. Наши эксперты хорошо знают путь к группам поддержки отечественных SAST-инструментов, сообщая им о том, как можно оптимизировать их работу для снижения ложноположительных срабатываний. Тем полезнее будет совместная работа плечом к плечу с разработчиками SAST.

Вопрос необходимости сравнения SAST-инструментов мы поднимали в процессе согласования ГОСТ по статическому анализу.

Мы всецело приветствуем инициативу и надеемся на выработку полезных критериев по оценке инструментов. Эти критерии дадут компаниям-новичкам в данной области больше информации для выбора, облегчат им «первый старт», а зрелые компании, вероятно, найдут ответы на давно волнующие их вопросы.

В любом случае подобные коллаборации ведущих разработчиков ПО приносят пользу и ускоряют развитие всей индустрии разработки.

Пожелаем нам всем удачи и будем с нетерпением ждать результатов!

ОБ АВТОРЕ

Дмитрий Шмойлов. Более 23 лет опыта в IT, из них 18 — в сфере ИБ (от специалиста до CISO) и разработки (архитектура ИБ, Application Security, SSDLC, DevSecOps). Последние 7 лет руководит AppSec-подразделением в «Лаборатории Касперского», где отвечает за совершенствование процессов безопасной разработки. Сфера профессиональных интересов: безопасная разработка, безопасная архитектура, DevSecOps, пентест, Bugbounty, data privacy (в том числе GDPR).

АНАЛИЗАТОР КОДА ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ АК-ВС 3



КОМПЛЕКСНОЕ РЕШЕНИЕ ДЛЯ ОБЕСПЕЧЕНИЯ
БЕЗОПАСНОСТИ КОДА В СОВРЕМЕННЫХ РАЗРАБОТКАХ



**Виталий
ВАРЕНИЦА**
заместитель
генерального
директора
АО «НПО
«Эшелон»

В эпоху стремительного роста киберугроз защита программного обеспечения становится приоритетной задачей. Компании обязаны соответствовать требованиям регуляторов и обеспечивать безопасность своих решений. Регулярные проверки кода являются ключевым аспектом обеспечения безопасности программного обеспечения. Применение инструментов тестирования не только способствует улучшению качества про-

граммного обеспечения, но и обеспечивает соответствие актуальным требованиям регуляторов в области разработки безопасного ПО.

ВВЕДЕНИЕ

АК-ВС 3 представляет собой инструмент, предназначенный для автоматизации процесса проведения испытаний при сертификации в соответствии с требованиями различных регуляторов, а также для выполнения периодических проверок в рамках разработки безопасного программного обеспечения.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

◆ Все виды анализа в одном продукте: возможность проведения статического анализа кода (SAST), динамического анализа кода (DAST), полносистемного динамического анализа, фаззинг-тестирования (FAST)

в одном продукте в соответствии с требованиями разных регуляторов. В рамках одной лицензии разработчик получает продукт, который комплексно способен проводить сразу несколько независимых видов тестирования.

◆ Интеграция с CI/CD: АК-ВС 3 легко внедряется в DevSecOps-процессы благодаря консольному клиенту, который позволяет запускать анализ автоматически при каждом коммите. Это помогает обнаруживать уязвимости ещё на этапе разработки, а также автоматизировать проверку кода.

◆ Работа в собственной среде разработки: встроенная IDE «Эшелониум» на базе Visual Studio Code обеспечивает удобство работы с кодом и анализом результатов, поддерживает патчи, плагины и интеграцию с системами разработки, что исключает необходимость в дополнительных редакторах (рис. 1).

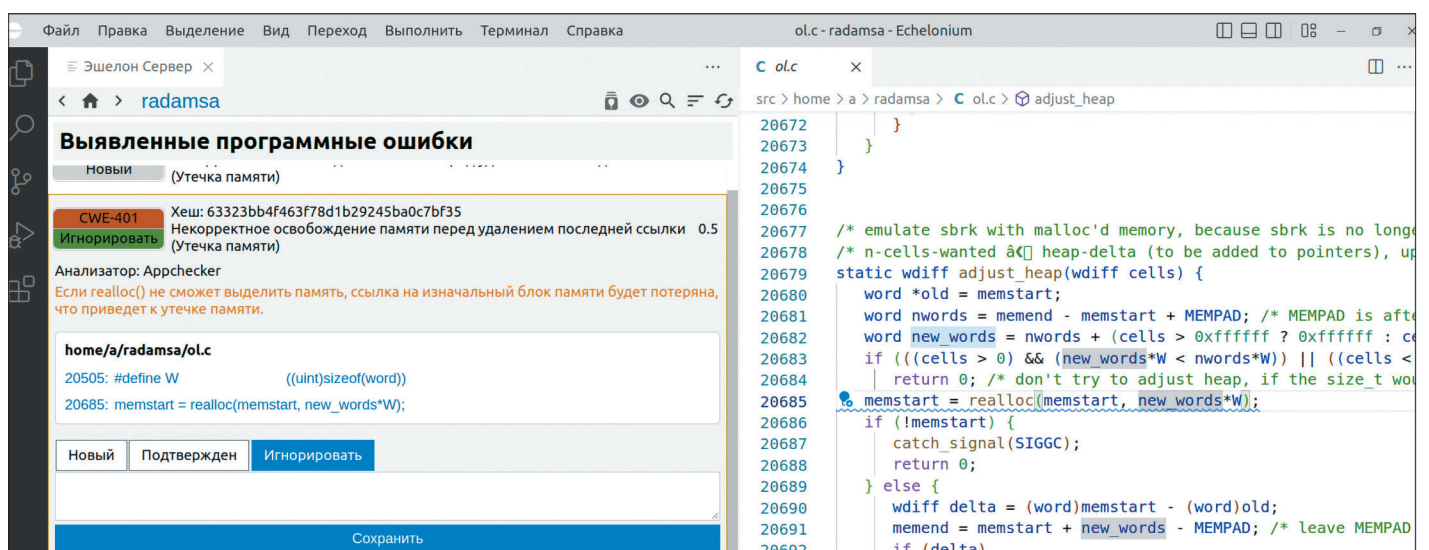
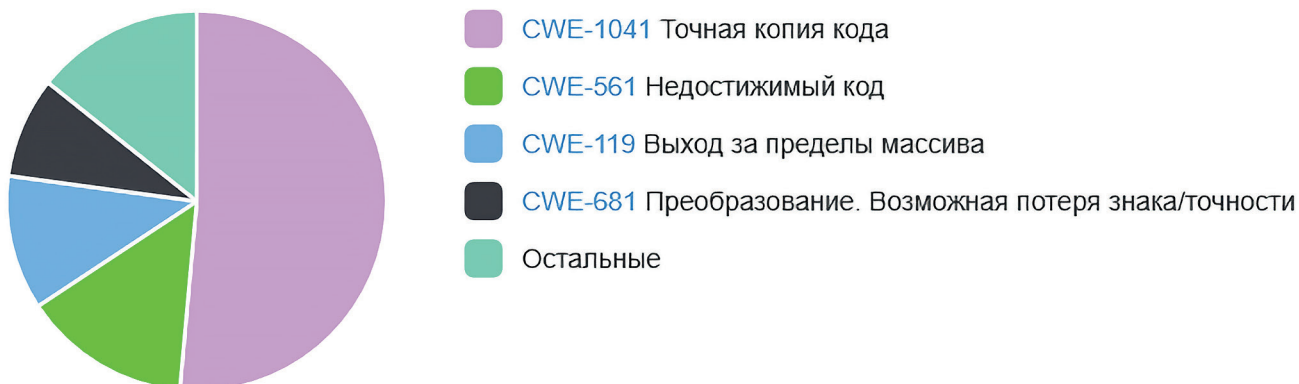


Рисунок 1. Работа в IDE «Эшелониум»

Топ дефектов по типам (CWE)

[Посмотреть все →](#)

Распределение дефектов по категориям

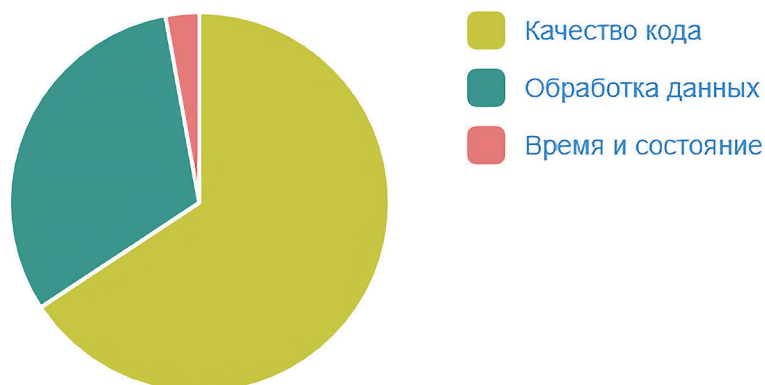


Рисунок 2. Классификация выявленных дефектов

♦ **Соответствия требованиям регулятора:** АК-ВС 3 выполняет требования:

- ФСТЭК России в части:
 - «Статический анализ объекта оценки (САО)»;
 - «Фаззинг-тестирование объекта оценки (ДАО.2)»;
 - «Системное тестирование объекта оценки (ДАО.3)».
- Министерства обороны Российской Федерации в соответствии с руководящим документом «Защита от несанкционированного доступа к информации Часть 1. Программное

обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей в части:

- п. 3 «Статический анализ исходных текстов программ»;
- п. 4 «Динамический анализ исходных текстов программ».
- Требования по разработке безопасного ПО в соответствии с ГОСТ Р 56939–2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» в части:

- п. 5.3.3.4 «Статический анализ исходного кода программы»;
- п. 5.4.3.3 «Динамический анализ исходного кода программы»;
- п. 5.4.3.4 «Фаззинг-тестирование программы».
- Требования по разработке безопасного ПО в соответствии с ГОСТ Р 56939–2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» в части:
 - п. 5.10 «Статический анализ исходного кода»;
 - п. 5.11 «Динамический анализ исходного кода».

♦ **Проведение различных видов статического анализа исходного кода.** Поддерживается статический анализ исходного кода на уровне:

- сигнатурного анализа;
- анализа потоков;
- межпроцедурного контекстно-чувствительного анализа;
- анализа, чувствительного к путям выполнения.

♦ **Описание дефектов в соответствии с международным стандартом CWE:** представляет собой не просто получение сигнатуры или фиксирование срабатывания, а включает в себя указания соответствующей категории дефекта в системе CWE (рис. 2).

♦ **Построение различных отчётов для статического анализа исходного кода:**

- данные о базовых блоках, функциональных и информационных объектах;
- отчёт по выявленным вставкам кода на низкоуровневых языках программирования;
- список предполагаемых дефектов;
- блок-схемы функциональных объектов.

♦ **Построение различных отчётов для динамического анализа исходного кода:**

- отработавшие функциональные объекты и связи между ними;
- отработавшие базовые блоки и связи между ними.

♦ **Соблюдение ролевой модели:** гибкое разграничение доступа по ролям позволяет чётко разделять права пользователей и предотвращать несанкционированные изменения, что важно для команд с разными уровнями ответственности и защиты данных.

♦ **Удобство развёртывания:** архитектура «клиент-сервер» позволяет масштабировать систему в крупных компаниях, снижая нагрузку на локальные машины и обеспечивая централизованное управление.

♦ **Параллельность работы:** позволяет проводить одновременный анализ нескольких проектов и ко-

ординировать действия различных экспертов.

КАК АК-ВС 3 ПОМОГАЕТ БИЗНЕСУ?

Благодаря АК-ВС 3 компании могут:

♦ **повысить безопасность ПО, выявляя уязвимости до релиза:** выявление уязвимостей на ранних стадиях разработки позволяет минимизировать потенциальные риски, связанные с эксплуатацией уязвимостей злоумышленниками;

♦ **соответствовать нормативным требованиям без лишних затрат:** инструмент полностью отвечает требованиям ФСТЭК, Минобороны России, положениям Банка России и ГОСТ Р 56939, упрощая сертификацию и обеспечение регуляторного соответствия;

♦ **снизить затраты на исправление дефектов кода за счёт раннего выявления проблем:** обнаружение уязвимостей на этапе разработки снижает расходы на их устранение по сравнению с исправлением ошибок в выпущенной версии приложения;

♦ **автоматизировать проверки, экономя время команды разработчиков:** АК-ВС 3 легко интегрируется в конвейеры CI/CD, позволяя компаниям внедрять DevSecOps-подход и обеспечивать безопасность без замедления процессов разработки;

♦ **проводить анализ для широкого спектра языков программирования:** АК-ВС 3 анализирует код на C/C++, Java, C#, Python, PHP, Golang;

♦ **использовать интерактивные инструменты визуализации анализа:** механизмы построения графов зависимостей, блок-схем и маршрутов функциональных объектов упрощают понимание кода и ускоряют устранение уязвимостей;

♦ **применять гибкую настройку и расширяемость:** возможность адаптации инструментов анализа под требования конкретного проекта позволяет учитывать специфику используемых технологий и архитектурных решений.

ЗАКЛЮЧЕНИЕ

АК-ВС 3 представляет собой уникальное решение для обеспечения

безопасности программного обеспечения, сочетая в себе несколько типов анализа и соответствие нормативным требованиям. Его возможности по интеграции в процессы CI/CD, поддержка множества языков программирования и высокая гибкость делают его мощным инструментом для разработчиков и компаний, стремящихся обеспечить высокий уровень безопасности своих программных продуктов.

СПРАВКА О КОМПАНИИ

Группа компаний «Эшелон» специализируется на комплексном обеспечении информационной безопасности и включает в себя множество отделов, занимающихся вопросами защиты информации. Основными направлениями деятельности Центра оценки соответствия и тестирования являются:

♦ сертификация средств защиты информации (в том числе технических);

♦ внедрение, включая выстраивание всех процессов в соответствии с ГОСТ Р 56939;

♦ оценка соответствия по требованиям ОУД в рамках проверки банковских приложений (требования ГОСТ ИСО/МЭК 15408, Профиля защиты Банка России, положений Банка России);

♦ проведение тематических исследований по требованиям ФСБ России;

♦ проведение оценки по требованиям стандарта платформы Цифрового рубля.

Для отслеживания последних новостей в сфере информационной безопасности подписывайтесь на наш telegram-канал Echelon Eyes:



КАК РАБОТАЮТ ИНСТРУМЕНТЫ СТАТИЧЕСКОГО И ДИНАМИЧЕСКОГО АНАЛИЗА КОДА

ОПЫТ ИСПОЛЬЗОВАНИЯ АК-ВС 3



Роберт АРУСТАМЯН
заместитель
директора
Центра оценки
соответствия
и тестирования
АО «НПО
«Эшелон»



Нелли МАГАКЕЛОВА
руководитель
группы
Центра оценки
соответствия
и тестирования
АО «НПО
«Эшелон»



Илья АНТИПОВ
руководитель
группы
Центра оценки
соответствия
и тестирования
АО «НПО
«Эшелон»

В условиях развития технологий и возрастания угроз в сфере кибербезопасности обеспечение безопасности программного обеспечения становится приоритетной задачей для многих организаций. Одним из эффективных способов выявления потенциальных уязвимостей является использование инструментов статического и динамического анализа кода. Эти методы анализа играют ключевую роль в раннем обнаружении дефектов и уязвимостей, что позволяет значительно повысить безопасность разрабатываемых программных продуктов.

СТАТИСТИКА

АК-ВС 3 активно используется в различных сферах, включая государственные учреждения, коммерческие организации и высшие учебные заведения. Решение успешно интегрировано в процессы безопасности множества организаций, что подтверждается растущей статистикой его внедрения. Университеты применяют АК-ВС 3 для обучения специалистов в области информационной безопасности, а государственные структуры используют его для анализа критически важных программных решений.

С 2024 года по настоящее время 118 организаций, включая государствен-

ные учреждения, высшие учебные заведения и испытательные лаборатории, успешно приобрели продукт АК-ВС 3. Из данного числа 110 организаций представляют коммерческий сектор, что свидетельствует о растущем интересе бизнеса к современным технологиям анализа кода. С начала 2025 года около 10–15 организаций воспользовались возможностью протестировать демоверсию АК-ВС 3.

АРХИТЕКТУРА АК-ВС 3:

1. Модуль «Клиент» — IDE «Эшелониум»: осуществляет работу с проектами, предоставляет возможность для просмотра, анализа и разметки срабатываний.

2. Модуль «Сервер»: обеспечивает выполнение статического анализа кода, динамического анализа кода, полносистемного динамического анализа (Код2), фаззинг-тестирования, а также предоставляет веб-интерфейс для удобной работы.

3. Модуль сборки: включает утилиту для подготовки исходных текстов, необходимых для выполнения статического анализа в рамках проведения подконтрольной сборки исследуемого программного обеспечения.

4. Модуль фаззера: менеджер фаззеров, который выполняет фаззинг-тестирование.

5. Модуль «Код2»: отвечает за реализацию полносистемного дина-

мического анализа и подготовку полносистемных трасс для последующего анализа (рис. 1).

ИСПОЛЬЗУЕМЫЕ МЕТОДЫ АНАЛИЗА

Статический анализ исходного кода программы (SAST).

Статический анализ представляет собой процесс анализа исходного кода программы с целью выявления дефектов кода, в частности потенциально опасных конструкций. В соответствии с актуальной нормативной базой данный анализ также следует проводить в отношении компонентов, заимствованных у сторонних разработчиков, при условии доступности их исходного кода.

Первые версии статических анализаторов были схожи с линтерами — утилитами, которые выполняют анализ кода, ищут совпадения с заданными шаблонами и формируют выводы о наличии или отсутствии определённых конструкций в исходном коде. Например, это может касаться жёстко заданных паролей или использования небезопасных функций. Изначально линтеры разрабатывались с целью содействия разработчикам в написании качественного кода и не имели непосредственного отношения к вопросам безопасности.

Цели статического анализа кода программы:

- ♦ поиск дефектов кода;

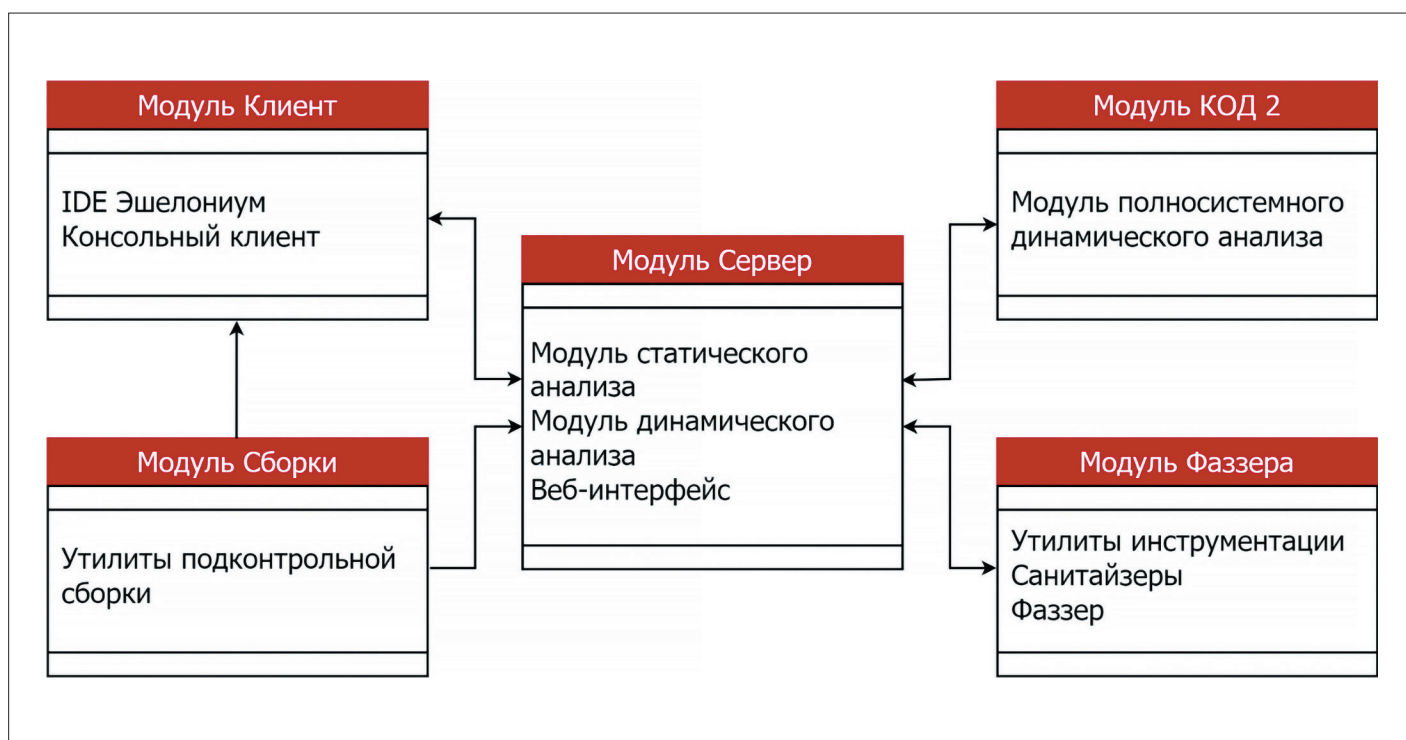


Рисунок 1. Состав и структура АК-ВС 3

- ◆ подсчёт метрик;
- ◆ рекомендации по оформлению кода;
- ◆ внедрение в рамках цикла безопасной разработки (SSDLC);
- ◆ обеспечение выполнения нормативных требований заказчика и регуляторов.

Основные применяемые методы статического анализа кода программы:

1. Синтаксический анализ: включает использование базы данных сигнатур, где ошибки выявляются путём поиска заранее известных антипаттернов в исходном коде.

2. Межпроцедурный анализ: позволяет выявлять сложные ошибки, возникающие из-за взаимодействия различных функций и методов. В этом случае анализируется не только отдельная строка кода, но и совокупность всех файлов и функций с учётом контекста и взаимосвязей.

3. Контекстно-чувствительный анализ: сохраняет контекст переходов между функциями и их состояниями. Например, если для входа в определённую функцию необходимо, чтобы переменная имела значение 0, статический анализатор будет отслеживать, что в дальнейшем

эта переменная не может принимать иное значение.

Дополнительно могут быть использованы межмодульный анализ, анализ потока управления, анализ потока данных и ряд других методов. Для более детального ознакомления с различными видами статического анализа рекомендуется обратиться к статье, в которой представлен сравнительный анализ работы статических анализаторов в соответствии с требованиями ФСТЭК России, Министерства обороны Российской Федерации, а также зарубежных стандартов, таких как NIST SP 500-268 и SATEC¹.



¹ Марков А. С., Антипов И. С., Арустамян С. С., Магакелова Н. А. Сравнительный анализ статических анализаторов кода. Современная методология // Вопросы кибербезопасности. 2024. № 5 (63). С. 79–88.

В ходе статического анализа кода акцент делается на выявление дефектов, однако уязвимости могут быть обнаружены исключительно в процессе динамического анализа. Значительная часть проблем, связанных с безопасностью программного обеспечения, проявляется лишь во время выполнения программы. Таким образом, динамический анализ играет ключевую роль в обеспечении безопасности программных продуктов, позволяя выявить риски, которые невозможно обнаружить, работая лишь с исходными текстами программы.

Динамический анализ кода (DAST).

Динамический анализ кода представляет собой процесс выявления уязвимостей в режиме выполнения (run-time) программного обеспечения. Основные методы динамического анализа включают общую сборку путей выполнения, полносистемный анализ и фаззинг-тестирование.

Общая сборка путей выполнения включает проведение сборки исходных текстов, в которые будут интегрированы специальные датчики. Эти датчики отслеживают прохо-

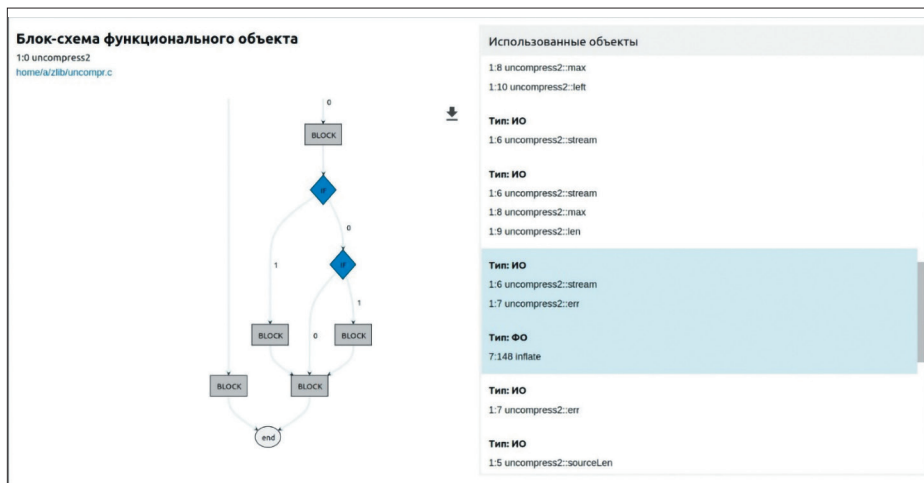


Рисунок 2. Построение блок-схемы для конкретного функционального объекта

tcl: отработавшие ФО (процедуры и функции)			
№	QID	Название	Отработал
№ 1001	QID: 44:48	Название: Tcl_NewListObj	Был вызван: +
№ 1002	QID: 44:73	Название: Tcl_DbNewListObj	Был вызван: -
№ 1003	QID: 44:79	Название: Tcl_SetListObj	Был вызван: +
№ 1004	QID: 44:106	Название: TclListObjCopy	Был вызван: +
№ 1005	QID: 44:133	Название: Tcl_ListObjGetElements	Был вызван: +

Рисунок 3. Анализ отработавших функциональных объектов, которые были проинструментированы датчиками при динамическом анализе

дящие через них вызовы функций и осуществляют запись логов в файл, на основе которых впоследствии осуществляется анализ и формируется трасса выполнения. Это позволяет определить, какие блоки кода были вызваны, а какие остались неиспользованными, а также проследить за прохождением по веткам выполнения (рис. 2).

Таким образом, этапы динамического анализа выглядят следующим образом:

1. Сбор логов по динамическому выполнению проекта.
2. Обнаружение путей ветвления и исполнения проекта на основе реального выполнения.

3. Определение модулей и функций, через которые проходило выполнение.

4. Выявление мест возникновения ошибок и сбоев (рис. 3).

Полносистемный динамический анализ (Код2).

Полносистемный анализ представляет собой анализ с полной трассировкой выполнения программы, что позволяет отслеживать помеченные данные, а также выполнение и пересечение различных элементов. Этот метод основан на использовании QEMU, в рамках которого осуществляется функциональное тестирование, трассировка и непосредственный анализ.

Этапы полносистемного анализа:

- ♦ полносистемный анализ трассы выполнения кода;
- ♦ запись данных всей системы с отслеживанием каждого элемента;
- ♦ поиск утечек данных и критической информации.

Фаззинг-тестирование (FAST).

Фаззинг-тестирование представляет собой методику, при которой на вход программы подаются сгенерированные или мутационные данные. В рамках фаззинга с обратной связью (feedback-based fuzzing) осуществляется сбор логов о том, как обработанные данные влияют на систему. Входные данные генерируются с использованием как мутационных, так и словарных (генерационных) методов.

♦ Мутационный фаззинг: данные могут принимать любые формы, включая изображения, видео, байты и произвольные наборы данных.

♦ Генерационный фаззинг: этот метод, хотя и имеет частичное совпадение с мутационным, позволяет генерировать входные данные, которые являются валидными для первого фильтра при взаимодействии с интерфейсом системы.

Фаззинг-тестирование в АК-ВС 3 реализовано на основе AFL++ с учетом оригинальной технологии разработки.

Вывод

Инструменты статического и динамического анализа кода играют важнейшую роль в обеспечении безопасности программного обеспечения, позволяя выявить уязвимости на разных этапах разработки. Статический анализ помогает обнаружить дефекты на уровне исходного кода, прежде чем они могут быть использованы злоумышленниками. Динамический анализ, в свою очередь, позволяет выявить проблемы, которые могут проявиться лишь во время выполнения программы, такие как утечки памяти или переполнения буфера. Оба метода являются неотъемлемой частью процесса безопасной разработки и позволяют предотвратить угрозы безопасности на ранних стадиях.

СЕРТИФИКАЦИЯ ПО

НОВЫЕ ВЫЗОВЫ И ВОЗМОЖНОСТИ



**Михаил
ГЕЛЬВИХ**
руководитель
отдела
технического
сопровождения
ООО ПВС

В эпоху цифровизации и растущих киберугроз сертификация программного обеспечения становится критически важной для бизнеса. Особую актуальность этот вопрос приобрёл после введения новых стандартов (таких как ГОСТ Р 71207–2024 и ГОСТ Р 56939–2024), направленных на обеспечение процесса разработки безопасного программного обеспечения (РБПО).

В то время как ГОСТ Р 56939–2024 охватывает более широкий спектр процессов и мероприятий по обеспечению безопасности на всех этапах жизненного цикла ПО, ГОСТ Р 71207–2024 фокусируется именно на инструментальных методах анализа, позволяющих повысить качество и безопасность создаваемых программных продуктов.

СТАТИЧЕСКИЙ АНАЛИЗ: ЧТО ЭТО?

SAST (Static Application Security Testing) — это методология тестирования, при которой код программы анализируется на наличие потенциальных уязвимостей без его фактического выполнения. Согласно стандарту, современные анализаторы должны обнаруживать наиболее распространённые критические ошибки, возникающие при разработке ПО:

- ♦ ошибки непроверенного использования чувствительных данных;
- ♦ ошибки некорректного использования системных процедур и интерфейсов;

- ♦ ошибки целочисленного переполнения и переполнения буфера;
- ♦ проблемы с управлением динамической памятью;
- ♦ ошибки в многопоточных приложениях.

ПРОБЛЕМЫ, РЕШАЕМЫЕ СТАТИЧЕСКИМ АНАЛИЗОМ

Соответствие требованиям ГОСТ Р 56939–2024 в рамках процессов разработки безопасного ПО подразумевает использование специализированных инструментов для систематического выявления и устранения уязвимостей. Как раз здесь на помощь приходят статические анализаторы, такие как PVS-Studio, которые позволяют решать ряд ключевых задач:

1. Раннее выявление уязвимостей. Статический анализ кода позволяет обнаруживать потенциальные уязвимости ещё на этапе разработки, что значительно снижает риск их использования злоумышленниками.

2. Экономия на исправлении ошибок. Исследования подтверждают: чем раньше будет обнаружена уязвимость, тем меньше будут затраты на её исправление. Это позволяет компаниям не только экономить деньги, но и сосредоточиться на разработке новых функций, а не на исправлении старых.

3. Защита корпоративной репутации. Репутационные потери от инцидентов безопасности часто превышают прямые финансовые убытки. Регулярное использование SAST-инструментов помогает минимизировать риски и защищает вашу репутацию.

4. Автоматизация и интеграция в CI/CD. Современные статические анализаторы легко интегрируются в процессы CI/CD. Это позволяет автоматически проверять код на наличие потенциальных уязвимостей после каждого изменения, что ускоряет процесс разработки и улучшает её качество.

5. Увеличение доверия со стороны клиентов. Наличие сертификации по ГОСТ Р 56939–2024 и использование инструментов статического анализа, таких как PVS-Studio, могут повысить доверие со стороны клиентов к разработчикам программного обеспечения или даже являться обязательным требованием, если речь заходит о проектах в области КИИ.

ПОЧЕМУ ЭТО ВАЖНО ДЛЯ БИЗНЕСА

Таким образом, внедрение статического анализа в процессы разработки и сертификация ПО по новым стандартам становятся необходимыми для компаний, стремящихся к повышению уровня своей информационной безопасности. Инструменты, такие как PVS-Studio, соответствующие требованиям ГОСТ Р 71207–2024, помогают разработчикам создавать более безопасные и надёжные программные решения, сокращая затраты на исправление ошибок и повышая эффективность разработки.

Предложите вашей команде разработки возможность бесплатно попробовать PVS-Studio в течение месяца, используя промокод **BIS, и на практике оценить возможности инструмента по выявлению дефектов безопасности в коде программ, написанных на языках C, C++, C#, Java.**



ПИЛОТ, ЧТОБЫ SAST «ЛЕТЕЛ» В ПЯТЬ РАЗ БЫСТРЕЕ

ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИИ ДЛЯ ЗАДАЧ СТАТИЧЕСКОГО АНАЛИЗА КОДА



**АНТОН
БАШАРИН**
старший
управляющий
директор
AppSec Solutions

Бизнес всё чаще начинает уделять внимание информационной безопасности, и компании неизбежно сталкиваются с ситуацией перегрузки ИБ-инженеров. Топ-менеджмент встает перед выбором: либо кратко увеличивать штат, либо пренебрегать безопасностью. И то и другое – дорого, поскольку найм редких специалистов затратен, а утечки данных могут привести к серьезным убыткам.

Сегодня бизнес, запустивший внедрение инструментов безопасной разработки и практику РБПО, ожидает сокращение рисков и времени на разработку в несколько раз. Однако быстро сталкивается с объективными трудностями. Внедрение SAST-инструментов не ускоряет разработку, а наоборот замедляет её, поскольку 80% срабатываний – ложные. Это показало исследование, которое провела команда AppSec Solutions на данных полутора десятков компаний-клиентов.

Статистика по автоматизации обработки результатов сканирования ПО в России улучшилась: в 2023 году такому разбору поддавалось лишь 35% срабатываний, в 2024 – уже 64%. Это значительно облегчает и ускоряет

работу ИБ-команд. Без таких инструментов инженерам приходится тратить недели на разбор срабатываний, большинство из которых ложные.

Команда из 10 000 разработчиков при интенсивной нагрузке может обрабатывать до 1000 сканов по 1000 записей в сутки. В сумме мы получаем ежедневно до 1 млн записей, которые необходимо разобрать и определить, в каких случаях требуется личное участие квалифицированного ИБ-инженера, а в каких ошибки типичны или вовсе не существуют. Для команды из 10 специалистов по кибербезопасности это работа приблизительно на 200 дней. Впечатляющие цифры, не так ли? Если учесть, что 80% срабатываний ложные, можно считать, что это время потрачено напрасно, при том, что каждый ИБ-инженер на вес золота.

Как сэкономить это время? Одно из решений – использовать искусственный интеллект. Мы разработали модуль AppSec.CoPilot. Это DevSecOps-помощник на основе ИИ, который в автоматическом режиме анализирует и сортирует уязвимости, определяя критические с точностью 96%. Он устраняет ложные срабатывания и сортирует уязвимости по критичности, позволяя команде сосредоточиться на самых серьезных недостатках кода и освобождая время инженеров для более важных задач.

Исследования команды AppSec Solutions на данных более 10 компаний показали, что применение ИИ-помощника сокращает время работы на 85%. Если в 2023 году обработка одной уязвимости занимала 26 дней, то сейчас – всего 1–2 дня, что позво-

ляет сократить Time-to-Market более чем втрое.

Аналогов AppSec.CoPilot в России пока нет, поскольку мы обучали его конкретно под сканирование и приоритизацию уязвимостей. В отличие от крупных универсальных нейросетей, которые обладают широкой специализацией, наш инструмент создан и обучен именно для обеспечения информационной безопасности. Он легко встраивается в любой SAST и адаптируется на стороне заказчика. Модель защищена от лишней информации и обучается на коде клиента, что позволяет эффективно внедрять ее в работу.

AppSec Solutions запустила AppSec.CoPilot осенью 2024 года. Изначально инструмент был «заточен» под финтех и защиту коммерческой тайны, но к настоящему моменту мы адаптировали его для удобной интеграции в работу промышленных компаний, будь то добывающая или обрабатывающая отрасли, где активы и секреты значительно отличаются от финансового сектора. Это особенно важно при решении проблем параллельного импорта и работы софта по управлению иностранным промышленным оборудованием, где каждое обновление ПО может привести к остановке процесса без возможности «восстановиться» из бэкапа.

До конца 2025 года мы планируем усовершенствовать модуль, добавив автоматическое закрытие уязвимостей, обучая его на исходном коде. Так AppSec.CoPilot сможет облегчать жизнь и ИБ-инженерам, и разработчикам, которым назначаются дефекты и тикеты по устранению подтвержденных уязвимостей.

ПОЧЕМУ БЕЗОПАСНИКИ НЕ ХОТЯТ ЗАКРЫВАТЬ ТАСКИ

АНАТОМИЯ КОРПОРАТИВНОГО КОНФЛИКТА



Андрей ЖАРКЕВИЧ
эксперт Start X,
ведущий рубрики

Однажды за чашкой чая друг поделился болью. Он работает в крупной финансовой компании. Его команда запускала новый продукт — мобильное приложение для клиентов. Всё было готово: интерфейс, код, тесты пройдены. Осталось последнее — согласование с департаментом информационной безопасности.

И тут началось то, что я называю «танцы с бубнами вокруг священных тотемов ИБ».

Сначала им вернули документы с комментарием: «Недостаточно проработаны аспекты защиты». Какие именно? «Все». После двух недель уточнений выяснилось, что разработчики должны подготовить документацию по 14 дополнительным пунктам, большинство из которых относились к гипотетическим угрозам с вероятностью реализации около 0,001 %.

«Вы понимаете, что задержка запуска на месяц обойдётся компании примерно в 20 миллионов рублей упущенной прибыли?» — спросили у руководителя ИБ.

Его ответ убил наповал: «А вы понимаете, что один инцидент безопасности может обойтись в 100 миллионов?»

Вопрос «откуда взялась эта цифра» так и остался без ответа.

КОРЕНЬ ПРОБЛЕМЫ: РАЗНЫЕ СИСТЕМЫ КООРДИНАТ

Позже я понял, что проблема гораздо глубже, чем просто бюрократия или личные амбиции. Дело в фундаментально разных системах координат.

Бизнес-подразделения живут в мире конкретных целей: выручка, прибыль, доля рынка, удовлетворённость клиентов. У этих показателей есть чёткие метрики, по которым оценивается эффективность работы.

Подразделение ИБ существует в иной реальности. Их основная задача — предотвращение негативных событий, то есть того, что не случилось. Как измерить то, чего нет? Как доказать, что именно твои действия привели к тому, что нечто не произошло?

Неудивительно, что безопасники создают собственную систему метрик: количество «отражённых атак», число выявленных уязвимостей, процент сотрудников, прошедших обучение по ИБ. Эти цифры впечатляют руководство, но редко коррелируют с реальной защищённостью бизнеса.

«В прошлом месяце мы предотвратили 3 миллиона атак», — с гордостью сообщил CISO на совещании. Когда у него спросили, что именно считается «атакой», выяснилось, что 99,9 % из них — это автоматизированное сканирование портов, которое блокируется стандартным межсетевым экраном без какого-либо участия сотрудников ИБ.

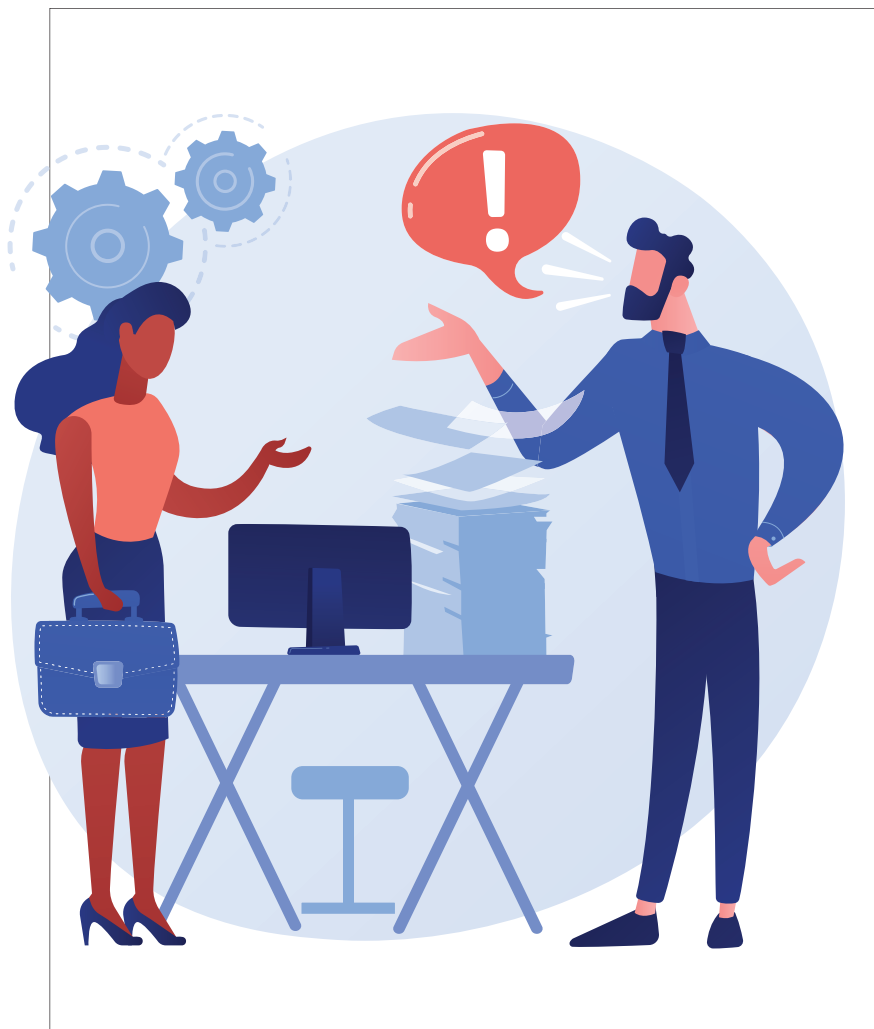
Пока праздновали эту «победу», реальный фишинг, нацеленный на финансового директора, остался незамеченным.

СИНДРОМ «ХВОСТ ВЛИЯЕТ СОБАКОЙ»

С ростом цифровизации бизнеса влияние службы ИБ только усиливается. И зачастую это приводит к парадоксальной ситуации: подразделение, созданное для обеспечения работы бизнеса, начинает им управлять.

В филиале банка, где я работал, существовало правило: «Коммерческое предложение не должно содержать точных процентных ставок». Причина? «Потенциальная утечка конфиденциальной информации». Исходящие письма реально мониторили, и нарушителей наказывали.

— Хорошо, — спросил я у главного по ИБ, — а как тогда сотрудники должны сообщать клиентам условия сделки?



- При личной встрече.
- А если клиент в другом городе?
- Можно по защищённой почте.
- Но это платная услуга для действующих клиентов, а тут идут переговоры с новым клиентом.
- Моя задача — не допустить утечки информации, а не организовывать работу с клиентами.

Такие диалоги стали обыденностью. Продажи падали, клиенты уходили к конкурентам, но отдел ИБ праздновал победу: ни одной утечки процентных ставок! В конце концов сотрудники отдела по работе с клиентами стали согласовывать процентные ставки с клиентами через WhatsApp с личных телефонов.

Постепенно я стал замечать, что до 40 % рабочего времени менеджеры тратят не на работу с клиентами, а на разработку способов обойти бессмысленные запреты. Или, что ещё хуже, на «аппаратные войны» — бесконечные совещания, где бизнес-подразделения пытаются объяснить ИБ-специалистам основы ведения бизнеса.

СВЯЩЕННОЕ ПРАВО НЕ ЗАКРЫВАТЬ ЗАДАЧИ

Особенно ярко этот конфликт проявляется в отношении к обычным рабочим процессам. Если любое другое подразделение обязано отчитываться о выполнении задач, соблюдать сроки и следовать регламентам, то ИБ существует как будто вне этой системы.

Со мной поделились случаем, когда подразделение разработки месяц ждало ответа на простой вопрос: можно ли использовать определённую библиотеку в проекте? Задача в системе трекинга висела без движения, напоминания игнорировались.

Когда главный по разработке наконец поймал ответственного сотрудника ИБ в коридоре, тот искренне удивился: «А зачем мне закрывать эту задачу? Моя работа — выявлять риски, а не помогать вам запускать непроверенный код».

Показательно, что в этой же компании за просроченную на день отчётность могли лишиться премии, но за висящие месяц задачи ИБ никто не получал даже устного замечания.

ИСТОКИ КУЛЬТУРНОГО РАЗРЫВА

Чтобы понять, откуда берётся такое поведение, стоит взглянуть на эволюцию роли ИБ-подразделения в компании.

В начале XX века в крупных компаниях появилась должность «заместитель по электрификации». Это был человек, понимающий таинственную силу электричества, от которой зависело функционирование предприятия. К его мнению прислушивались, его рекомендации выполняли беспрекословно, ведь альтернативой могла быть остановка производства или даже пожар.

В начале XXI века аналогичную роль получили ИТ-директора. Они говорили на непонятном языке серверов, баз данных и программных интерфейсов. Постепенно, однако, технологии стали более понятными, а ИТ-директора научились говорить на языке бизнеса.

Сегодня эстафету «таинственных хранителей корпоративных секретов» приняли CISO — руководители по информационной безопасности. Они оперируют терминами, которые звучат как заклинания для непосвящённых: «zero-day-уязвимости», «threat intelligence», «SOC», «периметр безопасности».

Эта таинственность вкупе с регулярными новостями о разрушительных кибератаках создаёт питательную среду для формирования особой касты «корпоративных жрецов», которые не считают нужным объяснять свои решения простым смертным.

КОГДА БЕЗОПАСНОСТЬ СТАНОВИТСЯ САМОЦЕЛЬЮ

Проблема усугубляется тем, что цели службы ИБ зачастую формулируются в отрыве от бизнес-целей компании. Вместо «обеспечить безопасную работу бизнес-процессов» ставится задача «минимизировать все возможные риски».

А поскольку единственный способ полностью избежать рисков — это ничего не делать, неизбежно возникает конфликт.

В банке, где работал мой институтский товарищ, служба ИБ гордилась внедрением многоуровневой системы аутентификации сотрудников. Для входа в систему требовалось пройти несколько этапов проверки, занимавших до 10 минут. Операционисты, работающие с клиентами, были в отчаянии: скорость обслуживания упала вдвое.

Когда у руководителя ИБ спросили, учитывалось ли влияние новой системы на работу фронт-офиса, он искренне удивился: «Это не моя зона ответственности. Моя задача — обеспечить безопасность».

ЭКОНОМИКА БЕЗОПАСНОСТИ, ИЛИ СКОЛЬКО СТОИТ ПАРАНОЙЯ

В основе проблемы лежит ещё и экономический фактор. Безопасность, особенно избыточная, стоит дорого — не только в прямых затратах, но и в упущенных возможностях.

Представьте ситуацию: компания тратит 100 миллионов рублей на защиту от угрозы, вероятность реализации которой — 0,1 %, а потенциальный ущерб — 200 миллионов. С точки зрения математического ожидания, это крайне невыгодная инвестиция ($0,001 \times 200 \text{ млн} = 200 \text{ тыс. рублей}$).

Однако попробуйте объяснить это CISO, и вы услышите: «А если это всё-таки произойдёт? Кто будет отвечать?»

Этот аргумент — козырная карта всех безопасников. «Кто будет виноват, если...» в корпоративном мире значит гораздо больше, чем экономическая целесообразность. Именно поэтому руководители зачастую закрывают глаза на избыточные требования ИБ. Страх персональной ответственности перевешивает потенциальные бизнес-выгоды.

ВОЗМОЖНЫЕ ПУТИ РЕШЕНИЯ КОНФЛИКТА

Очевидно, что сложившаяся ситуация вредит бизнесу. Но как её изменить? Есть несколько подходов, которые показали свою эффективность.

1. Привязка KPI службы ИБ к бизнес-целям. В одной компании новый CEO принял радикальное решение: 50 % премии сотруд-

ников ИБ стало зависеть от выполнения общих бизнес-показателей. Эффект был поразительным — количество безосновательных запретов резко сократилось, а скорость согласования выросла в разы.

2. Количественная оценка рисков и затрат. Внедрение практики обязательного экономического обоснования требований ИБ также даёт хорошие результаты. Когда CISO обязан не просто заявлять «это небезопасно», а предоставлять конкретные расчёты вероятности угрозы, потенциального ущерба и стоимости защитных мер, многие «страшилки» оказываются экономически неоправданными.

3. Культура совместной ответственности. Важно создать в компании культуру, где безопасность — это общая ответственность, а не эксклюзивная прерогатива одного подразделения. Когда разработчики, маркетологи и операционисты понимают базовые принципы безопасности, а ИБ-подразделение — основы ведения бизнеса, возникает продуктивный диалог вместо конфронтации.

4. Сервис-ориентированный подход. Переосмысление роли ИБ как внутреннего сервиса, а не контролирующего органа меняет всю динамику взаимодействия. Вместо «запретителей» безопасники становятся консультантами, помогающими бизнесу достигать целей безопасным образом.

ЗАКЛЮЧЕНИЕ: БАЛАНС КАК КЛЮЧ К УСПЕХУ

За годы своей трудовой карьеры я видел компании, где безопасники парализовали бизнес-процессы, и компании, где безопасностью пренебрегали ради быстрых результатов. Ни один из этих подходов не приводил к долгосрочному успеху.

Оптимальный путь — это баланс между защитой и развитием. Безопасность должна быть достаточно строгой, чтобы защитить от реальных угроз, но не быть чрезмерной, чтобы не блокировать инновации и рост.

Достижение этого баланса — сложная задача, требующая изменения не только процессов, но и корпоративной культуры. Но компании, которым это удаётся, получают серьёзное конкурентное преимущество: они способны быстро адаптироваться к меняющемуся рынку, не подвергая себя неоправданным рискам.

Кстати, в таких компаниях безопасники закрывают свои таски вовремя. Не потому, что их заставляют, а потому что они понимают: их истинная задача — не запрещать, поощряя внутреннего вахтёра, а помогать бизнесу безопасно достигать целей.

«OSINT НЕ СТАНЕТ ОРУЖИЕМ КИБЕРПРЕСТУПНИКОВ, ЕСЛИ МЫ БУДЕМ ЛУЧШЕ ОСВЕДОМЛЕННЫ»

НА ВОПРОСЫ BIS JOURNAL ОТВЕЧАЕТ USERGATE



Дмитрий КУЗЕВАНОВ
директор
по информационной
безопасности,
руководитель
центра мониторинга
и реагирования (MRC)
компании UserGate

— **Как бы вы описали понятие OSINT, о котором эксперты ИБ так часто говорят в последнее время? Какие цели преследуют лица, использующие OSINT?**

— Концепция OSINT (Open Source Intelligence) в последние годы стала занимать важное место в сфере информационной безопасности. Разведка по открытым источникам, то есть сбор и анализ информации, полученной из разных общедоступных каналов, при определённых обстоятельствах может стать одним из опасных инструментов в руках киберпреступников.

На мой взгляд, следует разделять OSINT, связанный с физическими лицами и с юридическими, поскольку цели сбора информации и её источники в двух этих случаях существенно отличаются. OSINT вокруг юридических лиц очень часто используется злоумышленниками как подготовительный этап перед атакой на организацию.

Для иллюстрации прибегнем к матрице MITRE ATT&CK — это матрица тактик и техник кибератак, которая может быть полезна для оценки угроз и разработки стратегии защиты информационной системы. Разведка по открытым источникам входит в самую первую тактику, позволяя злоумышленникам получить большой набор сведений. Затем они анализируется злоумышленником для того, чтобы найти слабое звено для организации эффективной атаки на избранную цель.

Например, злоумышленники после сбора необходимой информации могут приехать по адресу компании и подключиться к корпоративной Wi-Fi-сети, доступной без пароля, и таким образом попасть в периметр организации. На моей памяти было несколько таких атак на коммерческие организации в России,

и они были вполне успешны. Информация об используемых корпоративных сервисах и их уязвимостях, также может дать злоумышленникам доступ в организацию.

— **Каковы особенности атак злоумышленников в отношении физических лиц? В каких случаях они могут прибегать к более технически продвинутым атакам с использованием шпионских программ?**

— OSINT вокруг физических лиц имеет отношение к личной жизни. Правда, он может быть продолжением OSINT вокруг организации. Злоумышленники могут провести исследование доступной публичной информации о каком-либо сотруднике, чтобы потом использовать её для организации социотехнической атаки. Например, с помощью фейкового аккаунта «коллеги» можно злоупотребить доверием сотрудника и заставить его выполнить желаемые действия. В целом OSINT, связанный с физическим лицом, обычно имеет своей целью шантаж или мошенничество.

Однако бывает и так, что физическое или юридическое лицо атакуют не целенаправленно. Допустим, сделали массовую фишинговую рассылку с «вредоносом». А потом, оценив чувствительный характер полученной информации, злоумышленники решили ей воспользоваться. То есть конкретный человек или организация изначально не были целью, но стали ей по мере развития атаки.

Для лучшего понимания приведу несколько примеров социотехнической атаки. Злоумышленники использовали методику OSINT, чтобы выяснить, кто является генеральным директором фирмы, и собрать о нем информацию: фамилия, имя, отчество, фото. Затем создали фейковый аккаунт и начали писать от его имени. Другой пример: имея электронную почту главного бухгалтера и проанализировав публичную бухгалтерскую информацию об организации, которая, например, доступна на портале бухгалтерской (финансовой) отчетности (БФО), злоумышленники пишут ему письмо от лица налоговой службы и просят открыть вложение, которое содержит вредоносный код.

OSINT привлекает злоумышленников своей простотой. Зачем использовать специ-

альные программы, если информация есть в открытом доступе и можно идти по пути наименьшего сопротивления? Кроме того, в большинстве случаев публично доступной информации вполне достаточно для начала злонамеренных действий.

— **Как может повлиять на OSINT ужесточение законодательства в области защиты и нераспространения персональных данных? Позволят ли эти меры поставить барьер перед неправомерным использованием конфиденциальных данных? Следует ли идти по пути ужесточения наказания должностных лиц, ответственных за утечки данных, или сделать больший акцент на обучении сотрудников?**

— Решения государства в сфере законодательного регулирования, связанные с повышением ответственности организаций и должностных лиц, усилением штрафных санкций за утечку персональных данных, должны дать свой эффект. При этом не следует прибегать к ограничению доступа к информации. Я считаю это плохим подходом. В идеальном мире надо повышать осведомленность пользователей, сотрудников, разработчиков, чтобы, даже если произошла какая-то утечка информации, она не привела к негативным последствиям. Это первая мера противодействия.

Вторая мера, связанная с законодательным регулированием, более уместна в тех случаях, когда персональные данные получены незаконным путем и их появление в открытых источниках в принципе не было предусмотрено. Вот тогда должна быть ответственность, которая помогает такие ситуации устранить или предотвратить.

Например, в ноябре 2024 года вышли новые требования законодательства в области обработки персональных данных, которые очень сильно помогли поставить под контроль распространение информации. Например, в случае с одним телеграм-ботом, который выступал агрегатором утечек персональных данных, поправки в законодательстве ограничили эту деятельность. Теперь нельзя свободно распространять информацию, содержащую персональные данные, если она более не доступна в публичном пространстве. Думаю, было бы неплохо, если бы аналогичные меры были применены к сервисам «пробивов». Будем надеяться, что и до них дойдет черёд.

— **Есть ли на российском рынке информационных безопасности (ИБ) современные продукты и решения, помогающие в вопросах профилактики утечек дан-**

ных и их использования в преступных целях? Какие решения может предложить клиентам ваша компания?

— Есть решения, которые призваны бороться с утечками — это продукты класса DLP (Data Loss/Leak Prevention). Однако продукты класса NGFW, SIEM, WAF также могут дополнить и усилить комплекс технических средств и сервисов, применяемых для защиты от утечек. Например, они позволяют распознать вредоносную активность внутри сети, выявить событие информационной безопасности и, возможно, злоумышленников внутри организации, быстро локализовать обнаруженную проблему, устранить её и тем самым не допустить утечку.

Отдельное большое направление в ИБ — это обучение персонала и администраторов. Это могут быть учебные курсы, связанные с повышением осведомленности сотрудников, где специалисты рассказывают, что такое фишинг, как отличить легальное письмо от нелегального, подлинный аккаунт от фиктивного, и что делать в этой ситуации. Мы нацелены на осуществление целого комплекса мер, обеспечивающих ИБ.

Если вы осведомлены, это повышает общий уровень ИБ. И речь идёт обо всех — и технических специалистах, и разработчиках, и бухгалтерии, и обычных пользователях, и руководителях, и архитекторах, которые проектируют какие-то системы. Всё это положительно влияет на общий уровень защищённости.

— **Какие дополнительные меры контроля следует принимать компаниям, с тем чтобы снизить потенциальный ущерб от атаки с использованием OSINT и социальной инженерии? В каком направлении следует двигаться для решения проблем, связанных с таким ущербом?**

— Какие бы меры регулирования мы ни вводили, какую бы информацию ни пытались удалить из публичных источников, конечные действия все равно зависят от пользователя. Поэтому очень хотелось бы, чтобы повышение осведомленности людей помогло избегать инцидентов даже в случае утечек данных, будь то личных, или корпоративных.

Следует свыкнуться с мыслью о том, что в целом мы живем в довольно уязвимом мире с точки зрения данных, циркулирующих вокруг нас. Поэтому, наверное, нам всем стоит быть в определённой степени психологически готовыми к тому, что данные о нас в принципе могут быть раскрыты и известны окружающим. Если мы примем это как данность, то, пожалуй, станем более защищенными.

Вопросы задавал
Усам Оздемиров

БЕЗ ДОПОЛНИТЕЛЬНЫХ СРЕДСТВ

ИСПОЛЬЗОВАНИЕ ВСТРОЕННОГО МЕХАНИЗМА КОНТРОЛЯ ПРОГРАММНОЙ СРЕДЫ В ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА WINDOWS

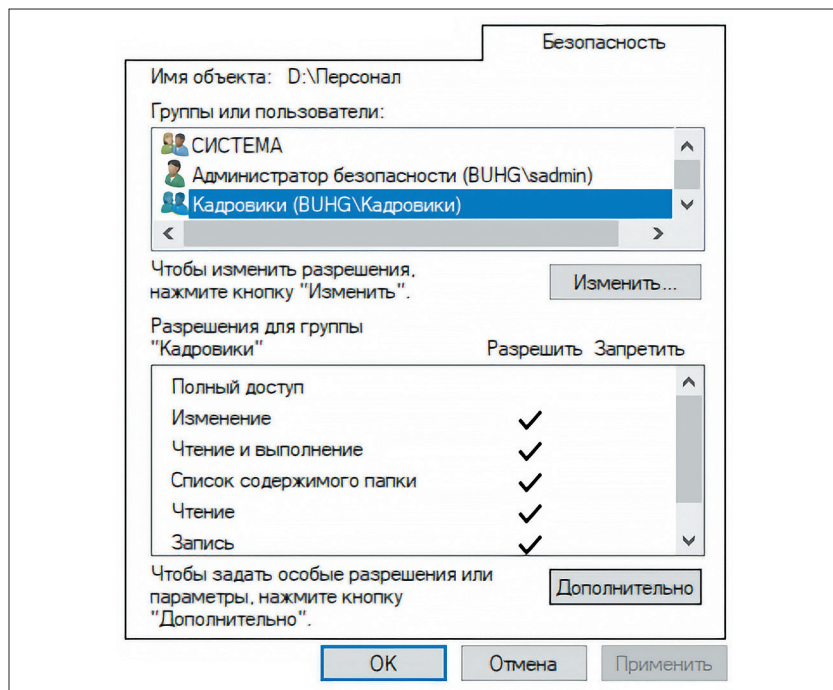


Рисунок 1. Привилегии прав доступа в ОС Windows

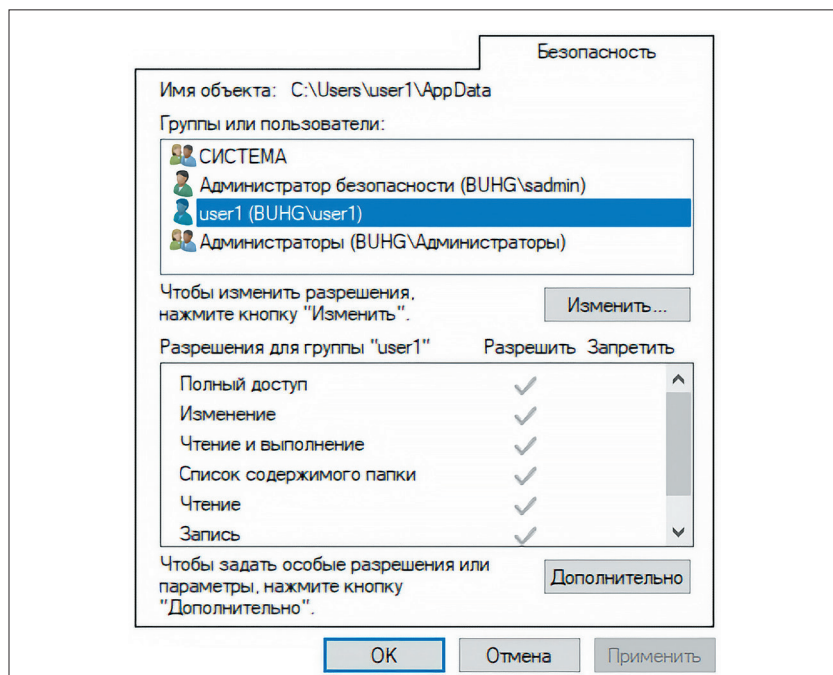


Рисунок 2. Права доступа пользователя к каталогам в его профиле



Ярослав ПРОКУШЕВ
эксперт Управления
по обеспечению
информационной
безопасности
ДБ Банка ВТБ (ПАО)

В данной статье рассматриваются практические аспекты применения одного из встроенных защитных механизмов ОС семейства Windows, позволяющего блокировать запуск не санкционированного программного обеспечения, в том числе и вредоносного.

СУТЬ ПРОБЛЕМЫ

Особенностью ОС семейства Windows является гибкий интерфейс настройки дискреционных прав доступа пользователей к каталогам. Однако он, на наш взгляд, содержит недостаток, который с момента появления Windows 2000 «мигрирует» из одной версии ОС в другую. Речь идёт о привилегии «чтение и выполнение». В частности, если пользователю предоставить доступ на изменение информации в папке, то он автоматически получает возможность запуска исполняемых файлов из каталога (рис. 1).

Если же администратор с помощью интерфейса *Дополнительных разрешений* отберёт у пользователя привилегию *Траверс папки / Выполнение файлов*, то у последнего возникнут проблемы с просмотром содержимого данного каталога. Рассматривая проблему контроля использования программного обеспечения в ОС семейства Windows, необходимо также упомянуть каталоги профилей пользователей, где им (пользователям) вообще предоставлен полный доступ (рис. 2).

Таким образом, возникает угроза бесконтрольного запуска пользователями программного обеспечения типа portable или его уста-

новки в каталоги собственного профиля. Кроме того, создаются отличные условия для первоначального внедрения и последующего запуска ВПО (вредоносного программно-го обеспечения) в атакуемой системе.

В домашних компьютерах, где многие работают с правами администраторов, ситуация с защищённостью ресурсов информационной системы ещё более тревожная. В них вредоносные программы часто изначально запускаются с правами привилегированной учётной записи.

ПУТИ РЕШЕНИЯ ПРОБЛЕМЫ

Выходом из сложившейся ситуации может стать применение политик ограниченного использования программ. Этот механизм способен блокировать несанкционированный запуск программ, даже если запуск был осуществлён от имени администратора. Чтобы использовать защитный механизм, следует запустить оснастку групповых политик *gpedit.msc*.

Доступ к редактору политик предоставляется, начиная с редакции *Professional*. Если же пользователь работает с редакцией Windows 10/11 Home Edition, то по умолчанию оснастка управления политиками безопасности недоступна. Тем не менее имеется несколько способов установки оснастки «Редактор локальной групповой политики»¹ для ком-

¹ Как добавить в Windows 11 Home Редактор локальной групповой политики. https://dzen.ru/a/ZLa_U-KVKTHUCBVM

пьютеров и с такой операционной системой². Рассмотрим настройку *политик ограниченного использования программ*. Изначально они отсутствуют, поэтому их надо создать (рис. 3).

Сразу после создания политик какие-либо ограничения на запуск программного обеспечения отсутствуют, установлено значение уровня доступа к программному обеспечению *Неограниченный*. Поэтому следует установить уровень безопасности запуска программного обеспечения (рис. 4) в положение *Запрещено*. При появлении предупреждения о повышении уровня безопасности ответьте утвердительно.

Затем требуется скорректировать *Дополнительные правила* для доверенного программного обеспечения (рис. 5) с учётом особенностей защищаемой системы.

Необходимо обратить внимание на каталоги, в которых размещаются файлы антивирусной программы и другого защитного программного обеспечения. Например, файлы антивируса *Microsoft Defender* находятся в каталоге *C:\ProgramData\Microsoft\Windows Defender\Platform*³. Для этой папки следует установить неограниченные права запуска, как и для каталога с 32-разрядным ПО *C:\Program files (x86)*. Отметим, что для

² Как включить редактор локальной групповой политики в Windows Домашняя. <https://remontka.pro/enable-group-policy-editor-windows-home/>

³ Microsoft изменила стандартный путь Защитника Windows в Windows 10. URL: <https://www.comss.ru/page.php?id=4708>

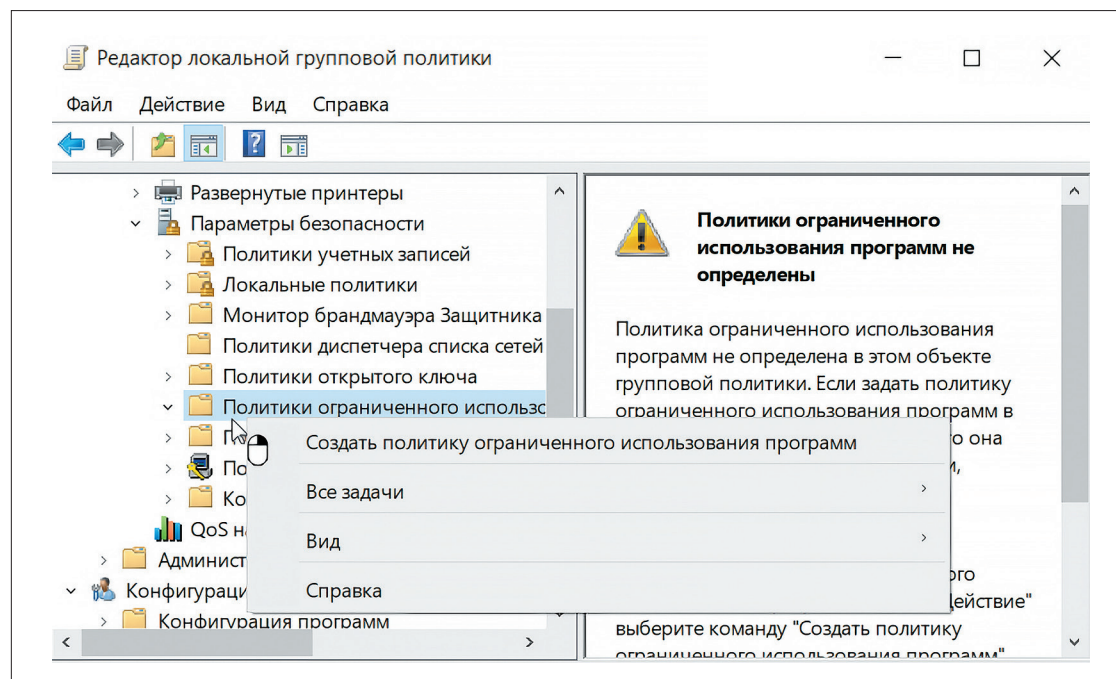


Рисунок 3. Создание политик ограничения запуска программ

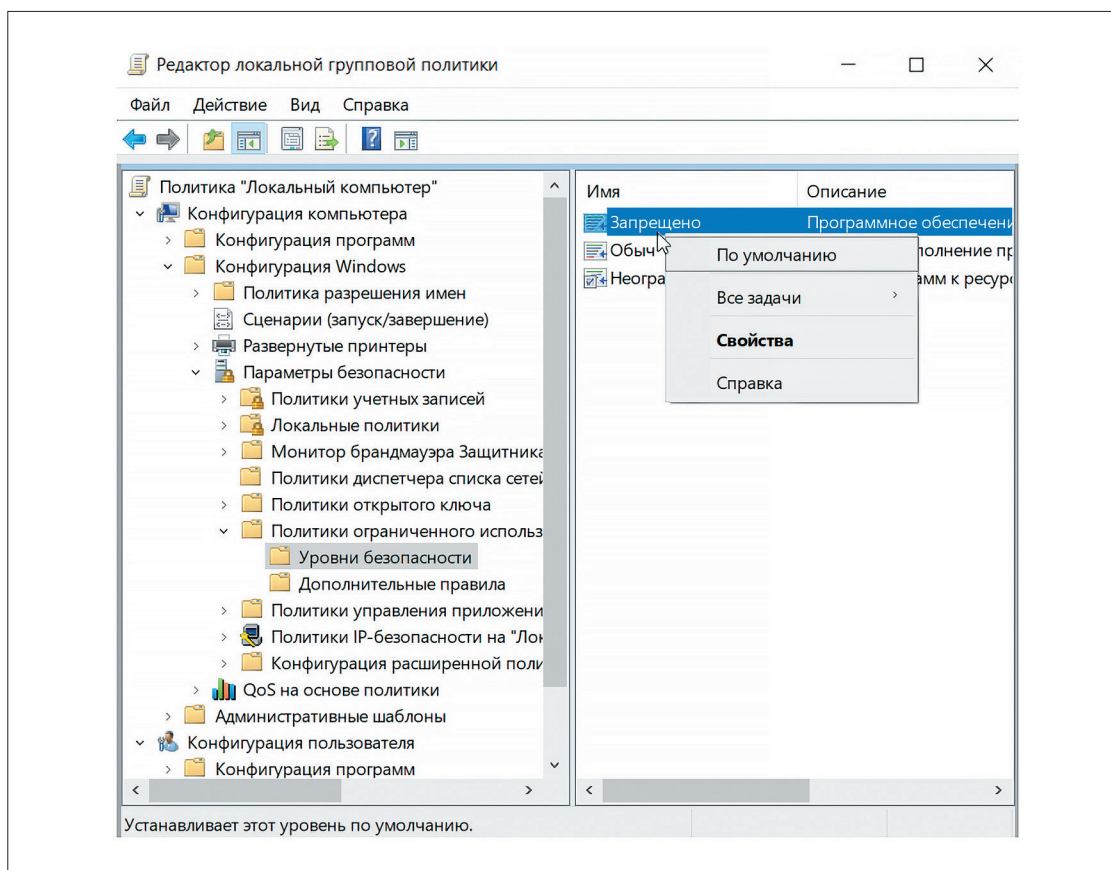


Рисунок 4. Установка уровня безопасности по умолчанию

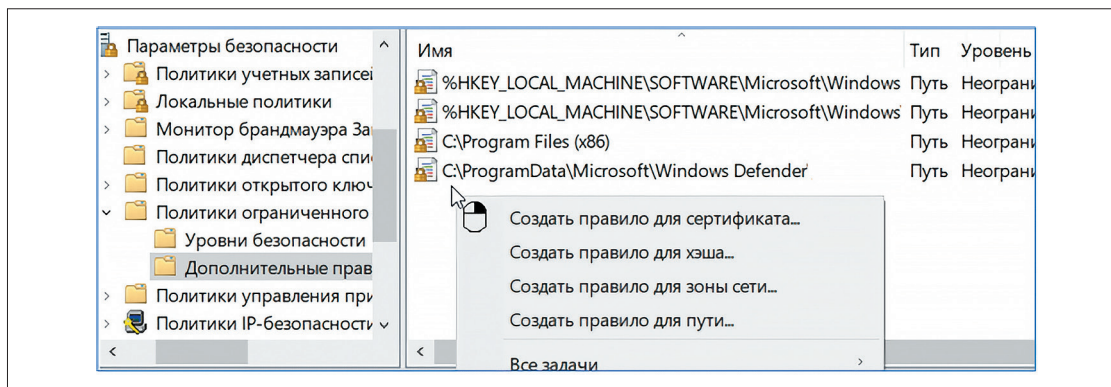


Рисунок 5. Создание правил для запуска программного обеспечения

запуска файлов из каталогов *C:\Windows* и *C:\Program files* правила в политике ограниченного использования программ создаются по умолчанию.

Наиболее простым способом формирования зоны запуска программного обеспечения является использование «правил для пути». Каталоги или файлы, разрешённые для запуска, определяются с указанием полного пути к ним. Если каталог с исполняемыми файлами антивируса не добавлен в *Дополнительные правила*, то он не запустится при старте операционной системы. Запуск будет блокироваться политиками безопасности.

Следующий этап — это корректировка типов файлов, распознаваемых политикой ограничения запуска программ как исполняемые, чей запуск будет ограничиваться (рис. 6) в окне настройки *назначенных типов файлов*. Расширения, которые указаны в этом окне, будут относиться к исполняемым файлам.

Дополнительно желательно добавить расширения *dll*, *sys*, *bin*, *cmd* и удалить тип *lnk*. Если расширение **lnk* не удалить, то ярлыки для запуска санкционированного ПО работать не будут, что создаст трудности в работе пользователей. Затем в окне *Применение* (открывается с помощью одноимённой надписи,

показанной на рисунке 6) надо указать, что на *dll*-файлы также распространяются ограничения использования (рис. 7) и что политика безопасности действует и на локальных администраторов (важно для безопасности домашних компьютеров, где почти все работают с правами администраторов). Чтобы принятые политики вступили в силу, надо перезагрузить компьютер.

Проверить работу созданных ограничений можно с помощью файла *calc.exe* (встроенная в ОС Windows программа *Калькулятор*) из каталога *C:\windows\system32*. Запустите файл *calc.exe* из разрешённой области – папки *C:\windows\system32*, где он изначально и находится. Запуск должен быть успешным. Затем скопируйте файл *calc.exe* и попробуйте запустить из любой папки профиля (рабочего стола или каталога с временными файлами *C:\users\user_name\appdata\local\temp*). Запуски должны быть неудачными.

Использование описанного метода существенно затруднит установку и запуск любого несанкционированного программного обеспечения.

ЗАКЛЮЧЕНИЕ

Тем не менее использование «правил для пути» не обеспечивает стопроцентной надёжности, поскольку этот тип ограничений контролирует только путь к объекту запуска, но не его содержимое. Например, средства защиты от НСД при настройке замкнутой программной среды дополнительно к пути исполняемого файла контролируют и его хеш-код, что делает крайне маловероятным эффективную его подмену. Тем не менее формирование перечня запускаемых файлов с помощью «правил для пути» позволяет быстро настроить ограничение запуска программ, в отличие от таких значительно более трудоёмких (хотя и более надёжных) способов, как использование правил для хеша или сертификата.

Отметим, что защита от подмены файлов программного обеспечения в Windows, хоть и не идеальная, но имеется. На стандартные папки размещения прикладных программ *C:\Program files* и *C:\Program files (x86)* установлены права доступа, разрешающие только их чтение для обычных пользователей. А на файлы из системного каталога *C:\Windows* даже группа *Администраторы* и учётная запись *Система* имеют только права чтения (рис. 8).

Для противодействия внедрению ВПО рекомендуется также периодически с помощью антивирусных сканеров *Dr. Web CureIt*

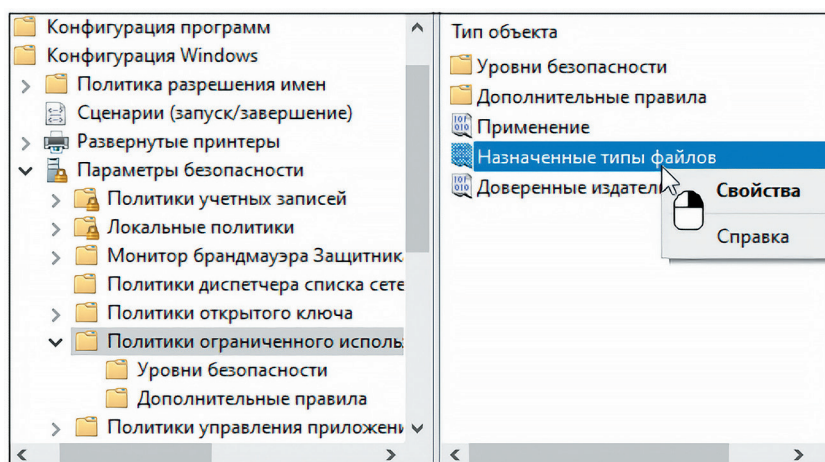


Рисунок 6. Доступ к настройке типов файлов

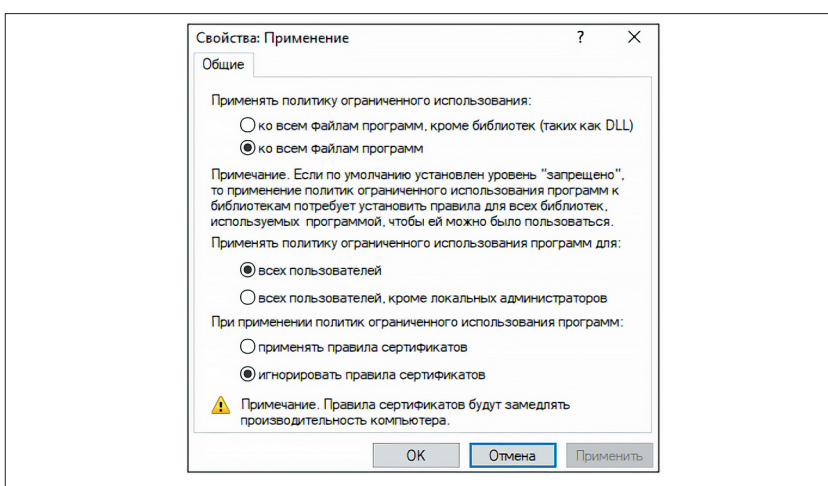


Рисунок 7. Выбор области применения политик

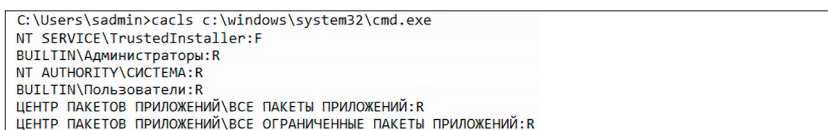


Рисунок 8. Права доступа к исполняемым файлам системного каталога

или *KVRT* осуществлять поиск вредоносных программ на компьютере.

Перед запуском сканеров на время их работы следует или отключить политику ограничения использования программ, или временно добавить правило для пути *C:\users\user_name\AppData\local\temp* (в этот каталог распаковываются файлы обоих сканеров в процессе работы), разрешающее из каталога запуск программ. После окончания работы сканеров надо вернуть все политики в исходное состояние.

Рассмотренный в данной работе метод ограничения области запуска программ является эффективным способом повышения безопасности работы ОС семейства Windows в случае, если не используются дополнительные средства защиты информации.

УТЕЧКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

НЕ ДАЮТ ПОКОЯ ВЛАСТЯМ ПО ОБОИМ БЕРЕГАМ
АТЛАНТИКИ

Усам ОЗДЕМИРОВ
корреспондент BIS Journal

Власти Швейцарии решили штрафовать субъектов КИИ за несообщение о киберинцидентах, человеческий фактор лежит в основе 95 % утечек данных, прокуратура Нью-Йорка обвинила страховую компанию в слабой защите от киберугроз, Белый дом провёл перетряску Агентства по кибербезопасности (CISA), ФБР не советует жертвам кибератак выплачивать выкуп злоумышленникам Medusa, а британские власти пригрозили карой социальным сетям за нарушения в обработке данных детей.

ШВЕЙЦАРИЯ ВВЕЛА ОБЯЗАТЕЛЬНУЮ ОТЧЕТНОСТЬ О КИБЕРАТАКАХ НА КРИТИЧЕСКИ ВАЖНУЮ ИНФРАСТРУКТУРУ

Субъекты критической инфраструктуры в Швейцарии вскоре будут обязаны по закону сообщать властям страны о кибератаках. Принятая Федеральным советом 7 марта норма будет упомянута в поправке к Закону об информационной безопасности (ISA) от 29 сентября 2023 года, которая вступит в силу 1 апреля 2025 года.

С этой даты субъекты критической инфраструктуры, работающие в стране, включая поставщиков энергии и питьевой воды, транспортные компании, а также кантональные и коммунальные администрации, должны будут сообщать о совершенных на них кибератаках в Национальный центр кибербезопасности (NCSC) в течение 24 часов с момента обнаружения.

Норма отчетности будет применяться, если кибератака угрожает функционированию критической инфраструктуры субъекта, привела к манипулированию или утечке

информации или связана с шантажом, угрозами или принуждением.

Форма отчета будет доступна на Cyber Security Hub NCSC, портале для обмена информацией между федеральным правительством Швейцарии и субъектами критической инфраструктуры. Организации, не зарегистрированные на платформе, могут отправлять отчеты по электронной почте, используя форму, доступную на веб-сайте NCSC. После отправки первоначального отчета в течение 24 часов с момента обнаружения инцидента у них есть 14 дней на заполнение отчета.

Субъекты критической инфраструктуры, которые не сообщают о кибератаке, соответствующей определенным критериям, могут быть оштрафованы, хотя власти не указали точную сумму. Переходный период будет действовать до 1 октября 2025 года, чтобы дать пострадавшим организациям достаточно времени для подготовки к новому обязательству по отчетности.

Законодательство многих стран мира предъявляет аналогичные требования к отчетности в отношении субъектов критической инфраструктуры, в том числе в Австралии, ЕС, Японии, Сингапуре, Южной Корее, Великобритании и США.

95% УТЕЧЕК ДАННЫХ В 2024 ГОДУ СВЯЗАНЫ С ЧЕЛОВЕЧЕСКИМ ФАКТОРОМ

Согласно новому исследованию Mimecast, 95 % утечек данных в 2024 году были вызваны человеческими ошибками, связанными с внутренними угрозами, неправомерным использованием учетных данных и ошибками пользователей. Небольшая часть сотрудников внесла несоразмерный вклад в эти инциденты безопасности: всего 8 % сотрудников оказались ответственными за 80 % инцидентов.

В отчете отмечено несколько громких инцидентов за последний год, связанных с че-

ловеческими ошибками. В их число входит атака с использованием вымогателя Change Healthcare, в ходе которой учетные данные сотрудника были скомпрометированы через фишинговое письмо, что позволило злоумышленникам получить доступ к сети.

Почти половина (43 %) респондентов сообщили об увеличении числа внутренних угроз или утечек данных, инициированных по причине беспечности или небрежности сотрудников за последние 12 месяцев. Кроме того, 66 % респондентов ожидают, что в следующем году потери данных от внутренних нарушителей возрастут.

Опрошенные лица, принимающие решения в области безопасности, заявили, что утечки данных и кражи, вызванные инсайдерами, обходятся организации в среднем в 13,9 млн долларов. Большинство (87 %) организаций заявили, что не реже одного раза в квартал обучают своих сотрудников обнаруживать кибератаки. Несмотря на это, 33 % опасаются ошибок и человеческого фактора в противодействии реализации угроз по каналу электронной почты, а 27 % обеспокоены тем, что усталость сотрудников приводит к потере бдительности.

В отчете установлено, что 95 % организаций используют искусственный интеллект (ИИ) для защиты от кибератак и/или внутренних угроз. Напротив, более половины (55 %) респондентов признали, что они не полностью готовы к конкретным стратегиям борьбы с угрозами, связанными с ИИ. Кроме того, 81 % были обеспокоены возможностью утечки конфиденциальных данных через инструменты GenAI.

Хотя 85 % респондентов сообщили, что бюджет на кибербезопасность их организаций увеличился за последние 12 месяцев, 57 % заявили, что требуется дополнительный бюджет для сотрудников по кибербезопасности и сторонних служб (57 %), безопасности инструментов совместной работы (52 %) и безопасности электронной почты (47 %).

Опрос выявил обеспокоенность по поводу того, что инструменты совместной работы расширяют поверхность атак, при этом 79 % согласились, что их использование создает новые угрозы и уязвимости безопасности. Данные инструменты предназначены для того, чтобы помочь людям общаться и координировать работу над проектами, в качестве примеров можно привести Slack и Zoom. Почти половина (44 %) респондентов сообщили об увеличении угроз со стороны этих инструментов за последние 12 месяцев, а 61 % заявили, что ожидают негатив-



ное влияние на бизнес из-за атак на платформы коммуникации в 2025 году.

НЬЮ-ЙОРК ПОДАЕТ В СУД НА ALLSTATE ИЗ-ЗА УТЕЧЕК ДААННЫХ И СБОЕВ В СИСТЕМЕ БЕЗОПАСНОСТИ

Генеральный прокурор Нью-Йорка Летиция Джеймс подала иск против подразделения Allstate, National General, утверждая, что компания не смогла должным образом защитить данные потребителей и не сообщила об утечках данных, которые раскрыли тысячи номеров водительских прав. Иск, поданный в суд штата Манхэттен, требует финансовых штрафов и улучшения мер безопасности.

Утечки, произошедшие в 2020 и 2021 годах, были вызваны уязвимостями в онлайн-инструментах расчета стоимости автострахования National General. Хакеры воспользовались слабыми местами в этих системах, чтобы получить доступ к номерам водительских прав более 165 000 жителей Нью-Йорка и почти 200 000 человек в общей сложности.

Офис генерального прокурора утверждает, что National General не смогла внедрить достаточные меры безопасности для предотвращения несанкционированного доступа и своевременно не предупредила пострадавших лиц и государственные органы. Согласно иску, первое нарушение произо-

шло в период с августа по ноябрь 2020 года, но осталось нераскрытым. National General узнала о втором, более крупном нарушении только в начале 2021 года после нескольких месяцев изысканий.

В иске утверждается, что это бездействие нарушает Закон штата Нью-Йорк о пресечении хакерских атак и улучшении безопасности электронных данных (SHIELD), который обязывает компании защищать личные данные и своевременно сообщать о нарушениях.

Генеральный прокурор Джеймс раскрыл National General за ее слабые методы обеспечения безопасности, заявив, что слабая защита от киберугроз позволила злоумышленникам дважды атаковать компанию в течение короткого периода. В иске требуется штраф в размере до 5000 долларов за нарушение.

Эрих Крон, специалист по повышению осведомленности в области безопасности в KnowBe4, подчеркнул риски, связанные с не уведомлением клиентов о нарушениях, заявив, что злоумышленники могут использовать украденные данные, чтобы выдавать себя за страховые компании и обманывать клиентов.

АДМИНИСТРАЦИЯ ТРАМПА РЕОРГАНИЗУЕТ CISA, СОКРАТИВ ШТАТ И ФИНАНСИРОВАНИЕ

Агентство по кибербезопасности и инфраструктуре США (CISA) претерпевает значительные изменения при новой администрации Трампа: контракты примерно с 300 сотрудниками были расторгнуты, а финансирование проектов по кибербезопасности в агентстве существенно сокращено.

«Департамент эффективности правительства (DOGE), возглавляемый Илоном Маском, сократил всю нашу команду red team и все вспомогательные должности — это затронуло более 100 человек. Спустя неделю DOGE сократил вторую команду red team CISA, также выполнявшую критически важную работу. В результате я и многие другие опытные операторы команды red team теперь ищем новые возможности», — сказал старший пен-тестер в CISA Кристофер Ченовет.

По данным компании CBS, этот раунд сокращений произошел через несколько дней после того, как в середине февраля DOGE потребовал уволить 130 сотрудников CISA, находящихся на испытательном сроке. Представитель CISA заявил прессе, что предполагаемые увольнения будут вызваны «проблемами с контрактами, а не увольнениями сотрудников». При этом он не смог конкре-

тизировать, сколько человек сейчас работает в красных командах CISA.

Как сообщил независимый журналист Эрик Геллер, CISA прекратила соглашение о сотрудничестве с Центром интернет-безопасности (CIS) на сумму 10 млн долларов. Партнерство предоставило CIS управление двумя центрами обмена информацией о киберугрозах (ISAC) — Центром обмена и анализа информации между штатами (MS-ISAC) и Центром обмена и анализа информации об избирательной инфраструктуре (EI-ISAC).

За несколько дней до сообщения Геллера на веб-сайте CIS было размещено уведомление о том, что организация больше не поддерживает EI-ISAC «из-за прекращения финансирования» Министерством внутренней безопасности, частью которого является CISA.

Наконец, президент США Трамп назначил Шона Планки на должность будущего директора CISA, согласно уведомлению на веб-сайте Конгресса США. Планки занимал различные должности в сфере кибербезопасности во время первой администрации Трампа, а также в Киберкомандовании США. Он также был главным информационным директором BMC США.

CISA И ФБР ПРЕДУПРЕЖДАЮТ О ВИРУСЕ-ВЫМОГАТЕЛЕ MEDUSA, КОТОРЫЙ МОЖЕТ НАНЕСТИ УЩЕРБ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЕ

Агентство по кибербезопасности и безопасности инфраструктуры (CISA), Федеральное бюро расследований (ФБР) и Центр обмена и анализа информации между штатами (MS-ISAC) выпустили совместный информационный бюллетень, в котором предупреждают, что операция по вымогательству Medusa затронула более 300 жертв в критически важных секторах инфраструктуры. Пострадавшие отрасли включают здравоохранение, образование, юриспруденцию, страхование, технологии и производство.

Medusa, вариант программы-вымогателя как услуги (RaaS), впервые выявленный в июне 2021 года, использует модель двойного вымогательства — шифрует данные жертвы, а также угрожает опубликовать извлеченные данные, если выкуп не будет выплачен.

Расследование ФБР показало, что злоумышленники Medusa получают первоначальный доступ через фишинговые кампании и эксплуатируют неисправленные уязвимости программного обеспечения. Попав в сеть, они используют легитимные административные инструменты, включая PowerShell и

Windows Management Instrumentation (WMI), чтобы избежать обнаружения, перемещаться по сети и развертывать полезные нагрузки ки-шифрования.

Аффилированные лица группы Medusa используют различные инструменты удаленного доступа, такие как AnyDesk, Atera и ConnectWise, для проникновения в сети. Они также используют передовые методы, чтобы избежать обнаружения, включая запутанные скрипты PowerShell, отключение систем обнаружения конечных точек и использование инструментов обратного туннелирования, таких как Ligolo и Cloudflared.

CISA предупредила, что особенно тревожным аспектом деятельности Medusa является ее тактика вымогательства. Жертвы оказываются под давлением и обязаны заплатить в течение 48 часов. В противном случае, участники Medusa сливают украденные данные на свой сайт в даркнете, предлагая их на продажу до истечения таймера обратного отсчета. Отчеты показывают, что даже после уплаты выкупа жертвы могут столкнуться с дополнительными требованиями вымогательства со стороны различных участников Medusa.

В рекомендациях ФБР и CISA настоятельно рекомендуется организациям внедрять меры по смягчению последствий, и предотвращению, чтобы не стать жертвой атаки, в том числе:

1. Поддержание программного обеспечения в актуальном состоянии и применение исправлений безопасности
2. Внедрение строгого контроля доступа и многофакторной аутентификации (MFA)
3. Мониторинг необычной активности и ограничение использования протоколов удаленного доступа
4. Внедрение сегментации сети для сдерживания потенциальных нарушений

Между тем эксперты критикуют CISA за ущербную манеру предупреждать людей о программах-вымогателях, которые распространяются с использованием социальной инженерии, вместо того чтобы предложить обучение по повышению осведомленности о безопасности. По их мнению, социальная инженерия задействована в 70–90 % всех успешных хакерских атак, что следует принимать в расчёт при выработке рекомендаций.

Несмотря на это, ФБР и CISA настоятельно призвали организации сообщать об инцидентах с вирусом-вымогателем Medusa в правоохранительные органы и воздерживаться от выплаты выкупов, поскольку это может спровоцировать дальнейшие атаки.

БРИТАНСКИЕ ВЛАСТИ ДАЛИ «ПРЕДУПРЕДИТЕЛЬНЫЙ ВЫСТРЕЛ» ПО НАРУШИТЕЛЯМ

Британский надзорный орган по защите данных предупредил, что новое расследование в отношении TikTok и других компаний в связи с использованием ими данных детей следует рассматривать как «предупредительный выстрел» для небольших цифровых компаний. Комиссар по информации Джон Эдвардс сделал это заявление на конференции IAPP Data Protection Intensive UK 2025, прошедшей на днях в Лондоне.

Он сказал, что организации всех размеров должны рассматривать последние расследования регулятора как «знак наведения порядка в собственном доме» и не ждать, пока он постучится в дверь, чтобы обеспечить соответствие бизнес-процессов законам о защите данных.

«Я хочу заявить предельно ясно. Сосредоточив наши усилия на некоторых из крупнейших и наиболее известных платформ, мы не даем небольшим компаниям зелёного света для принятия или продолжения незаконных практик, — сказал Эдвардс. — Все организации, использующие данные детей или предлагающие продукты или услуги, предназначенные для молодежи, должны соблюдать закон и следовать нашему Детскому кодексу».

Ссылаясь на новое исследование Управления комиссара по информации (ICO), Эдвардс заявил: почти половина британских родителей считают, что у них «практически нет контроля» над информацией, которую социальные сети и платформы для обмена видео собирают об их детях. Примерно столько же считают себя неспособными объяснить это детям.

«Дети не должны разбираться в этом самостоятельно. Это не их работа. Платформы, которые они используют, должны сделать эту информацию легкодоступной, — добавил Джон Эдвардс. — И мы вмешались, потому что наша работа как британского регулятора защиты данных — призвать эти платформы к ответу. Если социальные сети и платформы для обмена видео хотят получать выгоду от работы в Великобритании, они должны соблюдать закон о защите данных».

На прошлой неделе ICO объявило о своем расследовании в отношении TikTok, Imgur и Reddit. Согласно предупреждению ICO, «системы рекомендаций» на сайтах могут привести к тому, что уязвимым детям будет предоставлен ненадлежащий или вредный контент. Кроме того, в случае Imgur и Reddit ICO заявило, что рассмотрит, как платформы используют личную информацию детей и меры по контролю возраста.

РЕСПУБЛИКА УЗБЕКИСТАН

ОБЗОР ЗАКОНОДАТЕЛЬНОСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Александр
ВИНОГРАДОВ**
ФГУП «ЦНИИХМ»

Сергей МЕНЬШИКОВ
основатель Belarusian
InfoSecurity Community

Андрей СИТНОВ
независимый
эксперт

Наталья КАЗАНЦЕВА
независимый
эксперт

Следующее государство, анализ законодательства в области информационной безопасности (далее – ИБ) которого мы проведем, – Республика Узбекистан.

БАЗОВЫЕ ДОКУМЕНТЫ И ПОНЯТИЯ

Вопросы регулирования в области информации и доступа к ней, обеспечения защиты информации.

Конституцией Республики Узбекистан, Законом Республики Узбекистан от 24.04.1997 № 400-I «О гарантиях и свободе доступа к информации», Законом Республики Узбекистан от 12.12.2002 № 439-II «О принципах и гарантиях свободы информации» предусматривается право каждого человека на поиск, получение и распространение информации, регулируются отношения, возникающие в процессе реализации прав свободно и беспрепятственно искать, получать, исследовать, передавать и распространять информацию.

В частности, Законом Республики Узбекистан от 12.12.2002 № 439-II «О принципах и гарантиях свободы информации» раскрываются основные понятия:

♦ информация – сведения о лицах, предметах, фактах, событиях, явлениях и про-

цессах независимо от источников и формы их представления (различают открытую и гласную информацию, конфиденциальную информацию);

♦ защита информации – меры по предотвращению угроз информационной безопасности и устранению их последствий;

♦ информационная безопасность – состояние защищенности интересов личности, общества и государства в информационной сфере.

Информационная безопасность делится на следующие виды:

♦ информационная безопасность личности – создание необходимых условий и гарантий свободного доступа к информации, защиты тайны частной жизни, защиты от противоправных информационно-психологических воздействий;

♦ информационная безопасность общества – достигается путём обеспечения развития основ демократического гражданского общества, свободы массовой информации, недопущения противоправного информационно-психологического воздействия на общественное сознание, манипулирования им, сохранения и развития духовных, культурных и исторических ценностей общества, научного и научно-технического

ОБЩИЕ СВЕДЕНИЯ

Республика Узбекистан – государство, расположенное в центральной части Средней Азии. Сопредельные государства: на востоке – Кыргызстан; на северо-востоке, севере и северо-западе – Казахстан; на юго-западе и юге – Туркменистан; на юге – Афганистан, на юго-востоке – Таджикистан.

Столица – город Ташкент. Государственный язык на всей территории страны – узбекский, в Республике Каракалпакстан (наряду с узбекским) установлен свой государственный язык – каракалпакский.

Узбекистан является членом ООН, СНГ, Шанхайской организации сотрудничества, Организации исламского сотрудничества, Организации тюркских государств, Международной организации тюркской культуры.

потенциала страны, создания системы противодействия информационной экспансии;

- ♦ информационная безопасность государства — обеспечивается путём реализации мер экономического, политического, организационного и иного характера по противодействию угрозам безопасности в информационной сфере, защите государственных секретов и государственных информационных ресурсов от несанкционированного доступа к ним, интеграции в мировое информационное пространство и современные телекоммуникационные системы и другими направлениями.

Конфиденциальная информация — документированная информация, доступ к которой ограничивается в соответствии с законодательством.

Информация о персональных данных физических лиц относится к категории конфиденциальной информации и рассматривается в рамках информационной безопасности личности.

Защита информации заключается в защите любой информации, противоправное обращение с которой может причинить ущерб её собственнику, владельцу, пользователю и иному лицу.

Целями защиты информации являются: предотвращение угроз безопасности личности, общества и государства в информационной сфере, сохранение конфиденциальности информации, предотвращение её утечки, хищения, утраты, искажения и фальсификации информации.

РЕГУЛИРОВАНИЕ В СФЕРЕ ИНФОРМАТИЗАЦИИ

Регулирование вопросов в области информатизации, использования информационных ресурсов и информационных систем.

Эти вопросы регламентируются **Законом Республики Узбекистан «Об информатизации» от 11.12.2003 № 560-П.**

Закон раскрывает основные понятия:

- ♦ информатизация — организационный социально-экономический и научно-технический процесс создания условий для удовлетворения потребностей юридических и физических лиц в информации с использованием информационных ресурсов, информационных технологий и информационных систем;

- ♦ информационная технология — совокупность методов, устройств, способов и процессов, используемых для сбора, хранения, поиска, обработки и распространение информации;

- ♦ информационная система — организационно упорядоченная совокупность информационных ресурсов, информационных технологий и средств связи, позволяющая

осуществлять сбор, хранение, поиск, обработку и пользование информацией;

- ♦ блогер — физическое лицо, размещающее на своём веб-сайте и (или) странице веб-сайта во всемирной информационной сети Интернет общедоступную информацию общественно-политического, социально-экономического или иного характера, в том числе для её обсуждения пользователями информации.

ПРАВОВОЙ РЕЖИМ

Правовой режим информационных ресурсов и информационных систем определяется нормами, устанавливающими:

- ♦ порядок документирования информации, формирования информационных ресурсов и создания информационных систем;

- ♦ право собственности на информационные ресурсы и информационные системы;

- ♦ категории информационных ресурсов по уровню доступа к ним;

- ♦ порядок защиты информационных ресурсов и информационных систем;

- ♦ порядок межсетевых соединений информационных систем.

Информационные ресурсы по категориям доступа делятся на:

- ♦ общедоступные, предназначенные для неограниченного круга пользователей;

- ♦ ограниченного доступа, содержащие информацию о государственных секретах и конфиденциальную информацию или информацию, доступ к которой ограничен собственниками информационных ресурсов; также есть отдельная категория — информационные ресурсы, содержащие информацию о персональных данных физических лиц.

Порядок формирования и использования указанных ресурсов устанавливаются законодательством.

В Республике Узбекистан создана Национальная информационная система, которая включает в себя информационные системы государственных органов, отраслевые и территориальные информационные системы, а также информационные системы юридических и физических лиц.

Специальным уполномоченным органом является Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан. К его компетенции относятся вопросы:

- ♦ в области информатизации, электронного правительства, электронной коммерции, использования электронной цифровой подписи, телекоммуникаций и сфере почтовой связи;

- ♦ по созданию технологических условий для разработки и внедрения программных

продуктов на основе искусственного интеллекта.

Также Министерство по развитию информационных технологий и коммуникаций Республики Узбекистан является лицензирующим органом в сфере телекоммуникаций, рабочим органом Республиканского совета по радиочастотам, радиочастотным органом, органом, уполномоченным представлять Республику Узбекистан в Международном союзе электросвязи, Всемирном почтовом союзе и других международных организациях в области информационных технологий и коммуникаций.

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ

Регулирование вопросов в сфере обеспечения кибербезопасности, в том числе объектов критической информационной инфраструктуры.

Указанные отношения регулирует **Закон Республики Узбекистан от 15.04.2022 № ЗРУ-764 «О кибербезопасности»**.

Под кибербезопасностью понимается состояние защищённости интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве (виртуальной среде, созданной с помощью информационных технологий).

К объектам кибербезопасности относится комплекс информационных систем, используемых в деятельности по обеспечению киберзащиты информации и кибербезопасности национальных информационных систем и ресурсов, в том числе объекты критической информационной инфраструктуры.

Киберзащита представляет собой комплекс правовых, организационных, финансово-экономических, инженерно-технических мер, а также мер криптографической и технической защиты данных, направленных на предотвращение инцидентов кибербезопасности, выявление кибератак и защиту от них, устранение последствий кибератак, восстановление стабильности и надёжности деятельности телекоммуникационных сетей, информационных систем и ресурсов.

Данным законом также определены понятия критической информационной инфраструктуры (комплекс автоматизированных систем управления, информационных систем и ресурсов сетей и технологических процессов, имеющих важное стратегическое и социально-экономическое значение), объектов критической информационной инфраструктуры (системы автоматизации, применяемые в различных областях экономики).

Единую государственную политику в области кибербезопасности определяет Президент

Республики Узбекистан. Уполномоченным органом является Служба государственной безопасности Республики Узбекистан.

В отношении информационных ресурсов и систем государственных органов, информационных систем, включённых в категорию объектов критической информационной инфраструктуры, проводится экспертиза на соответствие требованиям кибербезопасности (в обязательном порядке или по инициативе субъектов кибербезопасности).

Аппаратные, аппаратно-программные и программные средства, применяемые для обеспечения кибербезопасности вышеуказанных ресурсов и систем, подлежат сертификации в обязательном порядке.

Объекты информатизации и объекты критической информационной инфраструктуры, категории которых определяются законодательством, подлежат аттестации и обязательной оценке.

Уделяется внимание инцидентам кибербезопасности, их расследованию, принятию мер в отношении киберинцидентов, раскрытию информации о них.

Также законом определены основные направления обеспечения кибербезопасности объектов критической информационной инфраструктуры, порядок их категорирования, ведения реестра объектов критической информационной инфраструктуры, основные права и обязанности субъектов критической информационной инфраструктуры, требования по обеспечению кибербезопасности, порядок создания системы обеспечения кибербезопасности и оценке кибербезопасности объектов критической информационной инфраструктуры.

В развитие указанного закона **Постановлением Президента Республики Узбекистан от 31.05.2023 № ПП-167 «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан»** утверждены:

Положение о порядке обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан, которым определяются основные понятия, принципы, направления обеспечения кибербезопасности, участники государственной системы обеспечения кибербезопасности объектов критической информационной инфраструктуры, уполномоченный государственный орган, его задачи и полномочия, права и обязанности субъектов критической информационной инфраструктуры, основы создания системы

кибербезопасности объектов критической информационной инфраструктуры;

Общие требования по обеспечению кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан, которые определяются **Приказом Председателя Службы государственной безопасности Республики Узбекистан от 04.09.2023 № 91, которым утверждено «Положение о порядке оценки уровня обеспечения кибербезопасности объектов кибербезопасности и объектов критической информационной инфраструктуры Республики Узбекистан».**

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Регулирование вопросов в области обработки персональных данных.

Данные вопросы регламентируются следующими основными законодательными и нормативно-правовыми актами Республики Узбекистан.

Закон Республики Узбекистан от 02.07.2019 № ЗРУ-547 «О персональных данных» определяет правовые основы обработки и защиты персональных данных, а также права и обязанности субъектов персональных данных и операторов баз персональных данных.

Персональными данными является зафиксированная на электронном, бумажном и (или) ином материальном носителе информация, относящаяся к определённому физическому лицу или дающая возможность его идентификации.

Законом определяются следующие субъекты:

- ♦ субъект персональных данных (субъект) — физическое лицо, к которому относятся персональные данные;
- ♦ оператор базы персональных данных (оператор) — государственный орган, физическое и (или) юридическое лицо, осуществляющее обработку персональных данных;
- ♦ собственник базы персональных данных (собственник) — государственный орган, физическое и (или) юридическое лицо, обладающее правом владения, пользования и распоряжения базой персональных данных;
- ♦ третье лицо — любое лицо, не являющееся субъектом, собственником и (или) оператором, но связанное с ними обстоятельствами или отношениями по обработке персональных данных.

В рамках закона выделяются:

- ♦ биометрические данные — персональные данные, характеризующие анатомические или физиологические особенности субъекта;

- ♦ генетические данные — персональные данные, относящиеся к унаследованным или приобретённым характеристикам субъекта, которые являются результатом анализа биологического образца субъекта или анализа другого элемента, позволяющего получить эквивалентную информацию;

- ♦ специальные персональные данные — данные о расовом или социальном происхождении, политических, религиозных или мировоззренческих убеждениях, членстве в политических партиях и профессиональных союзах, а также данные, касающиеся физического или душевного (психического) здоровья, сведения о частной жизни и судимости);

- ♦ общедоступные персональные данные — персональные данные, доступ к которым является свободным с согласия субъекта или на которые не распространяются требования соблюдения конфиденциальности;

Трудовой кодекс Республики Узбекистан (параграф «Защита персональных данных работника») предусматривает, что работодатель обязан совместно с представителями работников вырабатывать меры по защите персональных данных работников для обеспечения защиты персональных данных и предотвращения незаконного распространения;

Постановление Кабинета министров Республики Узбекистан от 05.10.2022 № 570 «Об утверждении некоторых нормативно-правовых актов в области обработки персональных данных», которым утверждены:

- ♦ Положение об определении уровней защищённости персональных данных при их обработке — предусматриваются обеспечение безопасности персональных данных при их обработке, установление уровней защищённости (четыре уровня) персональных данных при их обработке в зависимости от угроз безопасности (три типа угроз), требования по обеспечению уровней защищённости персональных данных;

- ♦ Положение о требованиях к материальным носителям биометрических и генетических данных и технологиям хранения таких данных вне баз персональных данных — предусматриваются порядок хранения биометрических и генетических данных на материальных носителях, их использования и учёта, требования к технологиям хранения биометрических и генетических данных вне баз персональных данных;

Приказ Министра юстиции Республики Узбекистан от 14.11.2023 № 19-мх «Об утверждении Типового порядка организации деятельности структурного

подразделения или уполномоченного лица собственника и (или) оператора базы персональных данных, обеспечивающего обработку персональных данных и их защиту», которым определяется порядок организации деятельности структурного подразделения или уполномоченного лица собственника и (или) оператора базы персональных данных, обеспечивающего обработку персональных данных и их защиту;

Приказ Министра юстиции Республики Узбекистан от 15.11.2023 № 20-мх «Об утверждении Типового порядка обработки персональных данных», которым определяется порядок обработки и защиты персональных данных, принципы, цели и условия обработки персональных данных, права и обязанности собственника и (или) оператора базы персональных данных.

ПОЛНОМОЧИЯ РЕГУЛЯТОРА

Регулятором в сфере защиты персональных данных является Государственный центр персонализации при кабинете министров Республики Узбекистан, обладающий следующими основными полномочиями:

- ◆ реализация государственной политики в области персональных данных;
- ◆ ведение Государственного реестра баз персональных данных;
- ◆ выдача свидетельства о регистрации базы персональных данных в Государственном реестре баз персональных данных;
- ◆ осуществление государственного контроля за соблюдением требований законодательства о персональных данных;
- ◆ определение необходимого уровня защищённости персональных данных;
- ◆ внесение обязательных для исполнения юридическими и физическими лицами предписаний об устранении нарушений законодательства о персональных данных;
- ◆ направление в государственные органы, уполномоченные в области обеспечения государственной безопасности, применительно к сфере их деятельности, установленные сведения;
- ◆ осуществляет сотрудничество с компетентными органами иностранных государств и международными организациями в области персональных данных.

БАНКОВСКАЯ СФЕРА

Регулирование информационной безопасности в банковской сфере.

Регулирование отношений в области получения, хранения, защиты, опубликования и предоставления сведений, составляющих банковскую тайну, осуществляется на осно-

вании **Закона Республики Узбекистан от 30.08.2023 № 530-II «О банковской тайне»**. Понятие банковской тайны данным законом немного шире аналогичного понятия, используемого в Российской Федерации. В частности, под понятие банковской тайны попадает информация об участниках накопительной пенсионной системы, размере и движении сумм пенсионных взносов, пенсионных накоплениях на индивидуальных накопительных пенсионных счетах граждан.

Отдельным **Законом Республики Узбекистан от 01.11.2019 № ЗРУ-578-сон «О платежах и платёжных системах»** регулируются отношения в области платежей и платёжных систем. Деятельность операторов платёжных систем в Узбекистане является лицензируемой, и для получения лицензии банк должен представить документ о политике безопасности, включая подробную оценку рисков, а также описание мер, обеспечивающих информационную безопасность, кибербезопасность и минимизацию рисков для обеспечения защиты пользователя платёжной услуги, включая риски мошенничества и незаконного использования конфиденциальных и персональных данных.

Вопросы защиты информации в автоматизированных банковских системах регулируются **Законом Республики Узбекистан от 04.04.2006 № ЗРУ-20-сон «О защите информации в автоматизированной банковской системе»**. В соответствии с данным законом собственник автоматизированной банковской системы обязан информировать собственника информации и пользователя автоматизированной банковской системы об особенностях методов обработки информации в автоматизированной банковской системе, а собственник информации и пользователь автоматизированной банковской системы обязаны подтвердить своё согласие на применение предложенных методов обработки и отсутствие претензий. Аналогичные нормы отсутствуют в российском законодательстве.

Надеемся, что данная статья поможет вам не заблудиться в законодательстве Республики Узбекистан. Мы постараемся облегчить путь изучения и применения на практике нормативных законов и подзаконных актов в области ИБ.

В следующем номере журнала мы продолжим обзор законодательства в области информационной безопасности других стран.

«ТАК ПОХОЖЕ НА РОССИЮ...»

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО В КИТАЕ



Мария КОЗЛОВА
корреспондент
BIS Journal, Пекин

Номинация «преступление года» в Китае по праву принадлежит телекоммуникационному мошенничеству. Преступник, вооружённый компьютерной техникой, благополучно обошёл своих «коллег» — серийных убийц, грабителей, воров, совершив около 40 процентов всех уголовных преступлений.

ГЛАВА I

Познакомимся со схемами, которые используются особым почётом в мошеннической среде Китая (и не только).

Схема № 1: «Здравствуйте, это я!». Раздаётся звонок. Потенциальная жертва берёт трубку и слышит вполне естественную, на первый взгляд, фразу: «Привет, узнаёшь?» Злоумышленник не представляется первым, а ждёт реакции человека, чтобы под неё подстроиться. После этого мошенник жалуется, что попал в беду, и просит срочно перевести деньги. Как только доверчивая жертва нажимает на кнопку «подтвердить оплату», её банковская карта мгновенно «обчищается». Такую схему мошенничества несложно распознать: например, китайские злоумышленники сами себя выдают, выставляя лисий хвост — акцент. Люди из разных провинций говорят на своих диалектах, поэтому многие, когда переходят на путунхуа (общепринятый разговорный язык), не в состоянии полностью скрыть акцент, а у жителей Поднебесной на него абсолютный слух. Они быстро делают вывод, что на другом конце телефона находится не земляк, а мошенник, и предотвращают преступление.

Схема № 2: «Троянский конь». В Китае активно используются троянские программы. Так, утром 26 июня 2023 года директор компании по фамилии Ши сообщил по сети WeChat бухгалтеру Лю, чтобы она перевела депозит за строительные работы компании R. Примерно в 13 часов госпожа Лю получила от пользователя «директор Ли компании R» запрос на авторизацию в WeChat и добавила его в контакты. «Директор Ли» сразу же создал в WeChat группу из трёх человек, включив в неё бухгалтера Лю и пользователя «директор Ши». Последний дал бухгалтеру указание оплатить перевод. Ничего не подозревающая госпожа Лю перевела 4,8 млн юаней на указанный в группе счёт. Настоящий директор Ши узнал об этой транзакции, только получив СМС-сообщение о списании средств. Выяснилось, что за день до этого бухгалтер открыла прикреплённый файл в сообщении с темой «Квитанция выписана, проверьте вложение». Этот файл был троянской программой, которая стала передавать злоумышленникам переписку по WeChat. Так мошенники узнали о планах настоящего директора Ши по оплате депозита.

Схема № 3: «Лжеполицейский». В августе 2023 года 13-летняя школьница по фамилии Ли получила сообщение с приглашением войти в группу по QR-коду, чтобы позвонить поп-кумиру. Как только девочка вошла в группу, там появился «полицейский Чжан», который объявил, что произошла утечка личных данных известного поп-исполнителя и все участники группы должны содействовать расследованию. Школьнице Ли был выделен «адвокат Чжао», который уговорил ребёнка для улаживания дела перевести 350 тысяч юаней на указанный им счёт, купить телефон Apple и отправить по указанному им адресу.

Схема № 4: «Зигзаг удачи». Злоумышленники могут избрать другую стратегию: массово разослать СМС, несущие «радостную весть» — поздравление с победой в розыгрыше. Для того чтобы получить упавший с неба автомобиль, катер или билет на круиз, нужно сначала уплатить подоходный налог, оплатить некоторые формальности и т.п.



Список платежей не заканчивается, платежи становятся крупнее, а до выплаты приза дело, естественно, никогда не доходит.

Схема № 5: «Откорм поросёнка». Широко распространены и фарминговые схемы, в которых жертва направляется на фиктивный сайт, имитирующий площадку для онлайн-торговли, приобретения услуг, операций с акциями и т.п. Китайское название таких схем — «откорм поросёнка». «Клиенту» сначала предоставляют возможность легко заработать небольшую сумму, а когда он переходит на игру по-крупному — отбирают всё.

В июле 2023 года госпоже Чжан из города Чунцин прислали карту с QR-кодом. Недолго думая, женщина отсканировала код и вошла в группу WeChat. Оказалось, что там выдавались задания на размещение заказов на специальной платформе, а за их выполнение полагались щедрые бонусы. Госпожа Чжан сделала 21 заказ за один день и заработала более 200 юаней. На следующий день женщина перечислила 300 юаней в организацию «Красный Крест» и получила бонус в 450 юаней. Стоимость заданий и бонусов быстро достигла пятизначных цифр. Когда госпожа

Чжан перевела 80 000 юаней, в службе поддержки ей сообщили, что операция была выполнена неправильно и транзакцию нужно сделать заново. Она повторила перевод много раз, но он никак не проходил. Средства же между тем списывались с её банковского счёта каждый раз. Общий ущерб составил 1,17 миллиона юаней.

Схема № 6: «Попросить ключи от квартиры, где деньги лежат». В декабре 2024 года госпоже Чэнь позвонили, представившись службой поддержки «Тиктока», по поводу якобы оформленной женщиной «миллионной» страховки. Мошенники разъяснили, что бесплатный период закончился и теперь нужно платить по 2000 юаней в месяц, причём спишется сразу сумма в 72 000 юаней за 3 года вперёд. По словам злоумышленников, было ещё не поздно отказаться от страховки, но для этого нужно было совершить целый ряд операций онлайн. Госпожа Чэнь не успевала за инструкциями «службы поддержки», и злоумышленники предложили быстро всё сделать через удалённый доступ к компьютеру. Через некоторое время госпожа Чэнь получила СМС-сообщение о списании 362 тысяч юаней с банковской карты, а

её пароль к личному кабинету банка уже не действовал.

Схема № 7: «Номера-грабители». Так же, как и в России, в Китае распространены номера-грабители. Звонит незнакомый номер, а когда человек пытается ответить, вызов сразу автоматически сбрасывается. Жертва, ничего не подозревая, перезванивает — и попадает на удочку. Когда приходит время оплачивать счета, человек с удивлением обнаруживает списание средств за «специальные услуги», иногда в несколько сотен юаней.

Схема № 8: «Мошенники-оборотни». 20 апреля 2023 года господин Го, владелец технологической компании в городе Фучжоу, получил от «друга» видеозвонок по сети WeChat. «Товарищ» сообщил, что ему срочно нужно перевести 4,3 млн юаней для участия в тендере от имени компании господина Го, так как она имела соответствующую лицензию. Видя лицо друга по видеосвязи и слыша его голос, бизнесмен ничего не заподозрил и сделал нужный перевод, не проверив номер счёта «друга». Об этом господин Го вскоре пожалел, ведь лицо и голос были заменены при помощи ИИ-технологий в режиме реального времени.

ГЛАВА II

Все виды схем, пожалуй, перечислять не будем, мошенники со всего мира перенимают их друг у друга, нисколько не гнушаясь пользоваться чужими «находками». Поэтому в «работе» мошенников Поднебесной существует как своя специфика, так и черты, свойственные злоумышленникам других стран.

К примеру, и в Россию, и в Китай мошенники звонят в основном из-за рубежа. Лишь малая часть кол-центров размещена на территории РФ — в основном в местах лишения свободы, а в КНР подобные преступные организации практически отсутствуют: жёсткое регулирование даёт о себе знать. Подавляющее количество мошеннических звонков приходит в Россию с Украины. После начала СВО украинский режим возвёл обман российских граждан в ранг государственной политики.

В Китай мошеннические звонки поступают из Мьянмы, в сознании жителей Поднебесной эта страна давно стала именем нарицательным для контрабанды наркотиков, торговли людьми и человеческими органами. После начала гражданской войны, вспыхнувшей в мае 2021 года, в стране начались беспорядки: центральная власть окончательно ослабла, во многих штатах власть оказалась в руках у криминальных сепаратистских группиро-

вок, которым подчинились и местные правоохранительные органы.

Именно это способствует беспрепятственной работе кол-центров, количество которых, как указывает кандидат юридических наук Я. О. Кучина в своей работе «Основные направления уголовной политики по борьбе с телекоммуникационными мошенничествами (скам-коллами) в КНР», достигает тысячи в пограничных с Китаем районах Мьянмы. Там работает приблизительно 100 тыс. сотрудников, причём значительная их часть является жертвами.

Согласно сведениям полиции Таиланда, число этнических китайцев, заманенных в Мьянму на заработки, достигает 70 тыс. человек в год. Как только искатели заработка прибывают в «землю обетованную», «работодатели» отбирают у них паспорта и телефоны — так недавно свободные граждане становятся «кули», то есть рабами. Преступники распределяют людей по кол-центрам и раздают им задания: например, за день привлечь трёх «клиентов». Если план не выполнен, несчастного жестоко избивают. У человека есть призрачная надежда вернуться на родину, если за него заплатят выкуп. Однако зачастую после получения денег похитители выдвигают новые требования. Тем не менее есть и счастливые случаи. К примеру, в 2024 году преступники, получившие откуп в 200 тыс. юаней, вернули 18-летнего хэнаньского юношу родителям, но только потому, что у молодого человека не хватало опыта, необходимого для работы.

Несмотря на то что пленников стерегут вооружённые надзиратели, многие решаются на побег. Единицы, которым удалось вернуться домой, сходятся в одном: лучше погибнуть от пули, чем оставаться в мьянманском аду. Однако сбежать не так просто: местная полиция всячески помогает «предпринимателям» из кол-центров вернуть ценные кадры. Схваченных беглецов жестоко избивают, часто до смерти. Если пленник остаётся жив, его сажают на несколько дней в водную темницу — трёхметровую яму под навесом, наполненную мутной зловонной канализационной жижей.

В целях пресечения трансграничного телекоммуникационного мошенничества китайское правительство начало кампанию по добровольному возвращению преступников в обмен на снижение наказания. Для тех подозреваемых, кто отказался вернуться с повинной в Китай, были введены следующие меры наказания:

- ♦ аннулирование прописки;



- ◆ заморозка банковских счетов;
- ◆ блокировка сим-карт и запрет на банковское и телекоммуникационное обслуживание в течение 5 лет;
- ◆ запрет на передвижение на самолётах и скоростных поездах;
- ◆ аннулирование загранпаспортов;
- ◆ снос домов, построенных на незаконно полученные доходы.

Последняя мера зачастую означала, что родственники подозреваемых оказывались на улице. Сёла (общины), в которых был прописан хотя бы один из подтверждённых мошенников, лишались всех государственных субсидий.

Разъяснительная работа велась с оставшимися на родине родственниками, которые, в свою очередь, сообщали подозреваемым о сложившейся ситуации. Между низовым местным руководством (сёл и общин) и полицией было организовано своего рода соревнование. Руководителям недвусмысленно дали понять, что если их родственники занимаются телефонным мошенничеством из-за рубежа, то они должны в кратчайшие сроки убедить преступников вернуться. Если же полиция успевала установить вину до явки мошенников с повинной, то в отношении местного руководства автоматически открывалось расследование в укрывательстве,

и дело передавалось в уездные дисциплинарный и контрольный комитеты Компартии.

Местное руководство несло ответственность и за деяния односельчан. Если изобличался один телеком-мошенник из числа жителей села (общины), руководителям объявлялся выговор. Если же число задержанных достигало двух и более, то глава села (общины) и секретарь парторганизации освобождались от занимаемых должностей. О новой политике было объявлено на конференции с довольно витиеватым названием «Собрание по поводу клятвы «Стодневной борьбы» по искоренению организованной преступности и наведению порядка на малой родине тех, кто занимается телекоммуникационным мошенничеством из-за рубежа». Эта кампания принесла плоды: только с апреля 2021 по июль 2022 года 230 тыс. подозреваемых вернулись в Китай с повинной.

Позже правительство КНР перешло к организации полицейских операций за рубежом, ключевую роль в этом сыграло укрепление международного сотрудничества. К примеру, с 28 по 29 августа 2023 года в Пекине состоялось Семнадцатое совещание на ведомственном уровне по реализации Соглашения об управлении границей и сотрудничестве между Китаем и Мьянмой. Стороны договорились об упрощении процедур сотрудни-

чества при расследовании преступлений и передаче подозреваемых из Мьянмы на территорию КНР. Теперь экстрадиция будет занимать всего лишь несколько дней.

Кроме того, 16 августа 2024 года главы МИД Китая, Лаоса, Таиланда и Мьянмы обсудили вопросы по борьбе с трансграничной преступностью на неформальной встрече, которая проходила в городе Чиангмае (Таиланд). По словам министра иностранных дел КНР Ван И, для того чтобы преодолеть высокий уровень преступности, нужно прибегнуть к совместным усилиям стран региона. Страны договорились укреплять взаимное сотрудничество и поддерживать более тесную координацию усилий по борьбе с телекоммуникационным мошенничеством, азартными онлайн-играми, контрабандой наркотиков и торговлей людьми.

С сентября 2023 года по начало 2024 года благодаря общим усилиям властей КНР, Таиланда, Лаоса и Мьянмы были успешно проведены операции против кол-центров. Так, только за неполных три месяца (по состоянию на 21 ноября 2023 года) из Мьянмы в КНР было экстрадировано более 31 тыс. подозреваемых в телекоммуникационном мошенничестве, задержанных во время данных рейдов.

ГЛАВА III

В 2022 году был принят «Закон КНР о противодействии мошенничеству в телекоммуникационных сетях». Статья 3 Закона гласит, что он применяется для борьбы против телеком-мошенничества, которое совершено на территории КНР или гражданами КНР за пределами территории Китая. Таким образом, Закон действует в том числе против иностранных граждан и организаций, если ущерб причинён на территории КНР; а если преступники имеют гражданство КНР, то действие Закона распространяется на них вне зависимости от места незаконного присвоения имущества.

Статья 6 гласит, что Госсовет КНР (аналог правительства) создаёт специальный рабочий механизм по борьбе с телекоммуникационным мошенничеством и осуществляет планирование и координацию его работы, а местные правительства создают аналогичные местные механизмы. Это показывает, что руководство страны уделяет данной проблеме исключительное внимание.

Статьи 6 и 9 обязуют операторов связи и банков создавать системы предотвращения рисков телеком-мошенничества, а также регистрировать реальные имена пользователей.

Пользователям, «вовлечённым» в мошенничество (так обозначают лиц, не принимавших непосредственное участие в преступлении, но на которых, например, были оформлены сим-карты, фигурирующие в деле), могут ограничить действие их сим-карт и отказать в выдаче новых.

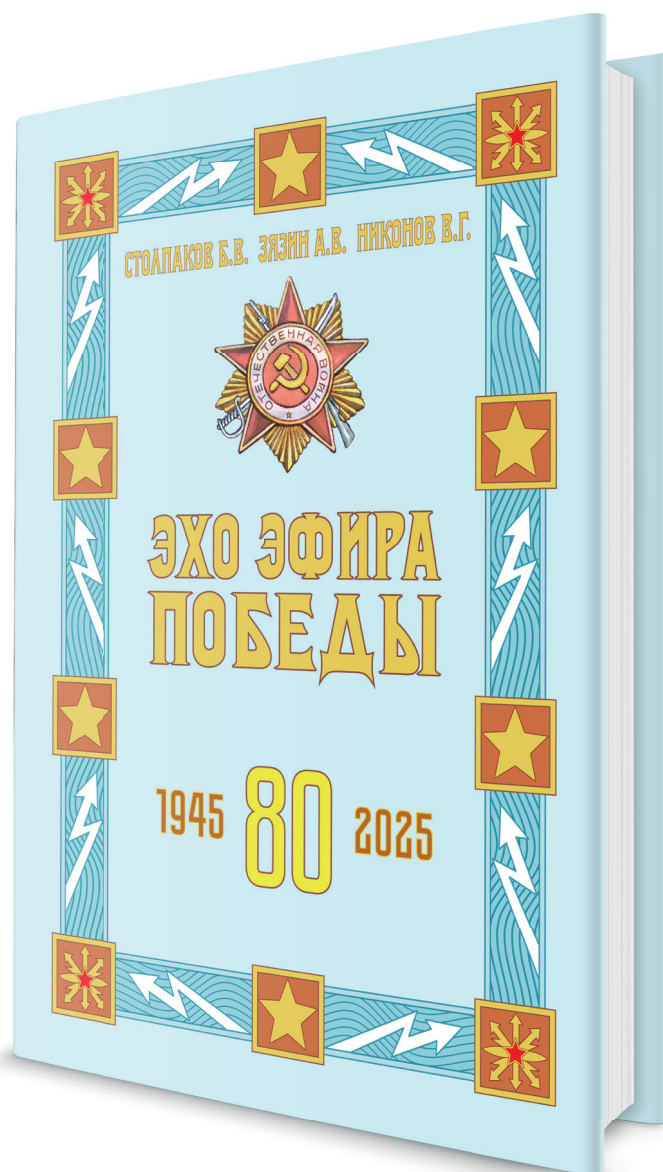
Статья 13 предписывает операторам связи обеспечивать отображение реального телефонного номера и отслеживать источник его подмены. Статья 14 запрещает производство и торговлю оборудованием и ПО для подмены номера, вставки большого количества сим-карт, незаконного входа из интернета в телеком-сеть для массового получения и заполнения верификационных кодов и другим, используемым в мошеннической деятельности. Операторы связи должны сообщать о фактах обнаружения такого оборудования органам безопасности.

Статья 25 запрещает продажу и предоставление личных данных, отмывание денег при помощи криптовалюты и любую иную помощь лицам, осуществляющим телеком-мошенничество. Операторы связи и интернет-провайдеры должны проявлять разумную предусмотрительность, стремясь исключить предоставление таким лицам соответствующих услуг. Такие расплывчатые формулировки, как «иная помощь», делают возможным привлечение к ответственности большего круга лиц и воспитывают у бизнеса практику самостоятельной проверки связи своих партнёров с телекоммуникационным мошенничеством.

Статья 36 разрешает органам иммиграции отказывать в выезде гражданам КНР в страны, где отмечен высокий уровень телеком-мошенничества. Эти государства не указаны в Законе; по некоторым данным, это Камбоджа, ОАЭ, Филиппины, Таиланд, Мьянма, Лаос, Малайзия, Турция и Индонезия.

Статьи 39–43 устанавливают ответственность физических и юридических лиц за нарушение Закона в виде штрафа до 5 млн юаней.

Работа китайских законодателей, дипломатов и правоохранительных органов принесла свои результаты. За период с августа по декабрь 2023 года количество телеком-мошенничеств снизилось на 29 % по сравнению с аналогичным периодом предыдущего года, а за январь – июль 2024 года – на 24 %. Изучение китайского опыта в этой сфере, безусловно, важно и полезно, однако ситуация в России отличается тем, что в нашем случае полицейские операции неприменимы – снижение телеком-преступности наступит только после успешного завершения СВО.



«ЭХО ЭФИРА ПОБЕДЫ»

В ЧЕСТЬ 80-ЛЕТИЯ ПОБЕДЫ МЕДИА ГРУППА
«АВАНГАРД» ВЫПУСТИЛА КНИГУ

Книга «Эхо эфира Победы» на основе рассекреченных в 2000-х годах архивных материалов и воспоминаний ветеранов Великой Отечественной продолжает знакомить читателей с малоизвестными страницами истории Второй мировой войны – деятельностью шифровальщиков и связистов, криптографов и радиоразведчиков. Роль этих направлений деятельности в достижении Победы осмысливается по-новому. Книга адресована широкому кругу читателей. Издание подготовлено с использованием результатов проектов Фонда содействия развитию безопасных информационных технологий (ФСРБИТ) «Криптографический фронт» и «Криптографический фронт: виртуальный музей» 2018–2022 гг.

BIS Journal попросил представить книгу одного из пионеров отечественной ИБ, ровесника Победы Владимира Георгиевича Матюхина.



Владимир МАТЮХИН
генерал армии, доктор
технических наук,
действительный член
Академии криптографии
России

Книга «Эхо эфира Победы»¹ не может не привлечь внимание любого, кто интересуется историей военной связи в России, прикладной криптографии и радиоразведки, наиболее впечатляющие события которой состоялись в период Великой Отечественной войны.

Этот исторический период выбран для раскрытия указанных тем не случайно. Хотя развитие технологий радиосвязи, борьба между защитой информации и ее дешифровкой не прекращались большую часть XX века, противостояние в период 1939–1945 гг. представляет одну из наиболее ярких страниц истории. Именно в годы Великой Отечественной заложенная в предыдущие десятилетия научная база, а также накопленный опыт, инженерный талант и самоотверженный труд наших специалистов позволили в судьбоносное для страны время реализовать ряд прорывных идей, которые сыграли весомую роль в ходе крупнейших сражений и военных операций.

Эти научные идеи и технологии позволили сохранить в годы войны тысячи жизней советских солдат и мирных жителей, обеспечить уничтожение боевых частей и техники врага, облегчить планирование военных операций и оперативное командование нашими войсками. С этого периода не только в нашей стране, но и во всем мире пришло осознание огромного значения защиты связи в важнейших областях жизни — в государственном управлении, международных отношениях и особенно военном деле.

Внимание коллектива авторов к периоду Второй мировой войны объясняется и ещё одной целью. Они ставят перед собой и с успехом выполняют задачу донести до широкого круга читателей многообразные заслуги отечественных учёных и инженеров, изобретателей и организаторов, военных связистов, шифровальщиков и даже метеорологов. В книге показан вклад этих людей в ключевые события Великой Отечественной — Сталинградская и Курская битвы, снятие блокады Ленинграда, Тегеранская, Ялтинская и Потсдамская конфе-

ренции, и также в ход менее известных, но знаковых военных операций.

Следует отметить, что это не первое подобное издание авторов. В 2016 году был опубликован исторический труд «Чтоб было в тех землях не знатно...», в котором подробно и ярко описаны важнейшие события давно минувших дней и персоналии, заложившие основы применения криптографии в российском государстве. А в 2023 году появилась книга «Сталинград и криптографический фронт», посвящённая одному из тяжелейших и судьбоносных сражений Второй Мировой войны. В ней в популярном изложении были представлены результаты тщательной и ответственной работы авторов с историческими документами и специализированной литературой.

Новая книга продолжает и развивает использованный авторами ранее подход. С одной стороны, она фокусируется на предмете проведенных исследований с изложением большого объема конкретных фактов и документов, прежде скрытых в архивах и на страницах специализированных трудов. Вместе с тем увлекательный рассказ раскрывает исторический контекст эпохи, знакомит читателя с удивительными фактами о ключевых событиях в области криптографии, случившихся перед началом и во время Великой Отечественной войны.

Наконец, выделена и развёрнуто описана роль ряда замечательных учёных и педагогов, изобретателей и организаторов, военных командиров, которые были по достоинству отмечены государственными премиями и воинскими наградами за победы на криптографическом фронте Великой Отечественной войны. С почтением описываются заслуги Б. А. Аронского, И. Т. Пересыпкина, В. А. Котельникова и других выдающихся личностей, которые оживают на страницах книги в ореоле своих деяний.

Интересны читателю будут и приводимые авторами документальные материалы — карты, шифровальные таблицы, свидетельства очевидцев. Они не только оживляют книгу, но и позволяют погрузить читателя в подлинную атмосферу того времени со всеми ее достоверными деталями.

В завершение хотелось бы выразить надежду, что книга окажется полезной не только специалистам, интересующимся вопросами связи и защиты информации, прикладной криптографии в контексте Великой Отечественной войны, но и позволит массовому читателю приумножить память о подвигах русского народа. Отголоски победных салютов того времени гремят и в наши дни, и новое издание — отличный подарок к 80-летию юбилею великой Победы.

¹ Столпаков Б. В., Никонов В. Г., Зязин А. В. «Эхо эфира Победы» / М.: Медиа Группа «Авангард», 2025. — 344 стр.

ПОБЕДУ ПРИБЛИЖАЛИ КАК МОГЛИ И ЗА ЦЕНОЙ НЕ СТОЯЛИ

ВЕЛИКАЯ ОТЕЧЕСТВЕННАЯ В ДОКУМЕНТАХ...



Борис СТОЛПАКОВ
историк криптографии

Документальные свидетельства прошлого всегда интересны и притягательны. Особенно это относится к документам Великой Отечественной войны, массовое рассекречивание которых началось в 2007–2009 годах. Среди документов, запечатлевших будни фронтовой связи и шифровальной службы, присутствуют редкие свидетельства начального периода войны — лета и осени 1941 г. Их мало, и они особенно ценны.

«ОТЧЁТ ПО ШИФРОВАЛЬНО-ШТАБНОЙ СЛУЖБЕ...»

О состоянии шифровальной работы в боевых авиационных частях в первые дни войны даёт представление Отчёт по шифровально-штабной службе 125 СБАП (скоростного бомбардировочного авиаполка) с 22 июня по 5 июля 1941 г. (илл. 1). Там отмечено:

«Обеспеченность полка основными документами СУВ (скрытного управления войсками — авт.) была. Однако для передачи оперативных и боевых распоряжений не были разработаны переговорные таблицы, следовательно, передача происходила открыто по телефону, например: сколько готово самолётов к вылету, сколько требуется горючего <...> Только в деревне Церковье 1.7.41 была получена переговорная таблица для связи полка с дивизией. Переговорная таблица полностью не охватывала боевые распоряжения, поэтому набор отдельных слов и фраз производился по буквам. Общевоинской командирский код «ЗОКК-40» совершенно не применялся, не было ключей для таблиц.

Шифрсвязь штаба полка со штабом дивизии применялась с 22.6.41 до 28.6.41 только на постоянных

аэродромах, за этот период передано всего четыре шифртелеграммы, дальнейшее применение шифрсвязи прекратилось за отсутствием телеграфа и радиостанции <...> Рации для применения шифрсвязи за период военных действий совершенно не применялись.

Воздушные авиационные коды «ВАК-40» были выданы экипажам для ЛТУ (лётно-тактических учений — авт.) 22.6.41, с которыми впоследствии полк произвёл боевой вылет. За период с 22.6 по 26.6.41 не было возвращено 16 кодов, которые были уничтожены командирами экипажей при вынужденных посадках и не возвратившимися экипажами. Утерь документов СУВ, кроме указанных кодов, не было».

125 СБАП накануне ВОВ размещался в Могилёвской области Белоруссии и имел 66 самолётов. В середине июля 1941 г. полк вывели в тыл с семью исправными машинами на пополнение.

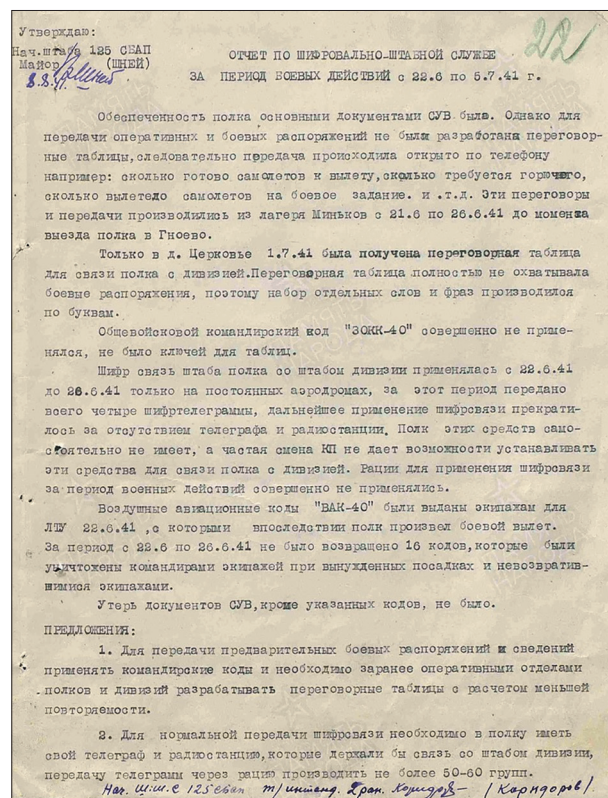


Иллюстрация 1. Отчет по шифровально-штабной службе за 22.6–5.7.41 г.

«НЕМЕДЛЯ ЭВАКУИРОВАТЬСЯ...»

В середине октября 1941 г., как известно, сложилось тяжелейшее положение под Москвой: в окружение попали сразу четыре армии, включавшие и дивизии, сформированные на основе московского ополчения. Не только тревогу, но и готовность к решительным действиям передаёт принятое тогда постановление ГКО «Об эвакуации столицы СССР г. Москвы».

В. А. Котельников вспоминал, что при приближении фронта к Москве ЦНИИС Наркомата связи, где он трудился, был распущен, а все сотрудники уволены. Оставили только его лабораторию, поскольку там велись работы по закрытой радиотелефонии, так необходимой для фронта. Им было поручено получить деньги и расплатиться со всеми уволенными сотрудниками института. Затем следовало сжечь всю документацию, кроме самой важной, и подготовить оборудование лаборатории к эвакуации в Уфу.

33-Я АРМИЯ НАЧАЛА НАСТУПЛЕНИЕ

Неожиданное для немцев декабрьское контрнаступление Красной армии под Москвой переросло в её январское наступление. Эти боевые действия, получившие название Ржевско-Вяземской операции, длились до середины апреля. Главная роль в них принадлежала 33-й армии генерала М. Г. Ефремова. Именно его войска, отразив к 5 декабря попытку прорыва немцев к Москве на Нарофоминском шоссе, перешли в победное контрнаступление на Нарофоминском направлении.

В первых числах января 1942 г. 33-я армия начала наступление на Вязьму. Главной ударной силой армии считалась 338-я стрелковая дивизия. Как известно, зимнее наступление под Москвой значительно улучшило положение советских войск, но для 33-й армии исход боёв под Вязьмой стал тяжёлым.

На 5.1.42 (илл. 3): «На правом фланге и центре положение частей без изменений. Противник ведёт редкий миномётный огонь по боевым порядкам частей. 338 с.д. в движении на Ивановская, 201 с.д. и 103 с.д. — положение без изменений <...> В Федорено обнаружено скопление пехоты противника до 100 человек с одним орудием и пятнадцатью пулемётами».

ПЕРВЫЕ ПРИЗНАКИ БУДУЩЕГО ПЕРЕЛОМА НА КРИПТОГРАФИЧЕСКОМ ФРОНТЕ

1942 г. принёс не только надежды и радость зимних побед, но и горечь летнего отступления к Сталинграду.

Вместе с тем 18 августа 1942 г. было принято постановление ГКО «Об обеспечении фронтовых правительственных связей специальной аппаратурой для телефонных и радиотелефонных раз-

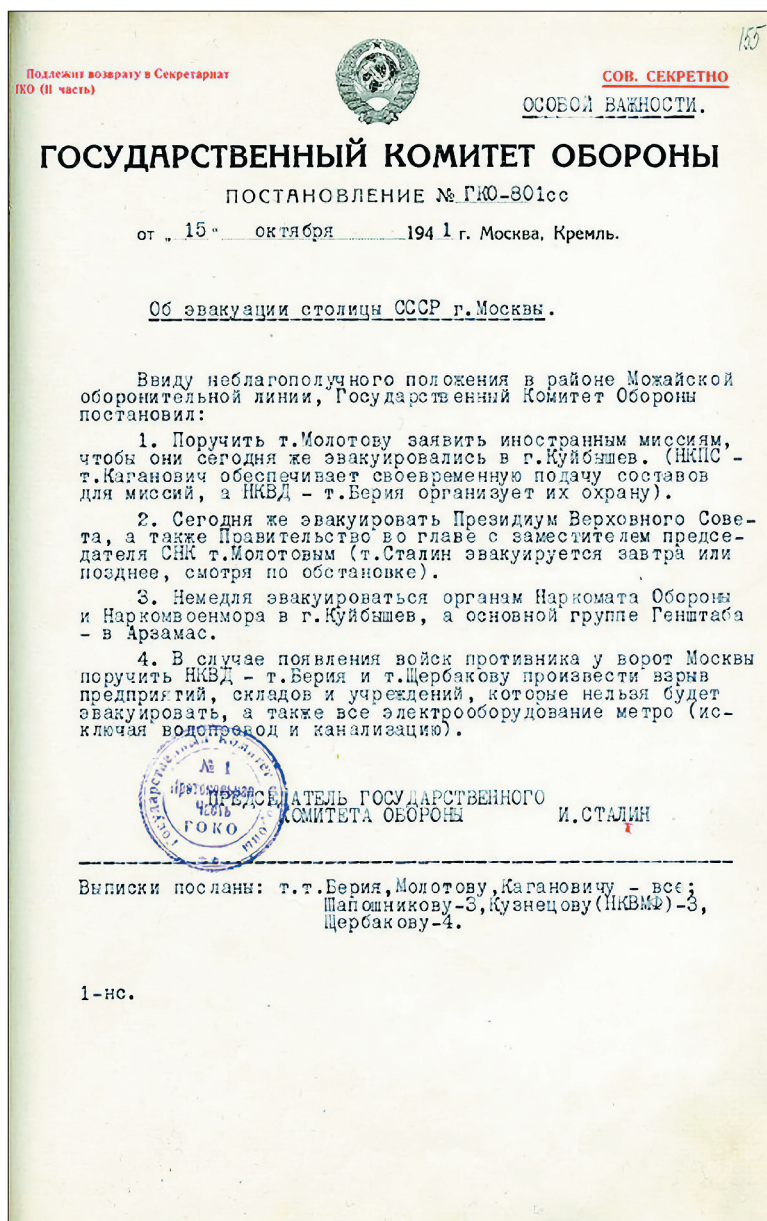
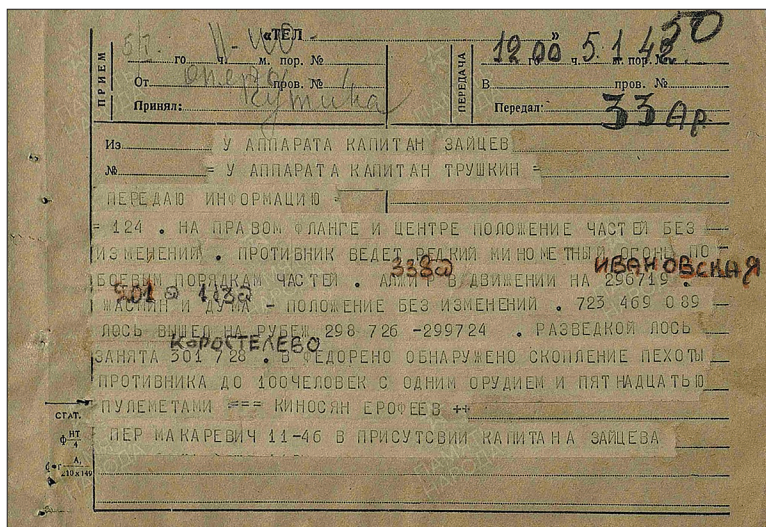


Иллюстрация 2. Постановление ГКО об эвакуации г. Москвы



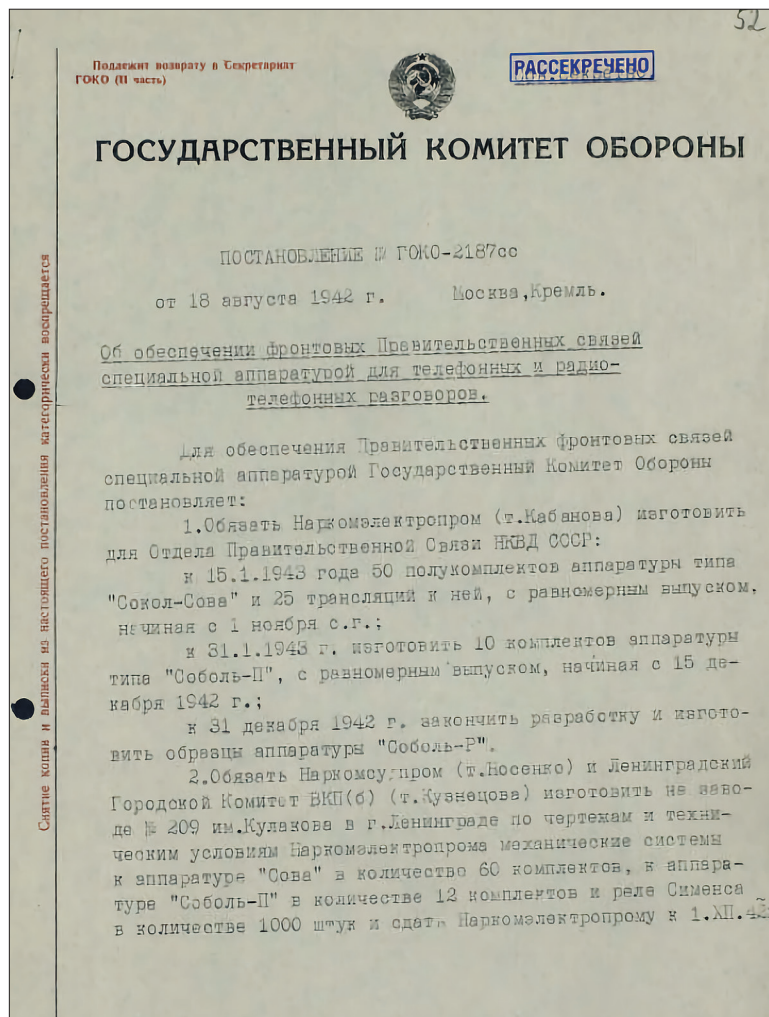


Иллюстрация 4. Постановление ГКО о специальной аппаратуре связи

говоров», обязывающее завершить разработку и начать производство аппаратуры уже к середине декабря (илл. 4).

Образцы аппаратуры «Соболь-П» получили боевое крещение уже в конце 1942 г. на радиолинии, восстановившей связь Москвы с Закавказьем. Закавказский фронт тогда имел исключительно важное значение. Он обеспечивал безопасность поставок грузов от союзников через Иран и Туркестан, по южному маршруту ленд-лиза. Кроме того, в портах Грузии базировался Черноморский флот, не позволявший румынским танкерам доставлять нефтепродукты на Кубань напрямую по Чёрному морю. Вызывает восхищение способность разработчиков во главе с В. А. Котельниковым, производственников и связистов, преодолев все трудности, за год создать сложнейшую, превосходящую мировые разработки аппаратуру и поставить её на боевую связь.

ВЕСТИ С «ОСТРОВА ЛЮДНИКОВА»

К концу октября защитники Сталинграда удерживали лишь небольшую часть его территории —

2 км берега в длину и, местами, всего 100 метров в глубину фронта. 9 ноября резко похолодало, сразу до 18 градусов мороза. Льдины на Волге сильно затруднили доставку пополнений и боеприпасов. В результате начатого тогда наступления немецких войск им удалось 11 ноября разделить оборону армии В. И. Чуйкова на три изолированных друг от друга плацдарма. Первый из них — в центральной части Сталинграда, с «домом Павлова» и восточными склонами Мамаева кургана. Чуть севернее — второй, самый малый, названный «островом Людникова». Третий плацдарм — севернее тракторного завода. Вот фрагмент боевого донесения по радиосвязи из 138-й дивизии, с «острова Людникова», от 17 ноября:

«В течение дня противник продолжает накапливаться в районе восточной части завода Баррикады <...> Каждый день дивизия несёт большие потери. Помощь, оказываемая самолётами, слишком мизерна. Количество раненых очень большое, каждый день — смертность, продовольствия нет, патронов ППШ нет. Кормить людей нечем, перевязочных материалов нет. Питание радиостанции на исходе, через сутки потеряю связь штабром. Прошу Ваших срочных мероприятий, обеспечивающих положенный план снабжения. Людников» (илл. 5).

До победного контрнаступления Красной армии под Сталинградом тогда оставалось всего два дня. Весь мир оценил его итог как начало перелома во Второй мировой войне. Победа в Курской битве в июле-августе 1943 г. сделала этот перелом необратимым.

«ПЕРЕПРАВА, ПЕРЕПРАВА, БЕРЕГ ЛЕВЫЙ, БЕРЕГ ПРАВЫЙ...»

В сентябре 1943 г. Красная армия с боями всё ближе подвигалась к Днепру. Фельдмаршал Э. Манштейн, командовавший отступавшей немецкой группой армий «Юг», так описал в мемуарах сложившуюся обстановку: «В зоне 20–30 км перед Днепром было разрушено, уничтожено или вывезено в тыл всё, что могло помочь противнику немедленно продолжить своё наступление на широком фронте по ту сторону реки, то есть всё, что могло явиться для него укрытием или местом расквартирования, и всё, что могло обеспечить его снабжение».

СТАВКА ВЕРХОВНОГО ГЛАВНОКОМАНДОВАНИЯ СЧИТАЕТ НЕОБХОДИМЫМ...

Предполагая тяжёлые бои за переправы и неизбежные потери, Ставка Верховного Главнокомандования 9 сентября 1943 г. издала приказ Военным Советам фронтов и армий, в котором говорилось:

«В ходе боевых операций войскам Красной армии приходится и придётся преодолевать много

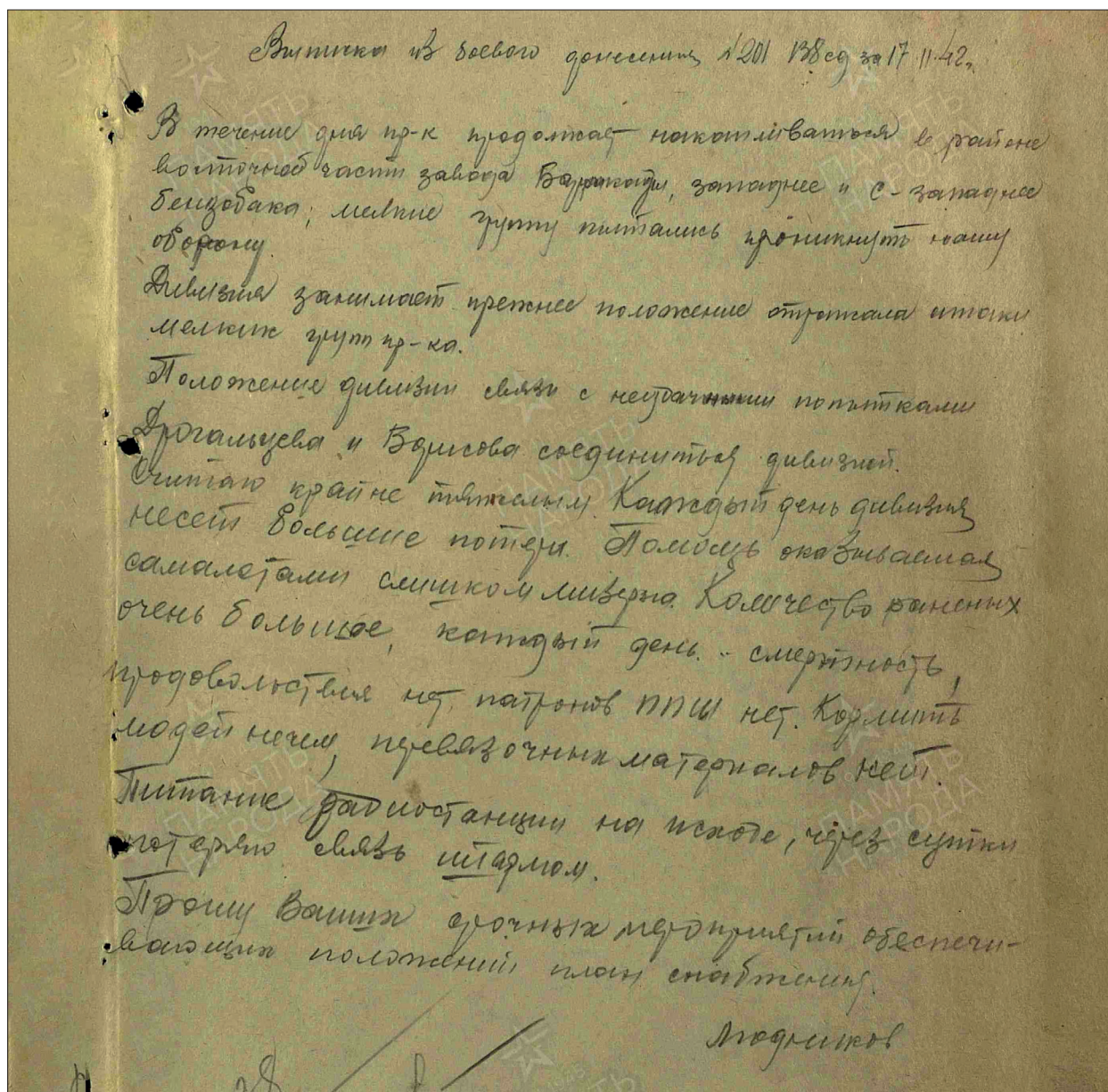


Иллюстрация 5. Донесение И.И.Людникова

водных преград. Быстрое и решительное форсирование рек, особенно крупных, подобных реке Днепр, будет иметь большое значение для дальнейших успехов наших войск.

В связи с этим Ставка Верховного Главнокомандования считает необходимым довести до сведения командующих армиями, командиров корпусов, бригад, полков, понтонных и инженерных батальонов, что за успешное форсирование крупных речных преград и закрепление за собой плацдарма для дальнейшего развития наступления, командиры названных соединений и частей должны представляться к высшим правительственным наградам. За форсирование такой реки, как река Днепр в районе Смоленска и ниже, и равных Днепру рек по трудности форсирования командиров соединений и частей представлять к присвоению звания Героя Советского Союза».

БИТВА ЗА ДНЕПР ДЛИЛАСЬ ТРИ МЕСЯЦА

Битва за Днепр началась 22 сентября и длилась три месяца (22.9–23.12): в боях на фронте длиной 750 км с советской стороны участвовали 41 армия, из них четыре танковых и одна воздушная. Первыми к Днепру подошли войска Воронежского фронта, 20 октября переименованного в 1-й Украинский.

Как известно, первые попытки переправ, не поддержанные отставшими артиллерией и авиацией, привели к тяжёлым потерям.

Виктор Петрович Астафьев, участник тех событий, оставил своё свидетельство:

«...Почти все понтоны с бойцами, батальонными миномётами и сорокапятками были на воде разбиты и утоплены, однако чудом каким-то, не иначе, словно по воздуху, некоторым подразделениям удалось добраться до берега, уцепиться за

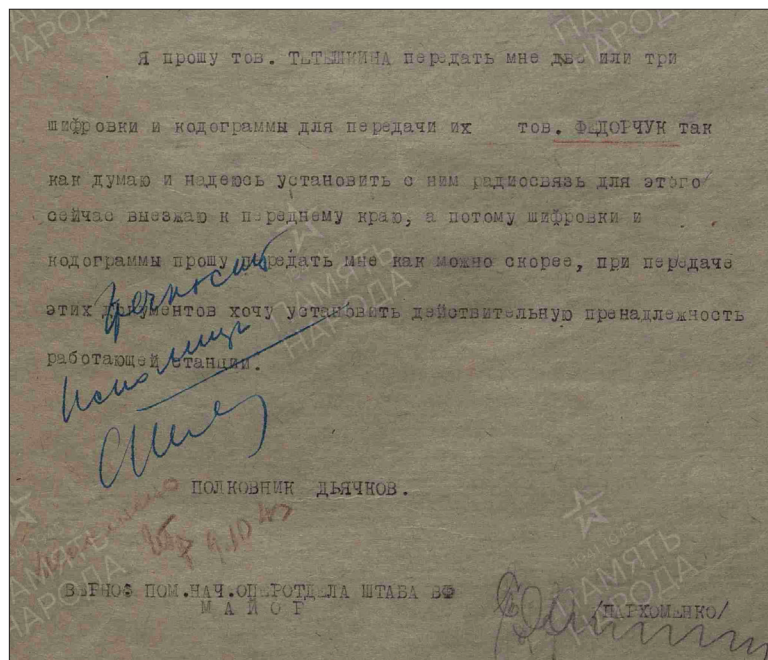


Иллюстрация 6. Обращение полковника Дьяčkова



Иллюстрация 7. Орден «Победа»

него и вслед за разрывами снарядов и мин продвинулись вперед, минуя осыпистый яр».

СРОЧНЫЙ ЗАПРОС

Понятно, что на левом берегу с надеждой ждали любой весточки с правобережья, особенно радио-сообщений. Напряжение той обстановки заметно и в документе фронтовой переписки, приведённом здесь (илл. 6).

«Я прошу тов. Тытышкина передать мне две или три шифровки и кодограммы для передачи их тов. Федорчук, так как думаю и надеюсь установить с ним радиосвязь, для этого сейчас выезжаю к переднему краю, а потому шифровки и кодограммы прошу передать мне как можно скорее, при передаче

этих документов хочу установить действительную принадлежность работающей станции.

Полковник Дьячков»

Сообщение зарегистрировано в оперативном отделе штаба Воронежского фронта 9.10.43. На документе имеются также надписи: «Срочность. Исполнить». «Исполнено 9.10. 43 г.».

АУТЕНТИФИКАЦИЯ — НАСУЩНАЯ ФРОНТОВАЯ ЗАДАЧА

Из содержания документа следует, что полковник Дьячков собрался решать задачу аутентификации, то есть проверки подлинности источника сообщений, обозначенного как Федорчук.

Конечно, хочется надеяться, что полковник Дьячков решил свою задачу положительно. А поддержкой такого предположения можно считать неоспоримый факт: красноармейцы сумели закрепиться на 23 относительно крупных плацдармах правого берега Днепра.

На документе видна пометка красным карандашом: «47 А». Ныне известно, что бойцы 47-й армии смогли форсировать Днепр и закрепиться на двух плацдармах уже 25 сентября. 29 сентября на правый берег был перенесён командный пункт 23-го стрелкового корпуса 47 А. Причём командиру корпуса генерал-майору Н. Е. Чувакову пришлось завершать свою переправу вплавь.

В ту позднюю осеннюю пору переправы бойцов на правобережье упорно продолжались, пока это было необходимо.

«БОЙ ИДЁТ СВЯТОЙ И ПРАВЫЙ...»

Александр Трифонович Твардовский:

«Было так: из тьмы глубокой, огненный взметнув клинок,
Луч прожектора протоку пересёк наискосок.
И столбом поставил воду вдруг снаряд. Понтон — в ряд.
Густо было там народу — наших стриженных ребят...
Переправа, переправа! Пушки бьют в крошечной мгле,
Бой идёт святой и правый, смертный бой не ради славы,
Ради жизни на земле».

Особое значение в боях за Днепр придавалось освобождению Киева. Войска Красной Армии заняли город 6 ноября 1943 г. «Занятие Киева советскими войсками является победой, имеющей огромное не только военное, но и моральное значение... Германия слышит звон похоронного колокола. На неё надвигается лавина», — так заявило своим слушателям британское радио.

И уже 8 ноября властными указами были учреждены орден «Победа» для награждения полководцев и солдатский орден Славы. Это произошло за 18 месяцев до победного мая 1945 г. (илл. 7).

Битва за Днепр завершилась в конце декабря 1943 г. По её итогам было подписано 2438 представлений на звание Героя Советского Союза, это без малого четверть всех присвоений геройского звания в годы Великой Отечественной войны.



Защита организации
от сложных и целевых
атак

Kaspersky Anti Targeted Attack

с модулем NDR

ЗАВЕТНЫЕ 0,1 %

ЗАМЕТКИ БЕЗОПАСНИКА



Александр ИГОНИН
эксперт BIS Journal,
ведущий рубрики

В этом году в действие вступают «долгожданные» оборотные штрафы за повторную утечку персональных данных. Пока трудно сказать, какова будет правоприменительная практика и начнёт ли государство кошмарить компании по новым правилам. Я не являюсь большим экспертом по регуляторным нормам и их последствиям, но, по моему впечатлению, предыдущие подобные акты к массовым изменениям ландшафта кибербезопасности не приводили. Тем не менее мне как человеку, далёкому от уютных кресел топ-менеджеров, приятно видеть,

что внимание небожителей-законотворцев нет-нет да и обратится к нашей многострадальной отрасли.

В новом законе прописаны поистине драконовские штрафы, но вместе с тем — и смягчающие обстоятельства, одно из которых — расход не менее чем 0,1 % от выручки на «мероприятия по обеспечению кибербезопасности, проведённые лицензированной организацией». Много ли это? На мой личный взгляд — вполне умеренно, хотя один мой уважаемый коллега, который куда лучше ориентируется в бизнесе, считает, что это очень даже солидный и ощутимый уровень инвестиций. В любом случае приятно наконец увидеть жёсткие требования к затратам, а не туманные абстракции. Давно пора!

Интересно, что в новом законе нет чёткого указания, на какие именно направления должны расходоваться эти средства: хоть наймите людей, хоть разверните аппаратные или программные решения, хоть закажите аудит, пентест или ещё чего. Это даёт бизнесу большую гибкость — хочется верить, что ей не будут злоупотреблять, списывая требуемые расходы на виртуальные, существующие только на бумаге, мероприятия. Также интересно, что заветные 0,1 % нужно отдать лицензированным подрядчикам. А чтобы иметь возможность тратить эти деньги самостоятельно, придётся получать лицензию самому. Ждём повышения спроса на лицензии по криптографии и ТЗКИ?

И в заключение ещё одна мысль. По-хорошему, компания должна обрабатывать лишь необходимый минимум персональных данных, и по завершении обработки они должны удаляться. На практике же зачастую собираются сильно избыточные массивы данных, которые удаляются примерно раз в никогда, потому что времени, желания и денег с этим разбираться нет. Между тем процесс удаления обязательно должен быть отлажен — хотя бы для случаев, когда пользователь, реализуя своё право, требует прекратить обработку его ПДн. С новым законом появляется шанс (хоть и призрачный), что компании станут более ответственными и внедрят-таки процедуры периодического удаления неактуальных массивов данных. В конце концов, нельзя украсть данные, которых нет в системе, верно?

Что ж, посмотрим, как новый закон отразится на практиках инвестирования в обеспечение ИБ. Будем надеяться на лучшее и верить, что увидим ощутимый рост интереса топ-менеджмента к стоящим перед всеми нами проблемам — с соответствующим ростом бюджетов.



ПРИСОЕДИНЯЙСЯ К НАМ В 2025 ГОДУ!



Цифровая устойчивость промышленных систем — 2025 (ЦУПС-2025)

27–28 февраля, Москва, Центр событий РБК

Организаторы: Медиа Группа «Авангард», ИнфоТеКС, InfoWatch



Защита данных

7 апреля, Москва, Холидей Инн Сокольники

Организатор: Медиа Группа «Авангард»



Кадровое обеспечение информационной безопасности РФ

16–18 апреля, Москва, конгресс-центр МТУСИ

Организаторы: АНО «НТЦ ЦК», ФУМО по ИБ, Медиа Группа «Авангард», ИнфоТеКС



Технологии доверенного искусственного интеллекта

20 мая, Москва, кластер Ломоносов

Организаторы: АНО «НТЦ ЦК», Академия криптографии РФ, ИСП РАН, Медиа Группа «Авангард»
При поддержке: Минцифры России



Современные тенденции в криптографии (СТСcrypt 2025)

3–6 июня, Великий Новгород

Организаторы: Академия криптографии РФ, Математический институт им. В. А. Стеклова РАН, АНО «НТЦ ЦК», ТК26



РКІ-Форум Россия 2025

16–18 сентября, Санкт-Петербург

Организатор: Медиа Группа «Авангард»
При поддержке: ФСБ России, Минцифры России



Технологии SOC (Киберзастава SOC Tech 2025)

7 октября, Москва

Организатор: Медиа Группа «Авангард»



Конференция «Сетевая безопасность»

25 ноября, Москва, Холидей Инн Сокольники

Организатор: Медиа Группа «Авангард»



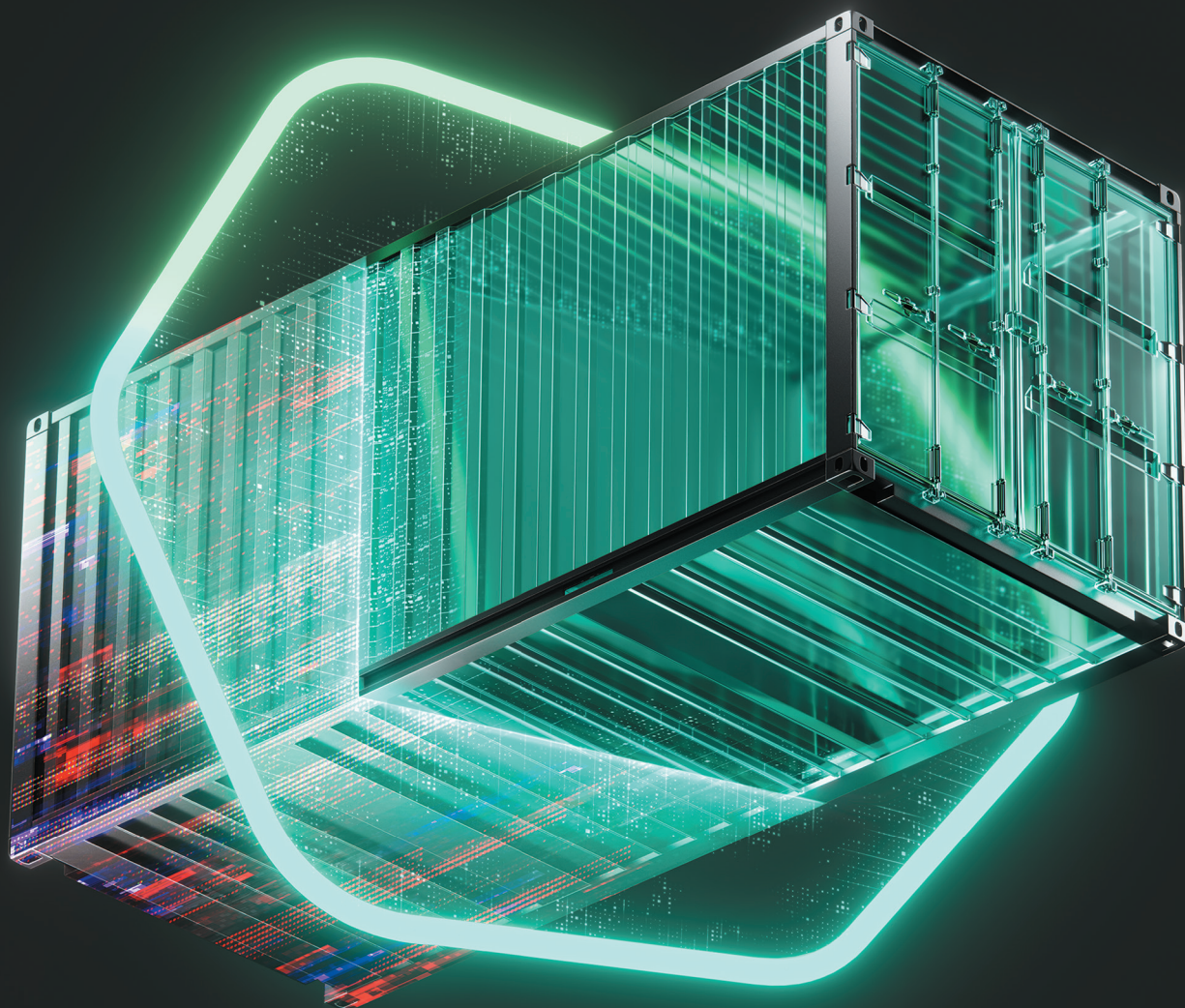
Открытая конференция ИСП РАН

9–10 декабря, Москва

Организатор: ИСП РАН



Kaspersky
Container
Security



Сканируем. Защищаем. Ускоряем.

Решение для безопасной разработки
и эксплуатации контейнерных приложений

kaspersky

kaspersky.ru