



BIS JOURNAL

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВ №4 (47) 2022



5 Игорь ЛЯПУНОВ
РТК-Солар
SOC в пейзаже кибервойны

18 Василий ПИСКАРЕВ
Государственная Дума РФ
Наша задача — сорвать планы запада по уничтожению России



28 Алексей ПЛЕШКОВ
Газпромбанк
ИБ превратилась в бизнес-преимущество

32 Александр ВЕЛИГУРА
Ассоциация российских банков
15 000 финансовых организаций остаются без защиты!

86 Екатерина СТАРОСТИНА
IThub college
Не надо бояться колледжа

SOC-ФОРУМ. ЭВОЛЮЦИЯ ТЕХНОЛОГИЙ, ЕДИНСТВО ЛЮДЕЙ



Форум

Цифровая устойчивость и информационная безопасность России

19–21

февраля

2023

Главные темы:

- Выполнение мероприятий, предусмотренных Указом Президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ»
- Импортозамещение в сфере ИБ
- Защита критической информационной инфраструктуры
- Идентификация недопустимых инцидентов для организации
- Практики повышения защищенности организаций: киберучения, социально-значимые проекты по повышению осведомленности, программы bug bounty
- Оценка цифровой устойчивости организации
- Обеспечение безопасности в цифровых реестрах и финансовых активах

Место

проведения:

Магнитогорск,

ДЦ «Юбилейный»

#ibbank

#magnitka



ib-bank.ru/secural



Артём ЗУБКОВ
генеральный директор
Медиа Группы «Авангард»

Нет, наверное, в этом мире большего чуда, чем рождение нового. Когда буквально из ничего, в данном случае из одного телефонного звонка, вдруг появляется целый мир, начинающий жить своей жизнью — развиваться, расти, поражать воображение. Семь лет назад мне позвонил Игорь Ляпунов, тогда еще, можно сказать, начинающий стартапер, и поделился мыслью, мол, не провести ли нам конференцию, посвященную исключительно SOC?

На первый — SOC-Форум 2015 — мы ожидали 200–300 участников, а когда пришло 600, и на сессиях было не протолкнуться, мы поняли, что звезды сошлись — мы угадали потребность отрасли. SOC «взлетел»! Сегодня мы ждем на SOC-Форум 2022 больше 4 тысяч специалистов-практиков в области ИБ, а насколько удастся превзойти ожидания — скоро узнаем!

Наш SOC-Форум растет, и мы вместе с ним. Игорь Ляпунов уже не стартапер, а вице-президент Ростелекома и руководитель одного из крупнейших SOCов страны, Медиа Группа «Авангард» — организатор крупнейших мероприятий в сфере ИБ.

Оценив масштаб и перспективы форума, к его организации подключились ФСБ России, ФСТЭК и другие регуляторы, что позволило нам выйти на немыслимый прежде уровень. Теперь коллективную работу над программой форума вполне можно сравнить с работой межведомственного научно-исследовательского института.

Но мне ближе другая сторона этой такой большой, такой красивой медали. Творчество и человеческое общение. Каждый год мы ищем новые формы, экспериментируем, чтобы снова и снова удивить нашу отрасль. Так, в результате наших безумных мозговых штурмов, появились блистательная АнтиПленарка, уникальный «телевизионный» онлайн-формат, захватывающие киберучения и киберполигоны...

Истина рождается в споре — для юной отрасли ИБ это особенно актуально. И перед коллективом «Авангарда», как оператора и организатора форума, всегда стоит сложная задача: как в сверхнапряженный график деловой программы вплести нити дружелюбия, добавить «человеческую» ноту. У нас это получается. Наверное, потому что мы любим наше неповторимое, неподражаемое детище — наш SOC-Форум.

Приходите, и вы это почувствуете.

До встречи!

ОБЩЕСТВЕННЫЙ РЕДАКЦИОННЫЙ СОВЕТ

Войлуков А.А. — вице-президент Ассоциации банков России
Сычев А.М. — доцент МГТУ им. Баумана, доктор технических наук

Шипилов В.В. — исполнительный директор Ассоциации российских банков, кандидат технических наук

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

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. — специалист Службы информационной безопасности КБ Максима (ООО)

Вихорев С.В. — советник генерального директора по информационной безопасности IT Expertise

Дзержинский Ф.Я. — независимый эксперт

Зубков А.Н. — генеральный директор ООО «Медиа Группы «Авангард», директор Фонда содействия развитию безопасных информационных технологий (ФСРБИТ)

Калашников А.И. — директор проекта, Газпромбанк (АО)

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

Левиев Д.О. — председатель Совета НП «Партнерство специалистов по информационной безопасности»

Мельников С.Ю. — заместитель генерального директора ООО «Лингвистические и информационные технологии», доктор физико-математических наук

Некрасов И.В. — главный редактор журнала

Одувалов М.В. — руководитель службы Управления по обеспечению ИБ Банка ВТБ (ПАО)

Окулеский В.А. — заместитель начальника службы ИБ банка «Возрождение», кандидат технических наук

Пазинин С.В. — заместитель начальника Управления по обеспечению ИБ Банка ВТБ (ПАО), кандидат физико-математических наук

Рачкова Е.В. — управляющий директор Управления по обеспечению ИБ Банка ВТБ (ПАО)

Филипчук А.А. — технический директор ГК ЦРТ

Шумский Л.С. — руководитель службы информационной безопасности Яндекс Банка

Янсон И.А. — бизнес-партнер по информационной безопасности, Департамент безопасности ПАО «Сбербанк России», кандидат физико-математических наук

ЭКСПЕРТНАЯ ГРУППА

Баранов А.П. — доктор физико-математических наук, академик Академии криптографии РФ

Батранков Д.В. — руководитель направления сетевой безопасности Positive Technologies

Гадарь Д.А. — вице-президент — директор департамента информационной безопасности, Tinkoff.ru

Калемберг Д.А. — генеральный директор ООО «Сэйфтек»

Лукацкий А.В. — бизнес-консультант по безопасности Positive Technologies

Сабанов А.Г. — заместитель генерального директора АО «Аладдин Р.Д.»

Сумманен К.Т. — директор по управлению проектами — вице-президент, Банк ВТБ (ПАО), кандидат физико-математических наук

Хайретдинов Р.Н. — директор по росту компании BIZONE

РЕДАКЦИЯ ЖУРНАЛА

Главный редактор: **Некрасов И.В.**

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

Арт-директор: **Мельников Н.С.**

Руководитель интернет-проектов: **Воробьева А.А.**

Ответственный редактор: **Седов О.В.**

Обозреватели: **Куликов В.А., Бродская М.А., Покатаева Е.Н.**

Иллюстрация на 1-й обложке: **Зинаида Серебрякова**

Фото в номере: **Envato.com**

Цветокорректор: **Науменко М.Б.**

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ

ООО «Медиа Группы «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). Свидетельство ПИ № ФС77-61378 от 10 апреля 2015 г.

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

Подписан в печать 25.10.2022. Тираж 5000 экз. Заказ № 1812022. Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 16, корп. 1, офис 201А

© BIS Journal, 2022



SOC-ФОРУМ 2022

- 5 **Актуальное интервью**
Игорь Ляпунов (РТК-Солар)
SOC в пейзаже кибервойны
- 6 **Актуальное интервью**
Известные CISO отрасли
о предстоящем форуме
- 8 **Актуальное интервью**
Алексей Плешков (Газпромбанк)
К чему должны стремиться
руководители SOC



5

НОВОСТИ

- 11 **В России, законодательство, технологии**

ТЕМА НОМЕРА

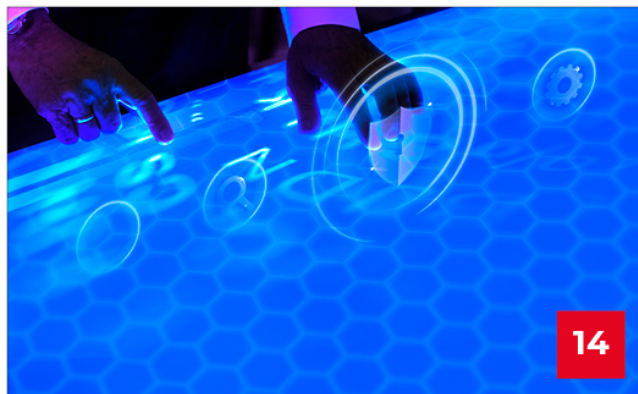
- 14 **ИБ 2.0**
Алексей Лукацкий
(Positive Technologies)
Результативная кибербезопасность

РЕГУЛЯТОРЫ

- 18 **ГосДума**
Василий Пискарев
(Государственная Дума)
«Наша задача — укрепить суверенитет, сорвать планы запада по уничтожению России»
- 22 **Нормативная база**
Андрей Макоско
(АО АКБ «НОВИКОМБАНК»)
Изменение структуры
- 25 **Комментарии / 266-ФЗ**
Сергей Вихорев (ИТ-Экспертиза)
Что день грядущий нам готовит?

БАНКИ

- 28 **Собеседник**
Алексей Плешков (Газпромбанк)
«ИБ на глазах превратилась в бизнес-преимущество»
- 32 **Вопрос залу**
Александр Велигура (АРБ)
Нельзя по-старому! А как по-другому?
- 32 **Вопрос залу**
Артём Калашников (Газпромбанк)
15 000 финансовых организаций остаются без защиты!
- 34 **Ответ из зала**
Андрей Курило (FBK CyberSecurity)
О централизации сервисов безопасности
- 35 **Ответ из зала**
Василий Окулесский (эксперт ИБ)
Каждый должен заниматься своим делом



14

УГРОЗЫ И РЕШЕНИЯ

- 36 Киберразведка**
Полина Перлова (R-Vision),
Валерий Горбачёв (ДиалогНаука)
Эффективное управление данными threat intelligence
- 38 ИБ + ИИ**
Иван Чурилов (ЛАНИТ-ТЕХНОЛОГИИ),
Иван Мелехин (Информзащита)
SOC + ML
- 42 XDR**
Антон Тихонов, Сергей Штин,
Дамир Шайхелисламов
(Лаборатория Касперского)
Альтернатива SOC?
- 45 SIEM**
Павел Пугач (СёрчИнформ)
Почему SIEM-система больше не роскошь
- 46 Управление уязвимостями**
Анастасия Зуева (Positive Technologies)
Дисциплины в банках больше
- 49 Threat intelligence**
Сергей Нейгер
(Перспективный мониторинг)
Поставщики Threat Intelligence ушли, но threats остались
- 52 DСАР-системы**
Владимир Ульянов
(эксперт по кибербезопасности)
Сильный конкурент западным решениям
- 54 Диагностика**
Константин Юдин (Доктор Веб)
Dr.Web FixIt!
- 56 Киберриски**
Максим Степченков (RuSIEM)
Страхование киберрисков — сегодня и завтра
- 58 ИБ + ИИ**
Сергей Парфенов (Фаззи Лоджик Лабс)
Современный антифрод
- 60 Экосистемы**
Иван Чернов (UserGate)
UserGate SUMMA



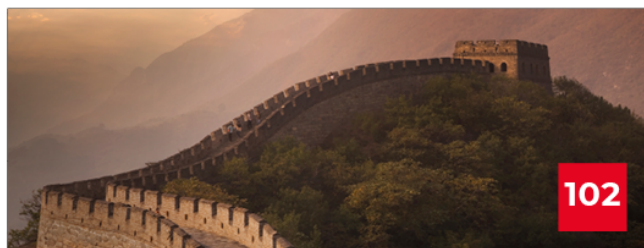
ИНФРАСТРУКТУРА

- 62 Деловые мероприятия**
XX PKI-Форум Россия
- 66 Деловые мероприятия**
Николай Кольский (BIS Journal)
Мастер-класс Школы управления Сколково
- 68 Деловые мероприятия**
Павел Никифоров (BIS Journal)
BIS Summit 2022
- 70 Деловые мероприятия**
Антон Реут (BIS Journal)
OFFZONE 2022
- 71 Деловые мероприятия**
Марк Новоначный (BIS Journal)
Прыжок веры или рост на основе экспертизы?
- 72 ИБ + ИИ**
Василий Окулесский (эксперт ИБ)
Одному банку не по силам
- 75 Персональные данные**
Павел Былевский
(Финансовый университет)
Футурология угроз больших персональных данных

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

78 Психология

Андрей Жаркевич (ООО «Антифишинг»)
Победить нельзя защитить



ОБРАЗОВАНИЕ И КАРЬЕРА

82 Высшее образование

Михаил Левашов (старший научный сотрудник)
Блеск и нищета ИБ-образования

84 Высшее образование

Василий Окулесский (эксперт ИБ)
Смещение акцентов

84 Высшее образование

Андрей Курило (FBK CyberSecurity)
Оптимальный путь — облачная платформа

86 Высшее образование

Екатерина Старостина (IThub)
Не надо бояться колледжа!

88 Рынок труда

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

89 Обзор

Анна Катанкина (BIS Journal)
Приёмная кампания — 2022

91 Обзор ИноСМИ

Марина Бродская (BIS Journal)
«Думать и вкладываться в образование!»

ЗА РУБЕЖОМ

95 Обзор

Кибератаки стали мировой угрозой

100 Беларусь

Александр Виноградов (ФГУП «ЦНИИХМ»), Сергей Меньшиков (Belarusian InfoSecurity Community)
Россия — Беларусь: диалог друзей

102 Китай

Алексей Савичев, Амина Замулина (Сбербанк)
Суровый опыт Поднебесной



СУБЪЕКТЫ

106 История

Борис Столпаков (историк криптографии)
Из тьмы веков звучат лишь Письмена

112 История

Борис Столпаков (историк криптографии)
«Одно образование умственное не довершает ещё воспитание»

116 Заметки безопасника

Александр Игонин (BIS Journal)
Сказка о Большой Красной Кнопке



SOC В ПЕЙЗАЖЕ КИБЕРВОЙНЫ

НА ВОПРОСЫ BIS JOURNAL ОТВЕЧАЕТ ИГОРЬ ЛЯПУНОВ

О ПЕЙЗАЖЕ

— Пейзаж рынка информационной безопасности сегодня — это не столько картина в раме — застывшая и неподвижная, сколько голограмма живого неба с постоянно бегущими и меняющимися очертания облаками. Можете ли вы зафиксировать эту картину перед SOC-Форумом. Что изменилось за последние год-два? Например, в 2020 году вы говорили, что ситуацию на рынке определяют Ростелеком, Сбербанк и Ростех, но в этом году подули другие ветры?

— Да, прямо сейчас рынок ИБ стоит на пороге глобальных перемен. Как и любой рынок, превращающийся из

небольшого, нишевого в быстрорастущий, нас ждёт структурная перестройка. И она уже началась. Первое — идёт серьёзное укрупнение игроков. Сейчас нас ждут большие сделки по слияниям и поглощениям. Второе — ушли иностранные вендоры, всегда игравшие большую роль и определявшие ландшафт. Теперь их нет, и этот вакуум начнёт быстро и серьезно заполняться. Третье — глобально меняется спрос, профиль спроса и потребления на рынке. Компании, зарабатывавшие сугубо на комплаенсе, сейчас уходят с рынка и со временем исчезнут. Останутся только те, кто может давать действительно классный продукт, полноценные сервисы.

Сейчас рынок ИБ проходит тот же путь, что и IT-рынок 10–15 лет назад. Одни игроки, в основном мелкие, уходят, а новые, существенно более крупные, остаются, и между ними начинается битва за технологичность. А у технологичности есть рычаг — объём инвестиций, вкладываемый в рынок технологий. За счёт этого динамика рынка ИБ сейчас кардинально поменяется. Если раньше рынок рос на 10–12% в год, в 2022 году в силу известных обстоятельств рост приостановился, зато 2023–24 годы станут золотыми для рынка ИБ.

— Какими были последние два года для рынка и для «Ростелеком-Солар» в отношении объемов выручки?



— В 2021 году мы вышли на показатель 12 млрд рублей с ростом 47%.

Мы осознаем, что являемся одним из системообразующих игроков рынка ИБ. Во-первых, потому что «Ростелеком» играет ключевую роль на рынке ИТ и во многом определяет на нем правила.

Во-вторых, мы инвестируем больше всех в рынок ИБ — более 22 млрд руб., что, конечно, серьезно на него влияет.

В-третьих, в фокусе внимания «Ростелеком-Солар» всегда было и будет обеспечение настоящей безопасности на основе полноценной сервисной модели. Сегодня кибербезопасность востребована как никогда, в режиме «здесь и сейчас». И никаких других способов её получить, кроме как в виде аутсорсинга, когда вместе упакованы экспертиза, технологии и человеческий ресурс, не существует. Только такая

сервисная модель может дать заказчику за две недели состояние защищённости. Мы, в отличие от большинства, это можем, что и определяет наше лидерство на рынке. Не зря многие называют нас «стандартом де-факто».

— **Как на вашей компании и на рынке в целом сказались события 2022 года (рывок в сторону отечественных решений, уход ряда конкурентов, новые угрозы и т.д. и т.п.)?**

— Доминирующим фактором сегодня является, конечно, колоссальная волна кибератак. По сути — это развёрнутая против России кибервойна. Это ключевое. Из этого вырастает спрос на информационную безопасность в двух плоскостях. В одной идет процесс переосмысления подходов к обеспечению ИБ. Стало понятно, что важны не только и даже не столько технологии. Ключ к защищённости сегодня — это высокий уровень системы управления и менеджмента. Это правильно выстроенная архитектура безопасности, инфраструктура, безопасные ИТ-системы.



Теймур ХЕИРХАБАРОВ, BI.ZONE:

— Тема SOC сегодня на подъёме, всё больше людей и компаний в неё вовлекается. Не сомневаюсь, что SOC-Форум в этом году станет ещё крупнее и круче и подтвердит свою репутацию самого знакового мероприятия в этой сфере. Наша компания представит участникам форума несколько докладов и те инструменты, которые мы сами для себя разрабатывали и совершенствовали. Надеемся, участники Форума смогут взять их в свой арсенал. И, конечно, будем рады видеть всех на стенде BI.ZONE и на выступлениях наших экспертов.

И всё вместе это складывается в систему киберустойчивости бизнеса. На такой комплексный подход сейчас большой спрос.

Другая плоскость — это консалтинг, когда нас приглашают не подрядчиком, а скорее идеологом, архитектором всей системы ИБ. На это тоже большой спрос.

— **А ситуация с импортозамещением?**

— Да, иностранные вендоры ушли и тем самым освободили часть рынка. Конечно, их никто сразу не заменит. Да, российские решения стали покупать несколько больше, но ненамного. Например, доля NGFW на рынке порядка 20 млрд руб., но хорошего отечественного файервола нового поколения не существует и заменить его нечем. В 2022 году импортозамещение еще не является драйвером рынка, а вот в 2023–24 уже появятся вполне рабочие технологии. То есть эта высвободившаяся ниша заполнится, но не сейчас, а на горизонте двух-трех лет.

— **Интерес к каким продуктам и услугам на рынке сейчас наиболее высоки? С чем это связано? Какие ваши решения и услуги востребованы, а какие нет?**

— Как я уже сказал, в первую очередь это сервисы и сервисные модели. С конца февраля мы получили удвоение, если не больше, клиентской базы, подключенной к нашим сервисам. И как-то очень быстро был преодолен барьер недоверия к аутсорсингу, видно, за отсутствием альтернативы.

А второе — это, конечно, технологии выявления и предотвращения кибератак. Плюс набирает новую силу тема DLP — защита от утечек, контроль сотрудников. Потому что уровень внутренних угроз тоже вырос.

— **«РТК-Солар» активно участвует в поиске и развитии новых технологий кибербезопасности. Какие технологические ниши сейчас наиболее интересны, и как скоро они появятся на российском рынке?**

— Если заглянуть чуть дальше, на 2–3 года вперед, то потребности рынка определяет, конечно, дефицит технологий сетевой безопасности. Второе, чем мы плотно занимаемся, — это выявление атак на ранних

”

Руслан ПАХМЕТОВ, Security Vision:

— SOC-Форум — главная ежегодная площадка для обмена опытом и общения с коллегами по цеху. Нам важно услышать потребности наших клиентов, как настоящих, так и будущих, а также обменяться опытом работы, понять ожидания, возлагаемые на новые решения и услуги. В условиях шквала кибератак такая совместная работа крайне значима для отражения внешней киберагрессии в масштабах всей страны, а коллективное обсуждение темы сейчас, возможно, является самым действенным и экономически целесообразным способом повысить общий уровень киберзащитности всех секторов экономики.

”

Михаил Шипицын, КСБ-СОФТ

— SOC-Форум — основная площадка для обмена мнениями экспертов в сфере практической ИБ, именно здесь рождаются новые идеи и тенденции. Очень рассчитываю, что в этом году форум задаст определяющие тренды на 2023 год, и они окажутся позитивными.

стадиях. И третье — это всё, что касается безопасной разработки: выстраивание как циклов безопасной разработки, так и инструментов.

— **Вы не раз говорили о смене парадигмы информационной безопасности, но это была скорее констатация процесса, а в этом году все настойчивее звучат слова о необходимости создания концепции «Информационная безопасность 2.0» — документа, фиксирующего принципиальные изменения в отрасли. Так ли это? Что это за концепция? Кто за ней стоит? К каким изменениям это может привести?**

— Парадигма не меняется. ИБ по-прежнему защищает инфраструктуру, бизнес-процессы, людей, что в этом нового? Важно не путать лозунги и маркетинговые тезисы с реальной жизнью.

Если говорить о действительно новом в сфере ИБ, я бы выделил два подхода. Первый: кибербезопасность сегодня — это в первую очередь не технологии, а система менеджмента, вписанная в общую систему управления компании. Второй: киберустойчивость — для бизнеса, а не наоборот. Когда мы встаем на точку зрения бизнеса, то начинаем

понимать, что ему без разницы из-за чего остановились бизнес-процессы — пожар, аппаратный сбой, ошибка в ПО, кибератака... В любой сфере важна устойчивость, а в сфере ИБ — это киберустойчивость. Бизнесу важна не столько причина киберинцидента, сколько скорость восстановления информационной системы и соответственно бизнес-процессов.

Да, ИБ эволюционирует. Десять лет назад мы все строили крепости с высокими стенами. И это было главным для нас. Пять лет назад мы поняли, что невзламываемых систем не бывает, кто-нибудь через «забор» перелезет. И стали считать, что главным является быстрый мониторинг, выявление атак до нанесения значимого ущерба. Сегодня мы делаем третий шаг, что, понятно, не исключает первых двух. Что будет завтра — посмотрим, но сегодня ключевое — это время восстановления. Это то, на что направлены киберучения, планы реагирования и т.д. И это то, что я вкладываю в понятие киберустойчивости. Только такая сборка, когда мы имеем защищенную инфраструктуру, быстрый мониторинг выявления кибератак и отработанные процедуры восстановления, минимизирующие



Андрей АРЕФЬЕВ, ГК InfoWatch

— Офлайн-мероприятия важны, это обмен профессиональными мнениями и информацией, новыми кейсами, общение с товарищами и знакомства с новыми интересными людьми. А сегодня качественные встречи, способные скоординировать, синхронизировать участников рынка важны как никогда. Мы поддерживаем SOC-Форум еще и потому, что в нем глубоко проработана программа, она актуальна, эффективна и стремится вскрывать болевые точки отрасли. Понятно, что общаться интересно и полезно только на важные, острые, часто неудобные, темы.

ущерб. Все это даёт бизнесу состояние такой динамической устойчивости — защищённости и минимизации ущерба.

— О темной стороне. Там дуют те же ветры, но идут другие процессы. Какие? Возможно, и там грядут принципиальные изменения, качественные скачки, новые ориентиры, цели и средства? А может, уже произошли?

— Россия словно получила от темной стороны черную метку. Похоже, все хакеры мира пытаются поразить

нашу инфраструктуру и, конечно, проверить в деле своё оружие. Это и неспециалисты-«сочувствующие», и профессиональные группировки. На нас отрабатываются очень современные, передовые способы атак. Даже те, которыми пользуется киберармия Украины, только на первый взгляд выглядят просто, но под капотом там очень высокие технологии. Вот оно — соревнование брони и снаряда. Конечно, в нём совершенствуются обе стороны.

И еще один важный момент: специалисты по кибернападению прямо сейчас готовятся, обучаются тысячами. Но эта кибервойна рано или поздно закончится, а обученные специалисты в огромном количестве останутся. Возникает вопрос: куда они направят свои умения? И как дальше будет использоваться этот темный, достаточно мощный потенциал? Вопрос тревожный, и теперь уже не столько для России, сколько для всего мира.

НЕПОСРЕДСТВЕННО SOC

— Опираясь на данные, которые вы собираете как крупнейший провайдер сервисов SOC, какие угрозы и проблемы с кибербезопасностью можно выделить в российских организациях? Какова ситуация в различных отраслях?

— Последние полгода большую часть проблем мы видим не в отсутствии каких бы то ни было средств защиты, а в целом в процессах управления IT. Например, сейчас основной вектор атак идет через подрядчиков: хакеры взламывают IT-компании и через них

Алексей ПЛЕШКОВ

заместитель начальника департамента защиты информации Газпромбанка

К ЧЕМУ ДОЛЖНЫ СТРЕМИТЬСЯ РУКОВОДИТЕЛИ SOC

Мнение Алексея Плешкова интересно тем, что он стоял у истоков создания SOC Газпромбанка в 2009–2010 годах и много лет следит за его формированием и развитием.

— Успевают ли развитие вашего SOCа за киберпреступниками, законодательством и глобальной цифровизацией?

— Успевают. В рамках ИБ у нас есть отдельное подразделение, отслеживающее все изменения в законодательстве. Оно активно участвует в деятельности коллегиальных органов при регуляторах. Поэтому многие вещи мы

знаем раньше рынка и всегда готовимся к ним.

— Какие изменения произошли в вашем SOCе за прошедший год? Какие компоненты/моменты/функции пришлось пересмотреть?

— Основной акцент мы как обычно делаем на сетевые атаки и противодействие мошенничеству — как внешнему, так и внутреннему. А в контексте происходящих вокруг событий, увеличилась важность реагирования SOC на кибератаки из Интернет. Пересматриваются и оптимизируются метрики и пороговые значения, характеризующие инциденты и подозрительную активность в

Интернет. На их основе, а также с учетом рекомендаций ФинЦЕРТ, ФСТЭК и производителей проводятся тонкие настройки.

— Как вы относитесь к мысли о том, что SOCи в основном создавались впрок и не совсем понятно зачем, и вот, наконец, они оказались востребованы в полном объеме. Применимо ли такое утверждение к SOCу Газпромбанка?

— Не согласен с тем, что SOCи создавались впрок. Возможно, у кого-то с точки зрения бизнеса и могла возникнуть такая позиция, потому что на начальном этапе, в отсутствии

проникают дальше — непосредственно на целевые объекты.

Почему такие атаки успешны? Потому что ИТ-подрядчики имеют прямой неперсонифицированный доступ к системам заказчиков. Когда мы проводим анализ и выстраиваем систему, то вычищаем сотни активных, но ненужных учётных записей администраторов. Инвентаризация периметра, сервисов, управление изменениями — это разгребание авгиевых конюшен, которое сейчас является одним из ключевых моментов. Качество ИТ, зрелость ИТ-процессов сегодня определяет и уровень информационной безопасности.

— **Насколько вырос в последнее время спрос российских компаний на услуги SOC?**

— С начала года больше, чем в два раза.

— **Получается, у вас очередь образовалась?**

— В первые два месяца СВО, в марте-апреле, очередь была. Сейчас мы, конечно, увеличили свои мощности и в части инфраструктуры, и в части кадров, и теперь вполне справляемся.

источников и согласованных метрик и признаков, характеризующих инциденты, SOCs дают не так много событий и инцидентов, значимых для бизнеса. Но когда мы говорим о зрелом SOCe, например, SOCe Газпромбанка, то здесь его значимость и статус трудно переоценить. В таких SOCs все инциденты четко выверены, признаки согласованы и понятны бизнесу, ошибок в них почти не бывает. Мы можем очень гибко настраивать системы реагирования с учетом имеющегося опыта и, настраивая фильтры, прицельно выявлять инциденты, значимые и критичные для бизнеса.

— **Что влияет на скорость и качество созревания SOC?**

— Считаю, что от правильности взаимодействия между ИБ, ИТ и бизнесом при расследовании инцидентов, зависит скорость становления SOC и приведения его к тем ожиданиям, которые ставит бизнес. Это первый момент.

Второй — последовательность и постепенность. SOC Газпромбанка по-



Сергей НЕЙГЕР,
Перспективный мониторинг

— SOC-Форум — ключевое мероприятие сезона. Нигде нет столько участников, столько тем, такого тесного контакта вендоров и провайдеров, заказчиков и регуляторов. Тут мы точно увидимся с теми, с кем хотели увидеться, всё расскажем и покажем, проведём киберучения и, что немаловажно, отлично проведём время и получим удовольствие от общения. SOC-Форум — это Топ!

— **Какие изменения произошли в теме SOC за прошедший год? С чем столкнулись SOC в прошлом году и в этом? Какие компоненты/моменты/функции пришлось пересмотреть и почему? Какие новые решения в SOC появились?**

— Ну, это набор тем для отдельной конференции. И на SOC-форуме, конечно, мы всё это будем обсуждать. Для меня сейчас очень важным является всё, что связано с ранним выявлением атак. Мы запустили на опорной сети «Ростелекома» систему раннего выявления кибератак, не ставя при этом ничего

на площадку заказчика. Дело в том, что через сеть «Ростелекома» проходит 60–70% всего российского трафика. Мы расставили по всей сети сенсоры и боты, которые позволяют по аномалиям в трафике выявлять признаки компрометации, атак, идущих на наших заказчиков. Это, конечно, предельно быстрое оповещение. Совместно с другими сервисами, такими как анализ даркнета, такой подход даёт колоссальный эффект.

— **Что ваша компания представит рынку на SOC-Форуме 2022? О чём будете рассказывать, каким опытом делиться?**

явился в 2009 году, когда не было никаких требований, рекомендаций регулятора, не было такого уровня киберугроз. У нас было время для поэтапного развития и отработки всех сложных и спорных моментов. За 13 лет наш SOC вырос от небольшой дежурной смены до целого департамента. Функциональные участки расширились, а глубина интеграции SOC с банковскими процессами увеличивалась.

— **Имеет ли руководство SOC вес и влияние в руководстве банка?**

— Тот факт, что руководитель и представители нашего SOC сейчас входят практически во все профильные комитеты и коллегиальные органы банка, связанные с непрерывностью бизнеса, говорит о том, что влияние и позиции ИБ в Газпромбанке стали существенно выше, чем раньше. Я думаю, это хороший пример того, к чему должны стремиться руководители SOCs и дежурных служб в других банках.

— **Будет ли Газпромбанк участвовать в SOC-Форуме, и какие темы для вас наиболее актуальны?**

— Мы являемся регулярным участником SOC-Форумов каждый год и очень ценим как само мероприятие, так и возможность принять в нем участие и выступить с докладами.

Я думаю, что в этом году основной фокус будет направлен на все, что связано с кибератаками на Интернет-ресурсы отечественных компаний в контексте происходящих в мире событий. Этих атак стало больше, они стали интенсивнее, они не ограничиваются только финансовым сектором. Обеспечение непрерывности бизнес-процессов — тоже важная тема. Также будет полезно выслушать мнение и рекомендации регуляторов для тех организаций, которые пока не считают себя субъектами КИИ и не получают от регулятора официальные рекомендации.

Беседу с Алексеем Плешковым читайте на стр. 28



Сергей ШЕРСТОБИТОВ,
Angara Security

— Форум — это неповторимая, единственная в своем роде «SOC-ярмарка», где можно на других посмотреть, себя показать и зарядиться могучим профессиональным импульсом. Мы, например, планируем донести наши конкурентные преимущества до максимально широкого спектра потенциальных заказчиков и рассказать рынку о новых предложениях компании. В том числе проведем презентацию нового потрясающего продукта ANGARA-РЕДУТ.



Александр БОНДАРЕНКО, R-VISION

— Тематика SOC не только не утратила своей актуальности, а стала ещё более актуальной. Теперь эта тема перешла из разряда хайпа в разряд «обязательно к реализации». Что здесь важно, так это накопление опыта, которым можно и нужно делиться. И именно этого ожидаем мы и, я думаю, все остальные участники рынка. Уверен, что будет много полезной информации, прикладного опыта и ценного профессионального общения.

— Для SOC-Форума мы подготовили целую программу. Понятно, что восьмимесячный опыт противодействия кибервойне уникален. В последнее время я много встречаюсь с коллегами из разных стран. У них у всех один вопрос: как вы это сделали? Как выдержали такое давление, как выстояли? И вот этот опыт именно практического противодействия сегодня очень важен и востребован. На SOC-Форуме мы сделаем акцент на практике защиты: как мы выявляем атаки, проникновения, как восстанавливаемся... Будем говорить именно о практическом опыте текущей кибервойны.

— Чем для вашей компании полезно участие в SOC-Форуме? Какие темы для вас наиболее актуальны?

— SOC-Форум — это отличное мероприятие, где всегда собираются лучшие эксперты отрасли. Так как кибербезопасность — это бурно развивающаяся дисциплина, то, конечно, в ней все рождается здесь и сейчас, на кончиках пальцев. И тут крайне важно неспешное человеческое общение профессионалов. SOC-форум — эпицентр

такого общения. Живой обмен мнениями, лучшими практиками, что получилось, что не получилось... Я лично в первую очередь ожидаю, что этот большой слет специалистов, так же, как и в прошлые годы, даст синергетический эффект, усилит потенциал отрасли.

— Успевает ли развитие ИБ (и SOC, в частности) за киберпреступниками, законодательством и глобальной цифровизацией? Почему? Что нужно еще сделать?

— Цифровизация движется наиболее быстрыми темпами, это запрос бизнеса, который, понятно, является катализатором, драйвером развития ИБ. Следом с небольшим отставанием — киберугрозы, хакеры. Третьим номером уже кибербезопасность. По идее она должна бежать в ногу с цифровизацией, но так не бывает, кибербезопасность всегда немного отстает от цифровых темпов развития. И вот цифровизация бежит первой и иногда спотыкается о киберриски. Тогда она притормаживает, чтобы дождаться зрелого обеспечения безопасности.

Ну, и последним эшелон, и это правильно, движется регуляторика. Она и не может бежать впереди паровоза, ведь ее задача — реагировать на изменения макроландшафта. Хотя сейчас, конечно, темпы нашей регуляторики очень высокие. Мы должны относиться к этой регуляторике, как к некой консервативной силе, которая задает систему координат. И эта система сейчас на высоком уровне.

— Как должен выглядеть идеальный SOC? Чего не хватает для его создания?

— Идеального SOC быть не может. Если он идеальный, значит, оторвался от земли, превратился в сияние чистого разума. Для SOC главное — скорость выявления и адаптации к новым атакам, постоянное развитие.

А если говорить, чего не хватает, то, конечно, сейчас это кадры. Безусловно, необходимы изменения на всех уровнях подготовки, и здесь есть две цели. Первая — повышение скорости подготовки специалистов, то, что называется time-to-market. Сейчас time-to-market специалиста по безопасности — 6 лет, это очень много. Нужно научиться готовить специалистов за 1,5–2 года. Для этого на первый план должно выйти среднее специальное образование. Второе — это практикоориентированность образования. Кибербезопасность — это в первую очередь не теоретическая наука, а практические навыки и актуализация знаний.

— Как вы решаете проблему кадрового дефицита у себя в компании?

— Во-первых, мы работаем с вузами, делаем вместе с ними интенсивы по практической кибербезопасности. Большую роль тут играет наш давний партнер «Сириус» — образовательный центр и университет, который создает действительно новую модель образования в сфере кибербезопасности в России. Второе — это наш Национальный киберполигон — большая площадка для практической подготовки специалистов. На его базе мы делаем много образовательных интенсивов, курсов для специалистов.

— Спасибо! Удачи на SOC-Форуме!

Вопросы задавал
Игорь Некрасов

ЦБ РФ УВЕДОМИТ МВД

Госдума приняла в третьем чтении Закон о противодействии хищениям с банковских карт граждан. В нём содержится требование к Банку России передавать правоохранным органам данные обо всех подозрительных операциях с банковскими картами.

«Попытки преступников обманом завладеть средствами, которые граждане хранят на банковских счетах, необходимо пресекать. Только с начала 2022 года с использованием пластиковых карт было совершено более 72 тыс. преступлений. Люди получают десятки звонков в день, мошенники представляются им работниками

банков, силовых структур», — прокомментировал принятие новых мер председатель ГД РФ Вячеслав Володин.

Так, силовики будут передавать регулятору данные о действиях, связанных с попытками перевода средств без согласия клиента, а тот, в свою очередь, будет предоставлять им информацию из базы данных о попытках совершения противоправных операций. По плану это позволит правоохранным незамедлительно приступить к проведению оперативно-розыскных мероприятий (сейчас финучреждения отвечают на запросы МВД по хищениям только через 30 дней).



400 КАТЕГОРИЙ СОФТА

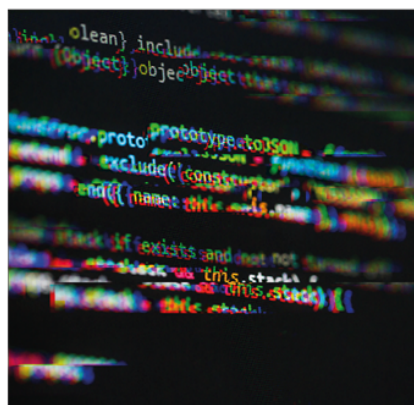
В рамках импортозамещения компаниям нужно 400 категорий корпоративного и промышленного софта, заявил глава Минцифры Максуд Шадаев, выступая на пленарном заседании Форума «Цифротех» 19 октября 2022 года.

«Поддержкой ИТ-отрасли занимается не только Минцифры, но и Правительство и Администрация президента. Это общий фокус и приоритет», — отметил он.

Что касается импортозамещения ПО в России, по словам Шадаева, складывается неплохая ситуация: «В рамках промышленных центров компетенций мы анализируем, какие решения нужны. Определили порядка 400 категорий корпоративного и промышленного софта, необходимого нашим компаниям. По 80% из них у нас есть конкурентные аналоги».

«За полгода мы получили колоссальный опыт (работы в области ИБ — ред.). Было принято ключевое

решение — смена парадигмы и отношения компаний к этому вопросу. Благодаря указу президента (о дополнительных мерах по обеспечению ИБ — ред.) главы компаний поняли, что кибербезопасность — это их задача. Компании сейчас прилагают много усилий, работа набирает темпы, и теперь главное — не останавливать её. Нужно быть начеку», — сказал Максуд Шадаев.



ПЕРВЫЙ ИНТЕРНЕТ-СПУТНИК

22 октября «Роскосмос» с помощью ракеты «Союз» запустил на орбиту первый спутник проекта «Сфера» — «Скиф-Д», а также три космических аппарата «Гонец-М».

«Скиф-Д» — демонстрационный спутник массой 160 кг, часть системы широкополосного доступа в интернет. Энергопотребление спутника — около 250 Вт, а срок активного существования — три года. В текущем году на реализацию проекта было направлено 14 млрд рублей.

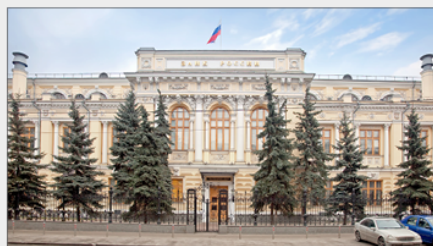
Проект «Сфера», анонсированный в 2018 году, предполагает обеспечение РФ спутниковым интернетом и связью посредством 600 спутников. В следующие три года на него планировалось направить 58,5 млрд рублей. В 2020 году стоимость всего проекта оценивалась в 1,5 трлн рублей, однако через год «Роскосмос» снизил оценку до 800 млрд рублей.

ВТБ И «ТИНЬКОФФ» О МОБИЛИЗАЦИИ

ВТБ и «Тинькофф» отметили в конце сентября рост числа трансграничных переводов в страны ближнего зарубежья. Эксперты связывают тренд с мобилизацией.

Клиенты ВТБ за последний месяц совершили на треть больше, чем обычно, переводов в «дружественные» страны. В «Тинькофф» сообщили, что самыми популярными направлениями для перевода по номеру телефона стали Узбекистан и Таджикистан: «В конце сентября наблюдаем рост спроса со стороны резидентов РФ».

Для россиян основными способами получения собственных средств за рубежом стали переводы с российской карты на карту иностранного банка либо получение их наличными. Россияне предпочитают снимать наличные, так как не у всех есть карты зарубежных банков.



13 ГЛАВНЫХ БАНКОВ

Банк России утвердил перечень системно значимых кредитных организаций страны. Он идентичен прошлогодней версии.

Всего в него входят 13 учреждений, располагающих около 77% совокупных активов отечественного банковского сектора. Это «ЮниКредит Банк», Газпромбанк, Совкомбанк, ВТБ, «Альфа-Банк», Сбербанк, Московский Кредитный Банк, «Открытие», Росбанк, Промсвязьбанк, Райффайзенбанк, Россельхозбанк и «Тинькофф Банк».

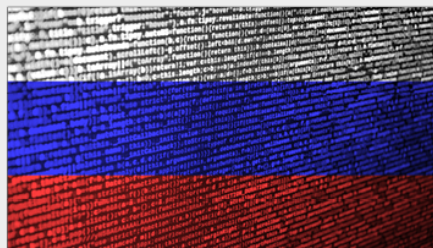
Последний стал участником списка в октябре 2021 года.

МИНЦИФРЫ НАЗНАЧИЛО

Минцифры назначило виды экономической деятельности, прибыль от которых будет учитываться при регистрации в реестре ИТ-компаний.

«Утвердить перечень видов деятельности, относящихся к деятельности в области информационных технологий, в соответствии с приложением», — гласит приказ министерства.

Речь идёт, например, о разработке или модификации программ для ЭВМ, производстве или проектировании программно-аппаратных комплексов, а также об оказании консультационных и экспертных услуг в отношении информсистем.



ЧЕЙ ГАДЖЕТ?

ЦБ РФ обязал российские банки с 1 октября идентифицировать все устройства, с помощью которых граждане проводят онлайн-транзакции, а также проверять их идентификаторы и телефонные номера. При этом некоторые финучреждения уже давно сами применяют эти способы защиты клиентов.

Новые меры описаны в указании регулятора, которое вносит изменения в положение Банка России № 683-П «Об установлении обязательных для кредитных организаций требований

к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».

«Даже если преступники выманят пароли и коды для доступа в интернет или мобильный банк, им не удастся войти в ваш личный кабинет со своего гаджета. Как только банк заметит подмену, он свяжется с вами и уточнит, вы ли заходите с другого устройства», — пояснили представители Центробанка.

УТЕЧКИ ДАННЫХ БУДУТ ДОРОГО СТОИТЬ

Минцифры доработало проект закона об оборотных штрафах за утечки персональных данных. Теперь наказания «рублём» предусматриваются не только для компаний, но и для их должностных лиц.

Согласно новой версии документа, для руководителей компании, допустившей утечку в 10–100 тыс. субъектов, штраф составит от 200 до 400 тыс.

руб. Для ИП и юрлиц — в 0,02% от оборота, но не менее 1 млн руб. (что следует из повестки к совещанию по вопросам регулирования законодательства в области ПДн).

Ужесточить наказание за такого рода инциденты власти решили после нескольких громких эпизодов в крупных российских компаниях и сервисах, имевших место весной этого года.



МИНПРОМТОРГ ПРОТИВ CISCO

В Минпромторге сообщили, что ведомство против возвращения бренда Cisco в Россию. Там уверены, что его продукты должны полностью заменить отечественные решения.



«Возврата назад к западному оборудованию не будет. Хотя наши уважаемые, в кавычках, партнёры всё время нас к этому подталкивают. Не так давно американцы вывели из-под санкций телекоммуникационное оборудование, и сегодня в средствах массовой информации прошло, что Cisco собирается возвращаться на наш рынок. Самое главное, чтобы мы сами понимали, что нельзя допустить, чтобы эта компания легко вернулась в ту же нишу, которую освободила», — заявил представитель министерства.

С его слов, местные заказчики уже сформировали запрос на российскую электронику с локальным софтом, и она — по планам — станет основой технологической независимости. «Эта ниша должна быть занята нашими производителями», — заключили в Минпромторге.

Ранее сообщалось, что Cisco может возобновить поставки оборудования через посредника — компанию IBS.



КУПИТЬ КОИНЫ? ЛЕГКО!

В начале следующего года Mastercard готовится запустить сервис для торговли криптовалютой Crypto Source — он будет работать с привязкой к банковским счетам через ЦФА-платформу Paxos Trust. Пилот программы реализуют в США, Израиле и Бразилии.

Paxos Trust будет предоставлять услуги по торговле и хранению коинов от имени кредитных организаций. А значит, те не будут держать криптоактивы у себя.

Mastercard же будет ответственна за решение проблемы, из-за которой американские банки сегодня не связываются с криптовалютами — безопасность и соответствие законодательству в процессе транзакций с определёнными «монетами».

FINO / 2021 / 22
POLIS
ФОРУМ
ИННОВАЦИОННЫХ
ФИНАНСОВЫХ
ТЕХНОЛОГИЙ

www.finopolis.ru

10-11 НОЯБРЯ
МОСКВА

- Цифровой рубль
- Цифровые платформы
- Цифровые финансовые активы
- Экосистемы
- Инновации в платежах
- Кибербезопасность

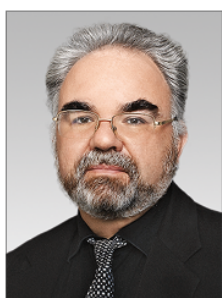
СТАНЬТЕ
УЧАСТНИКОМ
ГЛАВНОГО
ФИНТЕХ-СОБЫТИЯ
ЭТОГО ГОДА!



Реклама
12+

РЕЗУЛЬТАТИВНАЯ КИБЕРБЕЗОПАСНОСТЬ

КАК СОЙТИ С ПУТИ БЕЗ ЦЕЛИ И ВЗЯТЬ НА СЕБЯ
ОТВЕТСТВЕННОСТЬ



Алексей ЛУКАЦКИЙ
бизнес-консультант
по информационной
безопасности,
Positive Technologies

Многие знают поговорку о самурае, у которого «нет цели, есть только путь». Какое отношение она имеет к кибербезопасности? Как это ни удивительно, но специалист по информационной безопасности иногда оказывается таким самураем, который куда-то движется, конечно, но в целом маршрут его туманен и не ясен. И в спокойные времена это не слишком мешало: кто-то реализовывал требования регуляторов, кто-то в своем понимании занимался реальной информационной безопасностью, и пока не было того количества атак, которое мы видим сейчас, отсутствие четкой цели не было столь явным и критичным. Сегодня же такое «самурайство» и его неприемлемость с точки зрения цифровой устойчивости компаний стало явным как никогда. Что делать? Менять средства защиты? Менять себя как «безопасника»? Менять подходы к защите?

СПРОСИ СЕБЯ, ЗАЧЕМ?

Первое, что необходимо, — самому себе ответить на вопрос «ради чего вы занимаетесь информационной безопасностью?». Ответов тут точно будет больше одного: кто-то это делает ради денег (да, здесь платят неплохую зарплату), кому-то интересно это дело, кто-то просто работает по специальности (на что учился, там и ...), кто-то совмещает все три истории. Но тем не менее, чаще всего свою работу безопасник делает хорошо — и это нормально, но одновременно с этим и плохо. Обычно результат хорошей работы ИБ-специалиста — это отсутствие атак (результативных, конечно же, заметных), нарушений и простоев. То есть все работает как часы, и работа просто не видна ключевому заказчику (владельцу и руководителю того бизнеса или структуры, защите которой и обеспечивает специалист по информационной безопасности). Не видна, не понятна и, положа руку на сердце,



по большому счету, с точки зрения наказания за его несоблюдения у нас пока скорее никакой — штрафы настолько малы, что расходы на необходимые для обеспечения compliance средства защиты существенно выше). Когда единственным мерилom ИБ оказывается сравнение бюджетов на новые СЗИ, приобретение специфических услуг или запуска новых ИБ-проектов (тех же самых киберучений, к примеру) и потенциальных потерь в случае несоответствия compliance, информационная безопасность конечно же проигрывает в глазах бизнеса. Казалось бы тупик?

Нет. Чтобы из него выбраться, надо понять, каково видение результата в голове у бизнеса. А вариантов, как показывает практика, совсем немного. Во-первых, бизнес, как и все прочие, посмотрелся фильмов типа «Крепкий орешек 4», прочитался СМИ и понимает, что хакеры вокруг и атакуют, поэтому задача безопасника — не допустить атаку квалифицированного хакера, который может реализовать какие-то недопустимые для бизнеса последствия. Во-вторых, информационная безопасность должна уметь обеспечивать цифровую устойчивость организации в условиях непрекращающихся атак. И наконец, в-третьих, — безопасник должен уметь отвечать на вопрос «А как мы это делаем и делаем ли мы это правильно?». То есть видение бизнеса отличается от того, как смотрит на свою работу среднестатистический специалист по информационной безопасности, и базируется на гарантированной невозможности каких-то недопустимых для бизнеса ситуаций.

НЕ НОВОСТЬ, НО НОВЫЙ ВЗГЛЯД

Разберемся, что такое «недопустимость» в данном случае. Для этого можно обратиться к традиционному способу «спроси себя»: спроси себя, что недопустимо для тебя лично? В итоге окажется, что есть события нежелательные, но с ними как-то можно смириться, есть то, что постоянно с нами происходит и мы не расцениваем это как значимо негативное событие, а есть и, наконец, события, которые для нас настолько критичны, что совершенно недопустимы. Например, мы с вами можем, потерять сто рублей — ну потеряли и потеряли, с кем не бывает? Или, скажем, потерять сумму порядка 1000 или 5000 рублей, наверное, уже нежелательно, хотя мы и не умрем от этого — порой пятничныи счет в баре бывает на большую сумму. А вот потерять миллион — это для многих уже катастрофа и абсолютно недопустимо.

Так и у каждого бизнеса есть свой набор недопустимых событий — 3–5–7, не больше, — которые ставят на кон существование компании. Для

не интересна. Почему? Все просто: им не ясна взаимосвязь между целями, которые ставит для себя бизнес, и ИБ — обе зоны воспринимаются иногда как нечто, живущее и развивающееся в параллельных плоскостях, никогда не встречающееся и не зависящее друг от друга.

Топ-менеджмент условного бизнеса (условного, потому что государственные или муниципальные структуры в данном случае тоже бизнес, просто задачи у него немного иные — не заработать все деньги этого мира, а, скажем, оказывать населению услуги с должным качеством и в должные сроки) нередко просто не видит эффективности ИБ с точки зрения своего целеполагания. Им не понятны такие задачи, как «обеспечить соответствие требованиям регуляторов» (ФСТЭК, ФСБ, Минцифры, Центральный банк, Минэнерго, PCI DSS — все эти аббревиатуры для бизнеса часто просто набор букв) или обеспечить compliance (который,

кого-то это кража денежных средств, причем, в достаточно крупном размере (это может быть 10–15% от суммы, находящейся на корсчете), отзыв лицензии на оказание какого-то вида деятельности (например, банковской, что для банка означает, что он перестает работать с клиентами, финансами и по сути своей прекращает существование) или существенное время простоя при оказании услуги и проч. То есть у каждого бизнеса есть свои недопустимые события (да терминологически их могут называть по-другому, но суть от этого не меняется), а задача ИБ в данном случае — понять какие недопустимые события есть и, возможно, помочь их сформулировать.

Именно в этом направлении движется сейчас Минцифра, которая формирует реестр недопустимых событий, что сильно упростит жизнь компаниям и их службам информационной безопасности, которые смогут выбрать из нескольких десятков, а может быть и сотен событий, актуальных для разных отраслей, наиболее актуальные для себя. И дальше задача ИБ понять, как эти события могут быть реализованы в ИТ-инфраструктуре хакерами. Это то, с чего начинается диалог с бизнесом, который часто хочет понять, ради чего нужны вся та защита, на которую тратятся деньги. И именно недопустимые события позволяют ИБ не говорить о перманентной борьбе с некими угрозами, выполнении требований регуляторов, а перейти на уровень демонстрации недопустимости реальных событий (потерь), говорить о том, что ИБ работает для того, чтобы бизнес не обанкротился, или не понес какой-то иной катастрофический ущерб.

Отмечу, что термин «недопустимое событие» новый, но сама идея не нова — она очень близка к рискам, может быть без глубокой математики, без оценки вероятности реализации ущерба, с более бинарным подходом, когда событие либо можно реализовать, либо нельзя. Регуляторы двигаются в том же самом направлении: понять, что важно для бизнеса, и как это можно ретранслировать на ИТ-инфраструктуру. Например, многие знают, что есть методика оценки угроз ФСТЭК, которая сейчас претерпевает очередные изменения, и ожидается, что будет иметь больший фокус именно на негативных последствиях. И одна из важных задач сейчас — унифицировать терминологию, чтобы ИБ, бизнес и регуляторы смогли говорить на одном языке.

КАК ОПРЕДЕЛИТЬ ГЛАВНОЕ И НЕ ОШИБИТЬСЯ

Есть десятки сценариев, которые гипотетически могут привести к краху бизнеса, но в реальности их невозможно реализовать. Поэтому,

как я уже писал, необходимо понять, как каждый конкретный сценарий, недопустимое событие, может быть реализовано «плохими парнями» через ИТ-инфраструктуру, какие шаги они должны сделать, чтобы достичь некоей целевой системы, в которой недопустимое событие может быть реализовано. Если речь о краже денег, то это компьютер бухгалтера. Если речь об останове производства, то — какой-нибудь АСУ ТП-шный сервер или контроллер; если это, скажем, срыв контрактных обязательств, то речь может пойти о влиянии на систему контроля поставки товаров, к примеру, как это было в случае с Colonial Pipeline, когда фьючерсы на бензин выросли на 4%; или, например, когда взламываются системы доступа на крупное спортивное мероприятие и не работают системы fan-ID — это все примеры недопустимых событий, которые ретранслируются на ИТ-инфраструктуру. Задача безопасника, повторюсь, понять, как это может быть реализовано с точки зрения влияния на ИТ. И фокусировка на ключевых системах — а их очевидно гораздо меньше, чем всего узлов на инфраструктуре, позволит оптимизировать ресурсы и затраты, что является одной из ключевых задач в концепции результативной ИБ. Суть не только в том, что ИБ фокусируется на защите действительно важных объектов, но еще и экономит — людей, время и т.д.

Как определить главное — системы, в которых может закрепиться хакер и реализовывать недопустимые события? Вариантов существует несколько. Первый — исторический, когда сеть строилась «как-то» и никто не берет на себя смелость поменять это, потому что классический ИТ-шный принцип «работает — не трогай» нередко применяют и в ИБ. Второй вариант — попытаться оттолкнуться от требований регуляторов, которые говорят о необходимости определения контролируемой зоны, контура, сегмента, в которой нужно организовывать защитные меры. Третий вариант — ИТ-шный подход — провести сегментацию и микросегментацию, исходя из задач, которые реализует BisDev (это может быть физическая сегментация, виртуализация, контейнеризация, облачные инстансы и пр.). Ну, и, наконец, четвертый вариант — идти от недопустимых событий, хотя в этом случае суть не слишком сильно меняется. Скажем, когда сегментация проводится в соответствии с требованиями регулятора, это делается не просто, чтобы при аттестации или при проверке в дальнейшем не было проблем, а потому что при вдумчивом прочтении документов регулятора и учете негативных последствий в итоге сегментация все равно соответствует

системам, на которые скорее всего будет нацелен хакер. В этом случае сделать следующий шаг в сторону работы с недопустимыми событиями — совсем легко. Исключением является ситуация, когда сегментировали «исторически». Но опять же, без каких-либо изменений в подходе, ИБ не сможет сдвинуть эту гору с мертвой точки и доказать свою value для компании.

МЕЖДУ ХАРДЕНИНГОМ И МОНИТОРИНГОМ

Итак, недопустимые события определены, как и системы, в которых эти события могут быть реализованы. Следующий вопрос, на который надо ответить: «Как от всего этого защититься и какие защитные меры применять?». Здесь есть несколько вариантов. Во-первых, можно нейтрализовывать все эти недопустимые события на тех уровнях, на которых они проявляются (или благодаря которым они проявляются) — на уровне бизнес-процессов. Но обычно на этом уровне работает не ИБ, а другие подразделения и традиционно безопасники не слишком «любят» сюда идти. Во-вторых, это можно делать на уровне ИТ, — правильно выбирая технологии, правильно их сегментируя, устанавливая патчи и т.д. Но опять же традиционно это уровень ИТ, а не ИБ. В зоне ответственности ИБ чаще всего оказывается использование различных технологий обнаружения аномалий — EDR, SIEM, VM и т.д. — и с их помощью и надо выявлять то, что может привести к реализации недопустимых событий. Иногда это может тесно перекликаться с ИТ, иногда переплетаться с инжинирингом бизнес-процессов, но ситуация сильно зависит от того, каковы ресурсы, полномочия и зона ответственности конкретного CISO.

В любом случае, какой бы сценарий ни реализовывался — меняются ли бизнес-процессы, ИТ-инфраструктура, меняются ли решения в области информационной безопасности — все равно понадобится мониторинг. Он является неким контрольным мероприятием и позволяет убедиться, что инфраструктура не только правильно реализована (включая средства защиты), но и не допускает реализации недопустимых событий в процессе эксплуатации. Ну, и, конечно, здесь всегда будет некая дилемма — на чем сфокусироваться: закрутить гайки с точки зрения харденинга ИТ-инфраструктуры (и это больше ИТ-шный подход) или сделать фокус на мониторинге и реагировании. Речь о своеобразном балансе в зависимости от возможностей и ресурсов между харденингом, мониторингом и реагированием. В одном случае будут предотвращаться

события, которые приводят к недопустимым последствиям, во втором — будет максимально оперативное реагирование на эти события (когда первый шаг атакующим удался, но оперативная реакция на это не дает им шансов развить атаку дальше). Эту задачу решает центр противодействия киберугрозам (ЦПК). В отличие от традиционного SOC, который фокусируется на событиях безопасности, ЦПК базируется на идее недопустимых для бизнеса событий, и концепция выстраивается сверху вниз: определяется, что плохо для бизнеса, как это может быть реализовано в инфраструктуре, на каких системах это может быть реализовано, и мониторинг с реагированием фокусируется уже именно на них, а в ряде случаев делается и харденинг. Эта концепция позволяет достигать быстрых результатов, а не входить в историю, когда проекты растягиваются на 2–3–5 лет: выявили наиболее критичные недопустимые события, оперативно закрыли возможность их реализации, перешли к следующему пулу событий. В чем интересность такой концепции: закрывая недопустимые события, как правило, в большинстве случаев закрывают и все остальные нежелательные события в том числе. Потому что недопустимое от нежелательного часто отличается только размером ущерба: украли 50% денег со счета или 100 рублей со счета — технологически это одинаковое действие для злоумышленника.

КАК ПОДТВЕРДИТЬ, ЧТО НАМ НЕ ЗРЯ ПЛАТЯТ ЗАРПЛАТУ?

Как подтвердить, что все сделано правильно? Мы потратили немало времени и денег на то, чтобы выяснить, чего опасается бизнес, и сделали так, чтобы эти опасения не реализовались. Но как нам убедиться, что это действительно так? Мало просто сказать, что информационная безопасность реализована верно и соответствует лучшим мировым практикам. Главное — верифицировать невозможность реализации недопустимого события. Это можно сделать разными способами: с помощью пентестов, ред тиминга, киберучений, программ bug bounty — называть их можно как угодно, они разные, с разной методологией и командами, с юридически разными подходами и процедурами. Но результат они дают один — уверенность в том, что мы достигли результата, который понятен руководству компании, — хакеры не могут залезть внутрь и реализовать недопустимые для нас события. И в этом случае из самурая, у которого нет цели (только путь), мы превращаемся в службу ИБ, которая в прямом смысле слова готова отвечать за свои слова и демонстрирует это на практике.



Василий ПИСКАРЁВ
Председатель Комитета
Государственной
Думы по безопасности
и противодействию коррупции

«НАША ЗАДАЧА — УКРЕПИТЬ СУВЕРЕНИТЕТ, СОРВАТЬ ПЛАНЫ ЗАПАДА ПО УНИЧТОЖЕНИЮ РОССИИ»

ПРИЗЫВЫ К ФИНАНСИРОВАНИЮ ВРАГА БУДУТ БЛОКИРОВАТЬСЯ

В Государственную Думу депутатами, которые входят в Комиссию по расследованию фактов иностранного вмешательства, внесены поправки в Федеральный закон «Об информации, информационных технологиях и о защите информации». Они позволяют оперативно блокировать призывы к финансированию вооруженных сил Украины и других вооруженных формирований противника в условиях спецоперации.

Законопроектом предлагается принятие мер ограничения к информационным ресурсам, содержащим предложение о финансировании противника в условиях вооруженного конфликта, военных действий, контртеррористической операции или иных действий с применением вооружения и военной техники, участие в которых принимает Россия, а также сведения о возможных способах осуществления такого финансирования. Иногда такие сборы на вражескую армию объявляют, например, кафе или клубы — как это было летом в Москве. Внимание общественности тогда позволило оперативно пресечь такой сбор.

Любые призывы жертвовать деньги на противника, равно как и информация, как это сделать «безопасно», должны блокироваться. А виновные в этом должны быть привлечены к уголовной ответственности по ст. 275 Уголовного Кодекса РФ (санкция до 20 лет лишения свободы). Это вопрос безопасности нашей страны.

РАСПРОСТРАНЕНИЕ ФЕЙКОВ ОБ АРМИИ УДАЛОСЬ ПРЕСЕЧЬ

С самого начала специальной военной операции наш Комитет фиксировал многочисленные факты распростра-

нения заведомо ложной информации, просто вал фейковых новостей о ходе специальной военной операции, о количестве потерь наших войск и т.д. Понятно, что большинство таких фальшивок генерировалось на Украине. Тем не менее, они охотно распространялись рядом российских СМИ, а также пользователями в соцсетях. Массовый вброс фейков имел целью деморализовать общество, подорвать доверие к Российской Армии и силовым структурам, нанести удар по родным и близким бойцов.

Проанализировав эту информацию, обсудив с коллегами из Комитета по обороне, представителями фракций, мы пришли к выводу, что необходимо менять законодательство¹. Ведь одно дело, когда речь идет о мирном времени, а другое — когда наши военные выполняют важнейшие задачи по поддержанию мира и безопасности, пусть даже это происходит за рубежом.

В действующем законодательстве, как в Кодексе об административных правонарушениях, так и в Уголовном кодексе уже была установлена ответственность за распространение заведомо ложной информации. Речь в этих статьях шла о действиях в условиях чрезвычайных ситуаций и терактов, когда такая информация может вызвать панику. Также два года назад мы дополнительно ввели ответственность за распространение заведомо ложной общественно значимой информации о пандемии.

С учетом опыта правоприменения мы предложили дополнить эти же статьи положением об ответственности за

¹ Федеральный закон от 4 марта 2022 г. №31-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» (ст. 20.33 КоАП). Федеральный закон от 4 марта 2022 г. №32-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации» (ст. 2073 и ст. 2803 УК РФ).



искажение цели, роли и задач Вооруженных Сил РФ, а также других формирований во время специальных военных и иных операций. Первая часть предложенных нами поправок касалась изготовления фейков и их распространения, за эти деяния предусмотрено наказание до трех лет лишения свободы. Если подобная деструктивная деятельность осуществляется с использованием служебного положения, в группе или организованной группе лиц, с использованием интернета и других возможностей широкого распространения, то тогда наказание будет выше, от пяти до 10 лет лишения свободы. Если лицо, распространяющее фейки, заведомо знает, что они ложные, и они получили общественно опасные последствия, в этом случае наказание будет более суровым — до 15 лет лишения свободы.

Отмечу, что прошедшие с момента вступления в силу этих поправок месяцы показали правильность принятых решений. Они сыграли свою роль, сбив вал фейков, которые исчислялись миллионами единиц информации, и выполнили важную профилактическую функцию, остудив пыл некоторых поддавшихся эмоциям блогеров, тиражировавших непроверенную информацию.

При необходимости мы и дальше продолжим совершенствовать законодательство в этой сфере. Мы хотим сделать все, чтобы те, кто находится в тылу, не стрелял в спину нашим бойцам.

УЧАСТНИКИ СВО И ИХ СЕМЬИ ПОЛУЧАТ ПОДДЕРЖКУ

Отмечу, что с конца февраля Государственной Думой принято более 20 федеральных законов, связанных с

проведением специальной военной операции. Они направлены на совершенствование условий прохождения службы и поддержку военнослужащих. В частности, мы распространили статус ветерана боевых действий на лиц, выполнявших задачи в ходе специальной военной операции на территориях Украины, Донецкой Народной Республики и Луганской Народной Республики с 24 февраля 2022 г., включая военных корреспондентов.

Приняты важные федеральные законы, которые защищают трудовые права мобилизованных и добровольцев. Так, за ними сохраняется рабочее место, должность, а также социально-трудовые гарантии на весь период военной службы². Мобилизованным, контрактникам, а также заключившим контракт о добровольном содействии в выполнении задач, возложенных на Вооруженные Силы, и тем, кто находится у них на иждивении, предоставляются кредитные каникулы³. В случае гибели военнослужащего или получения им первой группы инвалидности предусмотрено полное прекращение обязательств по его кредитным договорам.

Кроме того, Государственной Думой принят закон об освобождении мобилизованных и членов их семей от пеней

² Федеральный закон от 7 октября 2022 г. N376-ФЗ «О внесении изменений в Трудовой кодекс Российской Федерации».

³ Федеральный закон от 7 октября 2022 г. N377-ФЗ «Об особенностях исполнения обязательств по кредитным договорам (договорам займа) лицами, призванными на военную службу по мобилизации в Вооруженные Силы Российской Федерации, лицами, принимающими участие в специальной военной операции, а также членами их семей и о внесении изменений в отдельные законодательные акты Российской Федерации».

за просрочку оплаты услуг ЖКХ и взносов за капремонт⁴. Работу по совершенствованию законодательства мы продолжаем. Сделаем всё необходимое, чтобы участники специальной военной операции были уверены, что за спиной у них крепкий тыл, а их семьи получают необходимую поддержку.

ГОСУДАРСТВЕННАЯ ТАЙНА ПОД ЗАЩИТОЙ

Также в этом году мы дополнили Уголовный кодекс РФ нормой⁵ об ответственности за нарушение требований по защите государственной тайны. Так, гражданину, который имеет допуск к гостайне и право которого на выезд из РФ ограничено законом, за нарушение ограничений будет грозить штраф от 200 тыс. до 500 тыс. руб. либо лишение свободы сроком до трех лет.

Законодательство уже предусматривает ограничения на выезд за рубеж для тех должностных лиц и сотрудников силовых структур, которые имеют допуск к гостайне, — он возможен лишь по согласованию с руководством. Мы же своей поправкой установили ответственность за нарушение данного ограничения. Это, с одной стороны, позволит дополнительно защитить безопасность страны — разведки недружественных России стран даже не скрывают того, что активно ищут потенциальных информаторов и шпионов. С другой, это обезопасит и самих чиновников, сотрудников правоохранительных органов, которые, находясь за рубежом, могут стать жертвами провокаций иностранных спецслужб.

Действие новой нормы коснется не только действующих сотрудников, но и тех, кто ушел со службы — ограничения, связанные с допуском к гостайне, действуют в течение пяти лет после увольнения.

Также, в соответствии с поправками, для имеющих доступ к гостайне устанавливается уголовная ответственность за перемещение и пересылку носителей закрытой информации за рубеж. За это будет грозить до четырех лет тюрьмы, если данное деяние не содержит признаков более тяжких преступлений — госизмены и шпионажа.

Принятие предложенного нами комплекса мер послужит укреплению безопасности и суверенитета нашей страны, окажет поддержку нашей армии и государству в условиях проведения специальной военной операции и санкционного давления извне.

ХОЧЕШЬ ПОБЕДИТЬ ВРАГА, ВОСПИТАЙ ЕГО ДЕТЕЙ

Одним из наиболее важных решений Государственной Думы в этом году стало принятие федерального закона «О контроле за деятельностью лиц, находящихся под иностранным влиянием»⁶. Он вступает в силу в декабре.

⁴ Федеральный закон от 7 октября 2022 г. N378-ФЗ «О внесении изменений в статьи 166 и 169 Жилищного кодекса Российской Федерации и Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации».

⁵ Федеральный закон от 14.07.2022 № 260-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации».

⁶ Федеральный закон от 14 июля 2022 г. N255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием».

При подготовке законопроекта было учтено, что действующее законодательство об иностранных агентах содержит разрозненные положения, которые закреплены в четырех федеральных законах, и, как показывает практика, такое разрозненное и такое многомасштабное закрепление норм в нескольких законодательных актах не очень удобно для правоприменения.

В частности, мы предложили имеющиеся сейчас четыре реестра иностранных агентов упорядочить и сделать единый реестр с тем, чтобы было удобнее нашим гражданам обращаться к нему и видеть, какие у нас субъекты являются иностранными агентами. Законом также определен порядок включения в реестр, и что очень важно, — здесь мы пошли навстречу пожеланиям общественности, — порядок исключения из реестра. Появился дополнительный реестр лиц, аффилированных с иностранными агентами.

Важным нововведением стало введение запрета влияния иностранных агентов на детей в Российской Федерации, в какой бы то ни было форме. Что имеется в виду? Иностранцам запрещено осуществлять преподавательскую, просветительскую, воспитательную деятельность в отношении несовершеннолетних, производить информационную продукцию для несовершеннолетних. Почему возникла необходимость введения такого института как запрета на работу с детьми иностранных агентов?

В качестве примера приведу распространявшуюся посредством интернета методичку, которая называется «Азбука антикоррупционера». Она разработана организацией — иностранным агентом для российских школьников. Идея благородная. Я сам всегда выступал за то, чтобы антикоррупционное просвещение начинать как можно раньше, еще со школы, когда у ребят формируются моральные принципы. Но если внимательно ее изучить, то выяснится, что «азбука» эта содержит ссылки на экстремистские сайты, и если ребенок обратится к этим сайтам, то там он увидит, как организовывать массовые беспорядки, как выходить на улицу и участвовать в незаконных акциях, которые могут угрожать его жизни и здоровью, потому что ребенок на улице на несанкционированном мероприятии всегда находится в состоянии уязвимом.

Ради справедливости должен заметить, что после моего выступления, где я продемонстрировал эту книжку, сработала обратная связь, и мы получили ответ от авторов издания. Они удалили противоправную информацию и сообщили нам об этом. Не скрою, для нас это очень важно, в том числе и потому, что Комиссия не ставит своей целью что-либо запрещать или блокировать. Главное требование, которое мы предъявляем к иноагентам, — соблюдение наших законов.

Но данный случай «исправления ошибок» — это скорее исключение из правил, потому что книжек таких, нацеленных на наших детей, еще много. К примеру, Комиссия выявила ряд изданий иноагентов, с помощью которых наших детей, даже школьников младших классов, избыточно «просвещают», раздавая брошюры о том, какие бывают наркотики и как они действуют, как называются в наркоманской среде, и попутно убеждают в допустимости наркопотребления, подводя к мысли о возможности легализации наркотиков.



На снимках: Заседание Комиссии Государственной Думы по расследованию фактов вмешательства иностранных государств во внутренние дела России

Убедительный пример, к чему всё это может привести, дает Украина. Наши депутаты и эксперты проанализировали более 300 книг и методических рекомендаций для учащихся и педагогов Незалежной. И пришли к выводу: большинство их учебников пропитаны ненавистью к России. Это отражает целенаправленную работу по воспитанию подрастающего поколения Украины в духе отрицания общей истории и возбуждения ненависти ко всему русскому. В процесс обучения детей на Украине вмешались иностранные агенты. И это ни в коем случае не должно повториться в России!

МИЛЛИАРДЫ ДЛЯ ТРОЯНСКИХ КОНЕЙ

Меня часто спрашивают, почему нас так беспокоит деятельность иноагентов, если их число невелико на фоне других НКО, действующих в сфере решения социальных проблем, науки, культуры, образования? В первую очередь, потому что именно эти организации пытаются активно воздействовать на внутривнутриполитическую ситуацию в нашей стране, влиять на результаты выборов, на нашу молодежь. Действия в таких чувствительных сферах не могут оставаться вне внимания и контроля со стороны государства и общества, тем более что на эти цели из-за рубежа вливаются огромные деньги. Так, по данным Минюста России, после включения в реестр иноагентов, эти НКО продолжают активно получать денежные средства из иностранных источников, что свидетельствует о сохраняющемся интересе к ним иностранных грантодателей.

Если вы посмотрите на английский перевод термина «иностранный вмешательство», то он звучит очень символично — «foreign intervention». Мы сегодня переживаем именно интервенцию, когда Запад закачивает в Россию огромные деньги на цели, которые расходятся с интересами нашего государства и представляют угрозу суверенитету страны.

По данным Минюста РФ, в прошлом году на счета НКО-иноагентов поступило около одного миллиарда рублей. И это

только официально задекларированные средства. Мы не знаем, сколько еще денег поступает к ним в наличной форме, в виде дебетовых карт и как-то еще через различных посредников. По экспертным оценкам, за последние два десятилетия таким образом в нашу страну поступили десятки миллиардов долларов. А с началом специальной военной операции такое финансирование резко увеличилось. При этом многие зарубежные фонды и организации под благозвучными названиями, которые спонсируют деятельность иноагентов в России, имеют недобрую славу организаторов «цветных» революций в десятках иностранных государств.

ЦЕЛИ И СРЕДСТВА ДОЛЖНЫ БЫТЬ ПРОЗРАЧНЫМИ

В самом факте поступления средств из-за рубежа нет ничего зазорного, если расходуются они открыто и с добрыми намерениями. Только вот нельзя не заметить, что, щедро направляя средства, как любят в США указывать их назначение, «на развитие демократии», зарубежные спонсоры поощряют своих грантополучателей к откровенно провокационным действиям под видом правозащиты, отрицанию действующих законов и Конституции нашей страны, поддержке экстремистских и националистических течений.

Всё это для нас неприемлемо. Именно поэтому мы хотим сделать деятельность лиц и организаций, занимающихся политической деятельностью в интересах иностранных государств, предельно прозрачной, понятной обществу и соответствующей требованиям наших законов, а зарубежные деньги, раз уж они приходят этим организациям даже в условиях санкций, использовались во благо нашей страны и общества, а не во вред.



Андрей МАКОСКО
вице-президент
по информационной безопасности
АО АКБ «НОВИКОМБАНК»

ИЗМЕНЕНИЕ СТРУКТУРЫ

НОВЫЕ «АКЦЕНТЫ» ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ИБ

Осложнение внешнеполитической обстановки, продолжение пандемии, перевод сотрудников на удалённый режим работы, активное внедрение новых технологий, финансовый кризис становятся предпосылками для роста компьютерной преступности. Для снижения киберрисков и повышения значимости вопросов кибербезопасности в организациях со стороны Государства произошли изменения законодательства с расстановкой новых «акцентов», были разработаны Указ Президента РФ № 250 от 01.05.2022 и Постановление Правительства № 1272 от 15.07.2022.

Указ и Постановление распространяются на:

- ♦ федеральные органы исполнительной власти;
- ♦ высшие исполнительные органы государственной власти субъектов РФ;
- ♦ государственные фонды;
- ♦ государственные корпорации и государственные компании, созданные РФ на основании федеральных законов;
- ♦ стратегические предприятия;
- ♦ стратегические акционерные общества;
- ♦ юридические лица, являющиеся субъектами критической инфраструктуры (далее — КИИ), т.е. подпадающие под действие Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

С учётом последнего пункта и определения субъектов КИИ из 187-ФЗ Указ, по сути, распространяется на большинство предприятий России (по некоторым экспертным оценкам — до 90% всех предприятий).

Согласно Указу, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации, к которым, в соответствии с п. 8 ст. 2 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», относятся и все кредитные организации, необходимо возложить на заместителя руководителя организации полномочия по обеспечению информационной безопасности, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты (далее — Заместитель руководителя).

Об этом также указано в п. 2 Приказа Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 10 марта 2022 г. № 186 «Об утверждении методических рекомендаций по обеспечению необходимого уровня безопасности в сфере информационно-коммуникационных технологий государственных корпораций, компаний с государственным участием, а также их дочерних организаций и зависимых обществ». Данный приказ распространяется, конечно, на более ограниченное число компаний.

Кроме того, необходимо создать в каждой организации структурное подразделение, осуществляющее функции по обеспечению информационной безопасности организации, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение. Для банков, как правило, это не является проблемой, так как уже давно в каждом из них функционирует такое подразделение, в организациях же, относящихся к другим отраслям, даже одного специалиста может не быть, не говоря уже о подразделении.

Подразделение должно быть подчинено заместителю руководителя организации, ответственному за обеспечение информационной безопасности в организации, либо иным лицам из состава руководства организации — при условии осуществления курирования со стороны руководителя организации (рис. 1).

Изменение структуры обеспечения ИБ — необходимый и важный этап развития системы обеспечения информационной безопасности организации для повышения эффективности и управляемости, обеспечивающий защиту от киберугроз. В среднем подразделением информационной безопасности крупной организации администрируются и проводится несколько десятков систем обеспечения защиты информации, и их количество постоянно растёт (антивирусы, защита почты, доступ в интернет, DLP, SIEM, система анализа защищённости, антифрод-системы, УЦ, криптография, MDM и т.д.).

В общем случае (с учётом собственного опыта и рекомендаций СТО БР ИББС) в деятельности подразделения



Рисунок 1. Структура обеспечения информационной безопасности в организации

информационной безопасности можно выделить следующие ключевые направления:

- ♦ «методология»;
- ♦ «реализация и сопровождение»;
- ♦ «контроль»;
- ♦ «криптографическая защита».

Указ позволяет также в случае необходимости привлекать сторонние организации к осуществлению мероприятий по обеспечению информационной безопасности организации, при этом обязательно наличие у них лицензии на осуществление деятельности по технической защите конфиденциальной информации. Можно привлекать сторонние организации и к осуществлению мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, но речь идёт исключительно об организациях, являющихся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.

Отдельно стоит упомянуть про разрешённый ФСБ России доступ, в том числе удалённый, к принадлежащим организациям ресурсам в целях осуществления мониторинга и необходимость обеспечивать незамедлительную реализацию организационных и технических мер, решения о необходимости которых будут приниматься Федеральной службой по техническому и экспортному контролю в пределах их компетенций. Пока непонятно, как будет осуществляться этот доступ.

Указ возлагает на руководителей организаций персональную ответственность за обеспечение информационной безопасности, которую необходимо зафиксировать в трудовых договорах и должностных инструкциях.

Правительство РФ в соответствии с п. 3 Указа разработало и утвердило Постановление № 1272, содержащее типовое

положение о Заместителе руководителя, ответственном за обеспечение информационной безопасности, и типовое положение о структурном подразделении ИБ.

Обязательным является наличие высшего образования в области информационной безопасности или соответствующей профессиональной переподготовки по направлению ИБ, знаний, умений и профессиональных компетенций в области ИБ.

В последние полгода существенно вырос спрос на специалистов по кибербезопасности. Недостаток квалифицированных кадров только нарастает. Где взять столько специалистов? По оценке ФСТЭК, необходимо более 500 тысяч специалистов, а вузов, готовящих таких специалистов, недостаточно. С переподготовкой тоже не всё так просто: необходимо не менее 500 часов с учётом требований для получения лицензий ФСБ и ФСТЭК, это 4 месяца учёбы. Заместителю по информационной безопасности это, возможно, и не нужно, но других требований к объёму переподготовки пока нет.

Интересный пункт Положения: «Указания и поручения ответственного лица в части обеспечения информационной безопасности являются обязательными для исполнения всеми работниками», то есть у заместителя по ИБ появляются дополнительные права и возможность добиваться от работников организации определённых действий.

Шестой пункт Указа — импортозамещение средств защиты — отдельная большая тема. С 1 января 2025 г. организациям запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

Таких стран более 20, с учётом аффилированности — гораздо больше. Получается, что практически любые иностранные средства защиты информации будут под запретом, и остаётся немногим более двух лет для перехода на российские средства защиты информации.

А импортозаместиться в текущих условиях непросто. Отечественные производители по ряду направлений защиты оказались не готовы предоставить аналогичные западным решения, со схожими характеристиками и функциональностью. Речь идёт, например, о межсетевых экранах и шлюзах доступа в интернет (замена Cisco, Palo Alto, Check Point и т.д.). Отечественные решения отстают в возможностях и характеристиках, при этом их стоимость сопоставима со стоимостью зарубежных аналогов, а порой и превышает её. Естественно, и процесс миграции также может занять не один год — в случае, если отсутствуют инструменты или технологические возможности по его оптимизации/автоматизации.

Проблемы с импортозамещением для некоторых систем могут привести к существенному снижению уровня защищённости. Чтобы это компенсировать, необходимо привлечь дополнительные ресурсы, а также разработать для вендоров механизм заинтересованности в улучшении их продуктов — через гранты, субсидии и другие преференции, разумеется, параллельно с системой контроля за результатами.

Стоит также отметить инициативы по составлению каталогов, в которых для западного ПО указываются замещающие их отечественные решения. Например, такой каталог достаточно оперативно выпустила АРПП «Отечественный софт». Понятно, что такая работа только начата, но её надо обязательно поощрять и развивать.

Начинать же, безусловно, нужно с Плана импортозамещения средств защиты.

Также необходимо подумать о переходе на отечественные решения и для остального ПО, так как есть проблемы с покупкой лицензий, обновлением ПО, «неприятностями» в виде различных закладок и т.п. Прямого запрета на использование иностранного ПО пока нет, но здравый смысл подсказывает, что лучше подстраховаться, и сделать это заранее. Кстати, госорганам и субъектам КИИ, имеющим значимые объекты инфраструктуры, Указом Президента РФ № 166 от 30.03.22 уже запрещено использование любого иностранного ПО с 1 января 2025 года.

Изменения законодательства, касающегося обеспечения информационной безопасности предприятий, безусловно, своевременны и разумны: в условиях новых вызовов они становятся ключевыми факторами достижения технологической независимости России.



АССОЦИАЦИЯ
БАНКОВ
РОССИИ

VIII Банковская юридическая конференция «Банки в эпоху кардинальных перемен: аспекты права»

1-2 декабря 2022 года

Гибридный формат - с возможностью очного и онлайн-участия

Оргкомитет:
Тел. +7 (495) 785-29-93, 785-29-88
e-mail: event@asros.ru
www.asros.ru



**Сергей ВИХОРЕВ**

советник генерального директора
ООО «ИТ-Экспертиза»

ЧТО ДЕНЬ ГРЯДУЩИЙ НАМ ГОТОВИТ?

РАЗМЫШЛЕНИЯ НАД ОЧЕРЕДНЫМИ ПОПРАВКАМИ К ЗАКОНУ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»¹

Вот и ещё новые правки в закон «О персональных данных», большинство из которых вступили в силу с 1 сентября этого года. Это уже 28-е изменения за 13 лет существования этого закона. Много? Да, много, но это говорит лишь о том, что закон актуальный, необходимый, затрагивающий важнейшие для личности сущности. Правда, на этот раз изменения не такие заметные, как в 2011 году, когда была уточнена сфера действия закона, основные понятия, принципы и условия обработки персональных данных, а также были существенно переработаны нормы, касающиеся трансграничной передачи ПД, мер обеспечения их безопасности, прав и обязанностей оператора, взаимоотношений оператора и субъекта персональных данных. Но всё же и в новых правках многие из этих аспектов опять затрагиваются. Я не буду пересказывать все изменения, появившиеся в новой редакции: до меня уже многие эксперты об этом рассказали. Кому интересно — можно найти в Интернете (правда, осмысления этих поправок маловато будет). И всё же...

О САМОМ ГЛАВНОМ

Пробраться к сути сквозь казённый язык новелл закона непросто. Попробую своим языком, как я вижу, выделить главные новшества (см. Таблицу 1). А кому интересно — может обратиться к тексту подлинника закона.

Кроме того, уточняются некоторые дефиниции закона, но, на мой взгляд, это не так критично. Вместе с тем, думаю, самым

главным, что может отразиться на операторах персональных данных, являются два момента: коренное изменение списка исключений, позволяющих обрабатывать персональные данные без уведомления Роскомнадзора, и полное изменение процедуры трансграничной передачи персональных данных.

Исключение из случаев обработки персональных данных без уведомления, обработки в соответствии с трудовым законодательством и в связи с заключением договора, стороной которого является субъект персональных данных, приведёт к тому, что любое юридическое лицо, от детского садика до государственной корпорации, будет обязано делать уведомление в Роскомнадзор. Всего в реестре ЕГРЮЛ² числится около 3 миллионов юрлиц. А ещё есть индивидуальные предприниматели... С одной стороны, мы стремимся к цифровизации и обмену информацией между ведомствами, чтобы не заставлять людей собирать различные справки, которые есть в другом ведомстве, а с другой — закон практически определяет необходимость ведения реестра операторов персональных

² ЕГРЮЛ — Единый государственный реестр юридических лиц.

Два главных момента, которые могут отразиться на операторах ПДн: коренное изменение списка исключений, позволяющих обрабатывать ПДн без уведомления Роскомнадзора, и полное изменение процедуры трансграничной передачи ПДн

¹ Федеральный закон от 14.07.2022 № 266-ФЗ.

Наиболее важные новшества	Чем грозят новшества
Расширена юрисдикция закона (ст. 1)	Теперь закон действует и на иностранных лиц, обрабатывающих ПДн российских граждан
Расширены требования к поручению на обработку ПДн для обработчика (ст. 6)	БД ПДн обработчика должны быть на территории РФ Обработчик обязан документально подтвердить выполнение мер для выполнения поручения Обработчик обязан принимать организационные и технические меры для защиты персональных данных Обработчик обязан в случае неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн уведомлять Роскомнадзор
Кардинально изменён порядок трансграничной передачи ПДн (ст. 12) (вводится с 01.03.2023)	Роскомнадзор утверждает перечень иностранных государств, обеспечивающих адекватную защиту Роскомнадзору дано право в определённых случаях запретить или ограничить трансграничную передачу Оператор до начала трансграничной передачи: проводит оценку соответствия иностранным оператором, конфиденциальности ПДн и обеспечения их безопасности; получает от иностранных контрагентов сведения о мерах защиты ПДн и правовом регулировании оборота ПДн; уведомляет Роскомнадзор о намерениях. После направления уведомления оператор: может осуществлять трансграничную передачу на территорию государств, подписавших Конвенцию; не может в течение 10 дней или до получения от иностранного контрагента сведений о мерах защиты осуществлять трансграничную передачу для государств, не являющихся стороной Конвенции Совета Европы; при получении запрета от Роскомнадзора на трансграничную передачу оператор обязан обеспечить уничтожение иностранным контрагентом переданных ПДн
Определены сроки предоставления сведений субъекту ПДн (ст. 14, 20)	Установлен срок в 10 дней с возможностью продления ещё на 5 дней
Расширен перечень информации, которой может получить субъект от оператора (ст. 14)	Субъект может запросить информацию о принимаемых мерах по обеспечению безопасности ПДн
Изменён статус принимаемых мер по выполнению требований закона (ст. 18.1)	Теперь такие меры перешли из статуса рекомендательных в статус обязательных (императивная норма)
Уточнён порядок оценки вреда (ст. 18.1)	Роскомнадзор определяет требования к оценке вреда
Дополнены меры по обеспечению безопасности ПДн (ст. 19)	Вводится обязанность оператора обеспечить взаимодействие с ГосСОПКА
Вводятся обязанность и жёсткие сроки уведомления об инцидентах (ст. 21)	Вводятся жёсткие сроки уведомления об инцидентах (24 часа и 72 часа для расследования)
Резко сокращён список исключений, когда возможно обрабатывать ПДн без уведомления Роскомнадзора (ст. 22)	Главное: исключена обработка в соответствии с трудовым договором. Теперь все должны уведомлять
Расширены права Роскомнадзора (ст. 23)	Функции по контролю и надзору за соответствием обработки персональных данных теперь реализуются Роскомнадзором самостоятельно (без Минцифры)

Таблица 1. Наиболее важные новшества в законе «О персональных данных» (ФЗ-266), вступившие в силу 1 сентября этого года

данных, который по своей сути дублирует ЕГРЮЛ. Оправдано ли это? Не знаю.

Изменение процедуры трансграничной передачи персональных данных, конечно, усиливает защиту интересов субъектов. Но, с другой стороны, обязывает оператора, во-первых, получать от зарубежных контрагентов информацию о принимаемых мерах по защите передаваемых персональных данных и об условиях прекращения их обработки, а также информацию о правовом регулировании в области персональных данных в чужом государстве. Кроме того, оператора обязывают, при запрете со стороны Роскомнадзора на трансграничную передачу, обеспечить уничтожение иностранным контрагентом ранее переданных им персональных данных. Интересно, как оператор со своими маломощными силами, да ещё в непростой международной обстановке сможет это сделать? Наверное, будем ждать разъяснений от Роскомнадзора, всё-таки до марта 2023 года время ещё есть.

ФЕДОТ, ДА НЕ ТОТ

А теперь не о самом законе, а о тех подзаконных актах, которые грядут с его вступлением в силу. В новой редакции статьи 18.1 введено новое и очень важное дополнение: оценка вреда субъекту персональных данных проводится оператором в соответствии с требованиями, установленными Роскомнадзором. Отрадно, что Роскомнадзор весьма оперативно опубликовал проект приказа «Об утверждении Требований к оценке вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» (невиданная оперативность, заслуживающая похвалы). Но вот внимательное знакомство с этим проектом наводит на размышления. Дело в том, что критерием оценки вреда в нём определяется нарушение процедуры обработки персональных данных, которая описана в законе.

Однако статья 2 закона определяет его целью обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. То есть вред субъекту от нарушения закона будет именно от нарушения его прав и свобод.

А что такое вред с юридической точки зрения? Гражданский кодекс РФ не содержит легального определения понятия вреда, но по смыслу ст. 1064 ГК РФ вред рассматривается как всякое умаление охраняемого законом материального или нематериального блага, любое неблагоприятное изменение в охраняемом законом благе, которое может быть имущественным или неимущественным (нематериальным)³. Одним из традиционных условий ответственности за причинение вреда является причинная связь между противоправным поведением и наступившим вредом. То есть противоправное поведение (читай нарушение процедуры обработки персональных данных) и вред — суть разные сущности. Противоправное поведение — это компетенция

В новой редакции статьи 18.1 введено новое и очень важное дополнение: оценка вреда субъекту персональных данных проводится оператором в соответствии с требованиями, установленными Роскомнадзором

КоАП РФ или УК РФ, а вред — это то, что требует денежной компенсации (как материального, так и морального вреда). Тогда и оценивать вред надо именно с точки зрения возможной компенсации. Ну если с материальными потерями более или менее ясно (например, в результате утечки персональных данных была проведена незаконная сделка по продаже квартиры), то с моральным вредом сложнее.

Моральный вред, в частности, может заключаться⁴ в нравственных переживаниях в связи с:

- ♦ раскрытием семейной, врачебной тайны;
- ♦ распространением не соответствующих действительности сведений, порочащих честь, достоинство или деловую репутацию гражданина;
- ♦ временным ограничением или лишением каких-либо прав.

А если гражданину причинён моральный вред, на нарушителя может быть возложена обязанность денежной компенсации указанного вреда⁵.

А какой вред может быть, например, от «несоблюдения оператором требований по представлению мотивированного ответа с отказом в представлении субъекту персональных данных или его законному представителю информации о наличии персональных данных о соответствующем субъекте» (так в проекте приказа Роскомнадзора) или «несоблюдение оператором требований по опубликованию или обеспечению неограниченного доступа к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных»? Да, процедура нарушена, наказать виновного, наверное, надо. Но к какому вреду это может привести и каков размер вреда, причинённого в результате таких действий? Разве это привело к раскрытию семейной тайны или распространению не соответствующих действительности сведений, порочащих честь, достоинство или деловую репутацию гражданина? Не надо путать причину и следствие. Так что, на мой взгляд, проект приказа Роскомнадзора требует существенной корректировки и изменения критериев оценки вреда. Будем надеяться, что Роскомнадзор это услышит.

⁴ Постановление Пленума Верховного Суда РФ от 20.12.1994 № 10 (ред. от 06.02.2007).

⁵ Гражданский кодекс РФ, ст. 151.

³ Определение Верховного Суда РФ от 27.01.2015 N81-КГ14-19.

**Алексей ПЛЕШКОВ**

заместитель
начальника
департамента
защиты информации
Газпромбанка

«ИБ НА ГЛАЗАХ ПРЕВРАТИЛАСЬ В БИЗНЕС- ПРЕИМУЩЕСТВО»

СЕМЬЯ И РАБОТА ИНТЕРЕСНЕЕ
ЛЮБОГО ХОББИ

Отрасль должна знать своих героев. В новой рубрике «Собеседник» BIS Journal представит наших современников — известных CISO банковской сферы. Возглавить этот неформальный парад мы пригласили Алексея Плешкова, заместителя начальника департамента защиты информации Газпромбанка. Алексей окончил МИФИ в 2006 году и с тех пор бессменно строит информационную безопасность Газпромбанка.

О РЫНКЕ

— Алексей, поделитесь, пожалуйста, вашей точкой зрения: что сейчас реально происходит на рынке информационной безопасности в России?

— Рынок ИБ на подъёме. Иностранные компании из России ушли, оставив ниши, которые начинают занимать наши соотечественники, причём не только крупные компании, но и никому не известные стартапы. Заказчики стали интересоваться не только дорогостоящими масштабными решениями, но и инновационными проектами, которые можно быстро доработать и адаптировать под текущие нужды.

Всерьёз заговорили о реализации стратегии импортозамещения. Большую роль в этом, конечно, сыграли известные указы Президента РФ. Сроки в них обозначены самые сжатые — до начала 2025 года. Для рынка это мощный катализатор.

ОБ ИЗМЕНЕНИЯХ

— У вас большой опыт в сфере ИБ. Как изменились типы кибератак за последние месяцы?

— Кибератаки разного типа были и будут всегда. Единственное, что меняется и расширяется, — это модель нарушителя и сценарии атак. Сегодня за счёт расширения модели нарушителя

и новых участников в киберпреступных сообществах количество атак увеличилось в десятки раз. Объекты внутри защищённого периметра любой финансовой организации сегодня атакуются постоянно.

Сместился фокус атак. Если раньше он лежал в области мошенничества и несанкционированных финансовых операций, то сегодня — это нарушение доступности для всех видов сервисов, предоставляемых банками через интернет. DOS-атаки, DDOS-атаки, дефейсы, взломы баз данных, получение доступа к админским панелям — весь этот спектр атак через интернет применяется прямо сейчас, во время нашего разговора. Тут Газпромбанк не исключение.

— Как происходящие изменения отразились на работе ИБ-команд в целом и команды Газпромбанка в частности?

— Если раньше бизнес воспринимал события ИБ как нечто фантастическое, сродни сценариям каких-то голливудских фильмов, то сегодня он воспринимает их более серьёзно. Раньше бизнес рассуждал примерно так: «Ваши ограничения избыточны, они не позволяют нам зарабатывать деньги» или «Эти риски ИБ никогда не реализуются на практике» и т.д. Сейчас все видят результаты действий злоумышленников, поэтому со стороны и бизнеса и ИТ-подразделений есть и понимание, и поддержка ИБ.

Раньше можно было слышать: «Незарабатывающее подразделение не должно много тратить». Сейчас таких аргументов стало гораздо меньше даже по сравнению с 2021 годом. Диалог стал адекватнее — ИБ на глазах стала превращаться в бизнес-преимущество. Банк, способный защитить свои продукты, сегодня получает неоспоримый авторитет у клиентов и, как следствие, плюс в конкуренции на рынке.

О СПЕЦИФИКЕ ГАЗПРОМБАНКА

— Какие основные задачи вы решаете, будучи заместителем начальника департамента защиты информации?

— В сферу нашего департамента входит эксплуатация и сопровождение разных средств защиты информации в рамках деятельности банка. У нас есть направления, связанные с сетевой безопасностью периметра, противодействием кибератакам из интернета, защитой каналов связи, обеспечением ИБ в платёжных системах и процессах. Сопровождаем средства криптографической защиты. Важная задача — администрирование комплексной системы технической безопасности объектов. Обеспечиваем режим ИБ применительно к внутренним процессам, сопровождаем средства защиты информации на рабочих станциях, расследуем инциденты, связанные с инсайдерами. Отвечаем за проведение мероприятий в соответствии с требованиями 187-ФЗ, управляем процессом безопасной обработки персональных данных согласно требованиям 152-ФЗ/266-ФЗ и т.д. и т.п.

Вся эта деятельность не ограничивается Москвой. В зоне ответственности нашего департамента вся филиальная сеть Газпромбанка, а это более 350 отдельных площадок по всей России.

— Как вы считаете, Газпромбанк защищён лучше других организаций на финансовом рынке или нет?

— Чтобы определить, лучше или хуже, должна быть согласованная всеми сторонами метрика. Пускай это будет уровень безопасности. К сожалению, есть много организаций, где специалистов по ИБ можно перечесть на пальцах одной руки, и такой штат не позволяет полноценно решать задачи ИБ. Это в основном банки за пределами топ-50. Их нельзя обвинять — они выполняют свои задачи стойко, исходя из имеющихся возможностей. Тем не менее по результатам проверок ЦБ там регулярно выявляются нарушения, так как у них нет необходимых систем, методологии, бюджета, штата...

У нас возможность заниматься безопасностью есть, и мы стараемся использовать её в полной мере. Например, сразу на стадиях проектирования новых банковских продуктов. Специалисты нашего блока участвуют в проработке технических заданий на такие продукты, формируют их безопасность на стадиях тестирования, доработок, то есть на всём пути от идеи до внедрения. Сегодня такой подход применяют не только в нашем банке, а везде, где уровень зрелости ИБ достаточно высокий.

Однако даже самая защищённая новая система без должного управления уязвимостями, без

постоянных проверок на наличие логических дыр очень быстро устаревает и становится потенциальной угрозой, особенно если речь идёт о системах, доступных из интернета. По-моему, специалисты по ИБ должны принимать участие во всех бизнес-процессах, чтобы не быть догоняющими, а иметь техническую возможность и запас времени, чтобы превентивно устранять как видимые, так и потенциальные угрозы.

— Специфика деятельности Газпромбанка накладывает какой-то отпечаток на решение ваших задач?

— Конечно. В 2016–2017 годах стратегия нашего банка изменилась в сторону розничного направления бизнеса. Это повлекло изменение банковских продуктов и систем и, как следствие, изменение подходов к обеспечению ИБ. Если раньше мы исходили из принципа: всё, что не разрешено, то запрещено, то теперь мы изменили подход с запрещающего на предполагающий изучение, оценку и управление рисками ИБ. Это позволяет быстро внедрять и развивать новые банковские продукты, минимизируя риски.

О ТЕХНОЛОГИЯХ

— Стек технологий, используемых в ИБ, постоянно меняется. Какие технологии вы считаете самыми современными и актуальными? Какие из них активно используете?

— На мой взгляд, стек технологий в ИБ меняется только потому, что меняются аббревиатуры в названиях и маркетинговая составляющая этих названий. Техническая составляющая и суть остаются прежними. Большинство решений, которые сейчас активно рекламируются и продаются, — это, по сути, те же решения 5–7-летней давности, с которыми мы работали и продолжаем работать. Изменили название, добавили актуальную функциональность, и вдруг они стали чем-то новым.

Что касается актуальности продуктов, тут каждый банк выбирает для себя сам, исходя из своих бизнес-процессов, ИТ-инфраструктуры. Если это маленький региональный банк, то для него актуален и базовый набор продуктов по ИБ в соответствии с требованиями ЦБ. У Газпромбанка, понятно, иные потребности. Нам важно обеспечить доступность банковских систем и непрерывность процессов, для чего мы используем самые современные отечественные ИБ-решения (межсетевые экраны, шлюзы доступа, фильтры трафика, балансировщики нагрузки и др.). Также нам важно обеспечить конфиденциальность при работе с чувствительной информацией, особенно при передаче через интернет. Поэтому мы активно применяем технологии VPN на базе сертифицированных

ФСБ решений, связанных с криптографической защитой каналов связи. Это касается как подключения дополнительных офисов, так и подключения через интернет устройств самобслуживания клиентов.

В целях противодействия мошенничеству мы используем разные виды решений класса антифрод, дополняющие друг друга.

В общем, универсального набора ИБ-решений, который гарантировал бы высокий уровень защищённости любому банку, не существует. Потому что информационная безопасность — это не состояние, а процесс. В нём всегда присутствует вероятностный фактор, определяемый спецификой бизнеса. Именно он в итоге влияет и на ИТ, и на ИБ-архитектуру.

ОБ УГРОЗАХ И РЕШЕНИЯХ

— Назовите самые актуальные угрозы на данный момент. Какие решения являются эффективными против них?

— Актуальные угрозы — это кибератаки, мошенничество и несвоевременное реагирование на инциденты. Назову три необходимых класса решений, которые позволяют их минимизировать.

Первый — это решения класса анти-DDOS, которые можно реализовать как собственными силами на базе сложной инфраструктуры межсетевого экранирования и фильтрации трафика, так и на стороне телекоммуникационного провайдера. Чаще всего защита от DDOS закупается как внешний сервис, а для небольших банков — это единственный возможный вариант.

Второй — это решения класса антифрод. Традиционный «внешний» или транзакционный антифрод в представлении не нуждается — он постоянно доказывает свою эффективность. Но в связи с текущей ситуацией в России стала повышаться значимость и «внутреннего антифрода». И он действительно быстро себя оправдывает, позволяя своевременно реагировать на внутренние нарушения. Чаще всего это касается манипуляций с персональными данными.

Третий — это класс SIEM — системы, предназначенные для своевременного выявления и обработки инцидентов в инфраструктуре, на периметре безопасности объекта, в прикладных системах. На мой взгляд, крайне важна аналитическая составляющая этих решений, позволяющая вовремя собирать возникающие инциденты, реагировать на них и предотвращать их как внутри, так и снаружи, а также отсеивать ошибки, неподтверждённые подозрения, тем самым минимизируя входящий поток и снижая нагрузку с дежурных служб.

О ПРОЕКТАХ И ТРЕНДАХ

— Какие проекты в сфере безопасности вы внедрили в этом году и планируете к внедрению в ближайшие месяцы?

— Мы регулярно планируем развитие и внедрение новых инструментов защиты. После выхода указов Президента РФ по импортозамещению мы закономерно скорректировали свои планы и теперь рассматриваем только отечественные инструменты. Речь не только о ПО, но и об аппаратной компоненте инфраструктуры, сервисах и даже партнёрских программах.

Например, ОС Windows, которую мы рано или поздно будем замещать. Вопрос — чем? В этом смысле решение не за безопасностью и даже не за ИТ, а за бизнесом. После того как коллеги примут своё взвешенное решение, а представители ИТ оценят ситуацию со своей стороны, только после этого мы сможем предложить адекватные средства защиты. Но мы уже об этом задумываемся.

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

— На мой взгляд, в ИБ заметно сузился горизонт планирования. Раньше мы работали над многоэтапными проектами на 2–3 года и были уверены, что нас поддержат и софтовые вендоры, и инфраструктурщики, и интеграторы. Сейчас такие сроки и масштабы немыслимы, хотя мы и стараемся придерживаться такого подхода. Но возникли многочисленные риски, среди которых отказ от поставок оборудования в Россию, непонятные сроки по возобновлению поставок, невозможность обеспечить интеграцию в силу отсутствия штата разработчиков и т.д. Раньше проектное, ситуативное управление считалось гипотетическим, но сегодня это реальность. Иметь налаженную сеть поставщиков, проверенных исполнителей, надёжных партнёров и гибких контрагентов — сегодня это огромное конкурентное преимущество, в том числе и в ИБ.

О КАДРАХ

— Есть ли в Газпромбанке проблема с ИБ-кадрами?

— Мы в этом смысле мало отличаемся от других. Текучка есть, особенно в региональной сети. У нас она связана с тем, что люди перерастают свои позиции и уходят в другие организации на руководящие должности, ведь Газпромбанк — отличная школа. В основном это молодые люди до 35 лет.

Мы осознанно воспитали команду универсальных ИБ-профессионалов. Такой, по моим данным, нет ни в одном региональном банке в РФ.

Наши эксперты умеют работать самостоятельно, непрерывно развиваются. К сожалению, наша территориально распределённая структура не всегда позволяет быстро среагировать на их потребности в самореализации.

— Вы много лет преподавали ИБ в МИФИ. Дайте совет молодым людям, которые хотят связать свою жизнь с ИБ. Какие вузы вы считаете лучшими?

— Я окончил МИФИ в 2006 году. Там одним из первых создали факультет информационной безопасности, который ежегодно выпускал порядка 50 специалистов. У меня интерес к ИБ проявился ещё в школе, и я с радостью поступил на этот факультет. К сожалению, какое-то время назад его расформировали как непрофильный, а специальность ИБ в МИФИ совместили с кибернетикой. Поменялась программа, ушли многие преподаватели...

Параллельно с этим другие вузы — в Томске, Санкт-Петербурге, Новосибирске, Бауманский университет в Москве — стали активно расширять направление ИБ, открывать кафедры, факультеты. Выпускники этих вузов сейчас весьма востребованы, мы, например, видим в них потенциальных кандидатов на замещение вакансий.

— Берёте ли вы на работу в Газпромбанк джуниоров?

— Да, мы берём стажёров по направлению ИБ. Если кто-то из выпускников (*профильных вузов — ред.*) хочет попробовать себя в ИБ в нашей банке, он может связаться с департаментом по работе с персоналом. Мы определим, что можно ему предложить. В процессе работы, решая поставленные перед ним задачи, он познакомится с командой, внутренними системами... По завершении стажировки мы можем рассмотреть его кандидатуру на замещение вакансии, если такая, конечно, на тот момент будет.

Но хочу подчеркнуть, что в Газпромбанке есть «входной профессиональный фильтр», и просто так, без его учёта, к нам не попасть.

БАЗИС И НАДСТРОЙКА

— В какой степени специалисту по ИБ нужны знания в области ИТ?

— Я считаю, что ИБ — это надстройка над ИТ. Эти сферы неразрывны. Безопасник обязан знать, что и от чего он защищает, как технологически устроены процессы в банке, какие инфраструктурные и прикладные системы их обеспечивают. Мы внимательно следим, чтобы наши сотрудники, помимо глубоких знаний ИБ, понимали ИТ-процессы и умели «видеть» проблему глазами ИТ-администратора.

РУКОВОДИТЕЛЬ И СПЕЦИАЛИСТ

— Как у вас получается совмещать функции руководителя и специалиста?

— Сейчас фокус задач у меня смещается: с сопровождения и линейной эксплуатации в сторону аналитики, расследований, больших данных. Есть сферы, в которых мне комфортно, и я стараюсь в них развиваться — это киберразведка, противодействие кибермошенничеству, большие данные. В смежных сферах я также стараюсь получать максимум информации, но не настолько глубоко, как профильные специалисты. Нюансы и детали стараюсь делегировать, обсуждать с экспертами. На глубокое изучение новых продуктов у меня просто не хватает времени. Но совместная проработка и обсуждение технических решений, архитектуры, сценариев возможных атак, инструкций по реагированию — всё это происходит с моим участием, и в этом смысле я активно применяю навыки линейного ИБ-специалиста, которые приобрёл за много лет работы.

В профессии мне интересно. Многие специалисты ИБ уходят в частный бизнес или организуют свои ИТ-компании. Но я для себя такой сценарий пока не рассматриваю.

О ДОСУГЕ

— Вы обозначили такой большой круг задач, которые вам приходится решать, что поневоле возникает мысль об отсутствии у вас свободного времени. И всё-таки, как вы проводите досуг?

— Действительно, времени мало, поэтому всё свободное от работы я стараюсь проводить с семьёй. У меня две дочери — пяти и семи лет. Мы с супругой играем с ними, ходим в театры, на выставки, в общем, всё, что может быть интересно и полезно детям в этом возрасте.

Дочери любят парк «Зарядье», ГУМ, но не из-за покупок, а из-за его ни с чем не сравнимой атмосферы и, конечно, мороженого. А мне нравятся книжные ярмарки. Этим летом их в Москве было несколько — в Измайлово, на Красной площади, в том же ГУМе. Там я совмещаю приятное с полезным.

Если погода позволяет, выбираемся куда-нибудь недалеко от Москвы. Летом я брал отпуск, и мы много ездили по соседним областям — посещали исторические места, музеи, ярмарки народного промысла, мастер-классы, направленные на развитие детей.

По-моему, проводить время с семьёй намного приятнее любого самого увлекательного хобби.

Беседовала
Оксана Дяченко

НЕЛЬЗЯ ПО-СТАРОМУ! А КАК ПО-ДРУГОМУ?

О ЦЕНТРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРУГРОЗАМ



Александр ВЕЛИГУРА
председатель комитета по банковской безопасности АРБ, руководитель комитета по безопасности НП НПС, к.ф.-м.н.

Важность противодействия киберугрозам, никогда не подвергавшаяся сомнениям, в последнее время возрастает просто лавинообразно. Нормативно-правовое и нормативно-методическое обеспечение этого процесса не отстаёт — успевай поворачиваться. Но есть проблема: не у всех есть возможности реализовать поступающие требования и рекомендации в сжатые сроки (да хотя бы и не в сжатые — сказали бы мы ещё недавно).

Чаще всего в профессиональном сообществе обсуждается скорость и проработанность принимаемых требований в ответ на вызовы, а также практическая возможность их реализовать, особенно силами небольших организаций. Темы таких обсуждений не меняются годами. Но сейчас, когда налицо коренные изменения

окружающей и внутренней обстановки, возникает вопрос: можно ли действовать по-старому? Действуя по прежней схеме, прилагая всё большие и большие усилия, чтобы успеть принять всё новые и новые соответствующие меры, мы, похоже, приблизились к пределу того, чего можно в принципе добиться таким путём.

А как по-другому? Методологически очень просто: передать часть функций снизу на уровень всей отрасли — финансового рынка. В качестве первого этапа — на уровень банковской сферы.

Как это будет выглядеть? Схема следующая, и она, в общем-то, уже предлагалась. Центральный Банк, наделённый ресурсами государства, строит территориально распределённый с иерархической структурой Центр противодействия киберугрозам (ЦПК). На него замыкается весь интернет-трафик, вся почта, все внешние каналы



Артём КАЛАШНИКОВ
Газпромбанк

BIS-КОММЕНТАРИЙ

15 000 ФИНАНСОВЫХ ОРГАНИЗАЦИЙ ОСТАЮТСЯ БЕЗ ЗАЩИТЫ!

Года три уже обсуждается тема централизации на единой гарантированной платформе услуг для финансового сектора. Эта идея навеяна тревогой и даже паникой небольших финансовых организаций, которые в быстро меняющихся реалиях не могут оперативно обеспечить ни гибкость в решениях, ни соответствие требованиям регулятора по причине отсутствия необходимых ресурсов — как финансовых, так и кадровых. Хорошие специалисты и менеджмент стоят дорого.

То же самое и в сфере обеспечения информационной безопасности: в условиях кибервойны, кратного увеличения числа кибератак и использования новых инструментов для осуществления этих атак, а также усиления требований регуляторов небольшие организации не в состоянии имеющимися ресурсами обеспечить выполнение требований

по обеспечению безопасности. Ввиду этого и встал вопрос централизации сервисов ИБ на одной платформе для оказания услуг организациям, нуждающимся в такой помощи. Ответом на этот вопрос родилась идея создания Центра противодействия киберугрозам (ЦПК). Пусть пока реализация имеет локальный характер (такая деятельность возникла стихийно и направлена, как правило, на защиту дочерних обществ крупных компаний и холдингов), но лиха беда начало.

Давайте посмотрим, как можно масштабировать такой проект. Что для этого нужно? Возьмём близкий нам финансовый сектор как самый зарегулированный в части обеспечения ИБ. На мой взгляд, в первую очередь стоит обратить внимание на следующие моменты.

Такой Центр, ЦПК (по сути, это Managed Security Service Provider — MSSP), должен быть независимым, обладающим

связи и предоставления услуг клиентам тех коммерческих банков, которые не обладают ресурсами для самостоятельного решения задач обеспечения безопасности. В идеале — всех банков, а потом и других финансовых организаций, но будем реалистами, не будем спешить, так как в проектах такого масштаба необходима этапность.

Этот ЦПК своими силами оказывает весь необходимый спектр сервисов по информационной безопасности. Помимо всего прочего, для эффективного реагирования на многие атаки сегодняшнего дня требуются люди с довольно редкими специальностями: реверсеры, вирусные аналитики, компьютерные криминалисты и т.п. Ни одна организация не может позволить себе держать в штате таких специалистов, если они востребованы считаное число раз в год.

ЦПК организует предупреждение проблемных ситуаций, включая инциденты, а также проводит выявление и анализ уязвимостей обслуживаемых информационных систем, координацию действий по устранению уязвимостей, анализ событий, регистрируемых компонентами обслуживаемых систем и средств их защиты, для поиска признаков атак, направленных на эти системы. Можно возразить, что тут есть

пересечение с функциями ГосСОПКА, но здесь шире: ЦПК очищает почту от спама и вирусов, защищает от ДДОС-атак, выявляет аномальный внешний и внутренний трафик, осуществляет межсетевое экранирование, обеспечивает безопасность проектной деятельности организаций, информирует их руководство о событиях с признаками инцидентов для дальнейшего совместного расследования, при необходимости организует проведение киберучений и т.д.

Мелкие кредитно-финансовые организации не имеют ни средств, ни компетенций для построения полноценной системы киберзащиты. ЦБ может их ругать, высылать новые требования и стандарты, проводить проверки и учения, даже наказывать, только защищённость от этого не улучшится. Там нет ни штата, ни финансов в необходимых количествах.

Опыт создания таких ЦПК сейчас, по имеющимся сведениям, набирается в некоторых крупных банках (по отношению к дочерним организациям и филиалам). Не поднать ли это знамя на более высокий уровень?

необходимыми лицензиями на осуществление своей деятельности. То есть «равноудалённым» для всех участников рынка финансовой сферы. В такой конфигурации ЦПК может стать независимым гарантом обеспечения безопасности. Вместе с тем для обеспечения гарантий безопасности и доверия со стороны участников рынка ЦПК должен стать структурой, поднадзорной Банку России, но не его дочерним обществом. Возможно, придётся пересматривать закон о ЦБ и Устав ЦБ.

С учётом реалий функционировать такой Центр должен на отечественных решениях. Есть ли такие решения для столь огромных масштабов, ещё предстоит выяснить. Безусловно, отечественные решения и сервисы для обеспечения безопасности есть, но вот смогут ли они функционировать в таких масштабах и при таких нагрузках? Два года назад количество организаций, поднадзорных ЦБ, составляло около 20 тыс. С учётом «оздоровления» финансового рынка и самостоятельного ухода ряда компаний осталось примерно 16 тыс. Из них вычитаем 1–2 тыс. крупных компаний, которые могут обеспечить свою ИБ сами. Остальные остаются «сиротами» в этом плане. Вот для них и нужен такой Центр.

Нельзя обойти тут и проблему кадрового голода. Тот факт, что в сфере ИБ не хватает квалифицированных специалистов, давно не секрет, об этом постоянно говорят на каждом мероприятии и пишут в каждом СМИ. На подготовку специалистов и экспертов ИБ нужно время. Централизация имеющегося кадрового состава в сфере ИБ могла бы решить часть проблем потребителей сервисов Центра. Другой вопрос, что кадры будут несколько «уязвимым местом». Нужны

будут инструменты контроля. Благо из предыдущего опыта ИБ есть кейсы для решения этого вопроса.

С учётом того, что Центр будет предоставлять сервисы огромному числу организаций, очевиден риск «единой точки отказа». Поэтому целесообразно разрабатывать Центр на геораспределённой архитектуре. Например, в каждом федеральном округе. Для обеспечения катастрофоустойчивого и безотказного функционирования архитектура должна строиться по схеме связи «каждый с каждым» с резервированием данных и информационной структуры. А возможно, и на основе технологии «блокчейн». Но это дискуссионный вопрос, так как успешно действующих технологий безопасности, построенных по технологии «блокчейн», в России я пока не встречал.

Принимая во внимание предполагаемый масштаб Центра и его геораспределённость, потребуются большие вложения в создание инфраструктуры, каналы связи. Финансирование может идти как из госбюджета, так и от игроков рынка, которые могут позволить себе «длинные деньги». Возможно, для возврата инвестиций имеет смысл рассмотреть предоставление Центром услуг на возмездной основе. При этом тарифная политика таких сервисов должна предлагать цены существенно ниже, чем затраты потребителей при децентрализованном обеспечении безопасности.

Кроме всего, вероятно, придётся пересматривать законы о защите информации, о защите платёжных систем и персональных данных. Но это вопрос для отдельного большого обсуждения.



Андрей КУРИЛО
советник
по вопросам
ИБ ФБК и FBK
CyberSecurity, к. т. н.

О ЦЕНТРАЛИЗАЦИИ СЕРВИСОВ БЕЗОПАСНОСТИ

МОЖЕТ, СТОИТ НЕ ИЗОБРЕТАТЬ ВЕЛОСИПЕД,
А ПРОСТО ДОСТАТЬ ЕГО ИЗ КУСТОВ?

Идея создания центра противодействия киберугрозам в кредитно-финансовой сфере хорошая, интересная, современная и наверняка найдёт своих сторонников. Тем более что уже много лет обсуждается вопрос централизации в некоем общем сервисе платёжных систем небольших банков с выводом в эти централизованные сервисы некоторых функций безопасности. Правда, этот вопрос дальше вялотекущих общих рассуждений никуда не продвинулся.

Тут же предлагается решить задачу не менее, а может быть, и более сложную.

Представляется, что при проработке вопроса создания такого центра (ЦПК) следует рассматривать три обстоятельства:

- 1) Правовой статус центра.
- 2) Перечень функциональных задач, которые можно передать в этот центр.
- 3) Ответственность центра в случае реализации инцидентов у обслуживаемых организаций.

Что касается правового статуса, то очевидно, что он должен находиться в позиции равноудалённости как от регулятора, так и от обслуживаемых организаций. Но это не мешает тому же регулятору войти в него своим капиталом (по схеме НСПК), что обеспечит возможность эффективного контроля его деятельности.

Но этот вопрос, по моему мнению, не самый главный. Важнее два других.

Первое. Какую функциональность в сфере информационной безопасности можно передать в этот центр и как можно обеспечить её выполнение?

Очевидно, что при анализе следует руководствоваться имеющейся нормативной базой по ИБ в кредитно-финансовой сфере, а это значит, два ГОСТа (57580.1 и 2) и несколько нормативных актов Банка России, включая Положение 716-П.

Также следует отметить, что нет никаких оснований рассчитывать на то, что требования по информационной безопасности, изложенные в нормативных документах регуляторов, будут каким-то образом упрощены и смягчены. Скорее наоборот, о чём говорит активность вокруг проблематики персональных данных и указа Президента № 250 от 1 мая 2022 года. Также должен отметить, что системно требования по ИБ, изложенные в отечественных нормативных документах, практически полностью соответствуют современным международным взглядам, зафиксированным в стандартах ISO 27-й и 19-й серий и вряд ли будут допущены отклонения от этих документов, принятых в том числе и в России в качестве государственных стандартов.

Отмечу также, что наиболее высокую эффективность в отражении атак показали мероприятия по оперативному контролю инцидентов и уязвимостей, то есть как раз те, которые в наименьшей степени оказались охвачены нормативным регулированием.

Тем не менее все требования по обеспечению информационной безопасности можно разделить на две большие группы.

Первая — требования, реализуемые нормативно-правовым способом, организационно, то есть требующие участия в этой деятельности самих, часто нескольких сразу, функциональных подразделений организации (распоряжения, приказы, инструкции, методики, отчётность, контрольные мероприятия, аналитическая

Наиболее высокую эффективность в отражении атак показали мероприятия по оперативному контролю инцидентов и уязвимостей, то есть как раз те, которые в наименьшей степени оказались охвачены нормативным регулированием

деятельность, администрирование средств защиты, управление РКИ-сервисами, экспертиза решений, обеспечение мероприятий безопасности на всех этапах жизненного цикла и т.д.). Этими способами решается добрая половина задач в области обеспечения безопасности по тому же ГОСТ Р 57580.1. —2017, и маловероятно, что какая-либо организация допустит вмешательство аутсорсера в свою административную и оперативную деятельность. Из этого следует, что все эти задачи должны остаться в поле деятельности, а главное — ответственности этой организации.

Вторая группа — техническое управление системой обеспечения информационной безопасности (СОИБ) СЗИ, а также средствами анализа событий, выявления и классификации вторжений и обработки инцидентов.

Отдельная подзадача — правильная регистрация технической информации по регистрируемым событиям, проведение расследований, форензика, взаимодействие с правоохранительными органами.

Технически такие решения возможны и при высокой степени централизации сервисов, и, возможно, они даже будут эффективны.

Но можно ли в полном объёме передать в аутсорсинг, а это он и есть, всю названную функциональность, отказавшись от собственных сотрудников? Практика говорит, что нет. Любые задачи в области информационной безопасности, переданные на аутсорсинг, требуют адекватной поддержки внутри организации. Тогда есть ли новизна в этом предложении?

И наконец, об ответственности.

Какую ответственность будет нести аутсорсер информационной безопасности в случае реализации инцидента, приведшего к ущербу на подконтрольном объекте? Вопрос неясен, но возможно, что это событие можно застраховать. А будет ли после этого снята с подконтрольного объекта ответственность за возникший у него инцидент? Чья вина в возникновении инцидента? В ГосСОПКУ что сообщать? Технически вопросов нет, понятно, а организационно? Кто будет виноват и как это записывать в отчётность и представлять публично? Означает ли заключение договора на аутсорсинг и договора SLA перенос ответственности на аутсорсера? Тут нет ответа. И вряд ли он будет положительным, если только аутсорсер вдруг не захочет сам себя запатовать возникающими у подконтрольных организаций инцидентами.

Тогда такой вопрос: а что сейчас нас не устраивает в сложившейся конфигурации? Ведь практически все возможные сервисы предлагаются и сейчас. Аутсорсинг есть по любому направлению, только выстраивается он индивидуально в каждом конкретном случае. Кстати, на основе прекрасного документа ЦБ СТО БР ИББС 1.4–2018 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление рисками нарушения информационной безопасности при аутсорсинге». Может быть, в этом направлении пойти, придав обязательный статус этому документу?

BIS-КОММЕНТАРИЙ

КАЖДЫЙ ДОЛЖЕН ЗАНИМАТЬСЯ СВОИМ ДЕЛОМ

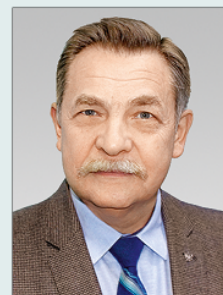
Поддерживаю саму идею создания такого централизованного органа (ЦПК), но предвижу ряд законодательных проблем при той реализации, о которой говорит Артём Калашников.

Если попробовать подойти к проблеме с учётом сегодняшних реалий, то вижу решение в углублении и повышении оперативности во взаимодействии МВД, Банка России, самих банков,

операторов связи и платёжных систем. Каждый должен заниматься своим делом.

Тем более что сейчас в МВД есть соответствующие подразделения, а в них часто очень адекватные сотрудники.

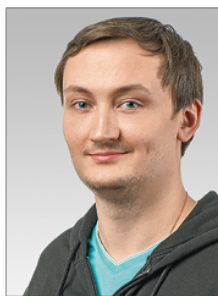
Опыт выявления признаков мошеннических операций в банках огромный. Не надо изобретать велосипед, надо как следует научить ездить на том, что есть.



**Василий
ОКУЛЕСКИЙ**
эксперт
информационной
безопасности, к. т. н.



Полина ПЕРЛОВА
менеджер по продуктовому
маркетингу R-Vision



Валерий ГОРБАЧЁВ
руководитель направления
внедрения СЗИ АО «ДиалогНаука»

ЭФФЕКТИВНОЕ УПРАВЛЕНИЕ ДАННЫМИ THREAT INTELLIGENCE

ОПЫТ ВЫБОРА ПЛАТФОРМЫ ДЛЯ АНАЛИЗА УГРОЗ

Информационная безопасность уже давно сводится не только к выстраиванию процесса реагирования на уже произошедшие инциденты: современный подход к ИБ включает в себя как реактивные, так и проактивные меры, а умение предугадать и распознать атаку по самым ранним признакам становится одним из ключевых факторов защиты бизнеса от киберугроз. Одним из инструментов, позволяющим снизить вероятность возникновения инцидентов, а также получить дополнительный контекст для их расследования, является использование данных Threat Intelligence (TI).

ЧТО ТАКОЕ THREAT INTELLIGENCE И ДЛЯ ЧЕГО НУЖНА КИБЕРРАЗВЕДКА?

Между понятиями TI и киберразведки часто ставят знак равенства, однако следует разделять эти термины на совокупность данных и собственно процесс их получения и использования. Если кратко, TI — это любые знания, позволяющие сделать выводы об актуальных угрозах в отношении конкретной организации или целой отрасли, спланировать защитные меры, а также повысить эффективность обнаружения и реагирования на них. Наряду с этим процесс получения данных TI напоминает классическую разведку: ИБ-специалисты

собирают информацию, обрабатывают её, ищут недостающий контекст, преобразовывают всё в единый вид и передают лицу, принимающему решения, для оценки рисков и принятия защитных мер. При этом качество данных TI напрямую влияет на скорость и эффективность решений.

Проактивный подход к защите особенно актуален для банковской сферы, где утечки конфиденциальных данных и денежных средств не только могут ударить по репутации организации, но и напрямую влияют на деятельность остальных участников финансового рынка. Одним из инициаторов такого подхода выступил ЦБ РФ, сформировавший в своей структуре специальный Центр мониторинга и реагирования на компьютерные атаки — ФинЦЕРТ. Система АСОИ ФинЦЕРТ¹, созданная на базе подразделения, аккумулирует всю информацию об угрозах в кредитно-финансовой сфере и позволяет обмениваться ею между всеми участниками системы: банками, правоохранительными органами, провайдерами связи, ИБ-организациями, а также получать рекомендации ФинЦЕРТ по реагированию на угрозы. Создаётся своеобразный эффект «коллективного иммунитета».

¹ Автоматизированная система обработки инцидентов ФинЦЕРТ.

ПРОБЛЕМА ОБРАБОТКИ ДАННЫХ TI

Чаще всего организация процесса киберразведки начинается с использования открытых источников, содержащих индикаторы компрометации: хеши вредоносных файлов, домены, IP-адреса и прочие артефакты, связанные с деятельностью киберпреступников. Основные проблемы на данном этапе происходят при попытке добыть максимум «разведанных» путём подписки на всевозможные доступные источники. Получается палка о двух концах: чрезмерный поток разрозненных данных неизбежно приводит к невозможности их обработать.

При этом важно понимать, как полученные индикаторы связаны с конкретными группировками, например ведущими свою деятельность в отношении банковской отрасли или действующими против конкретной страны. Таким образом, для принятия эффективных контрмер против киберпреступников необходимо не только использовать уже имеющиеся в наличии данные, но и быстро находить недостающий и актуальный контекст.

ЗАДАЧИ, КОТОРЫЕ РЕШАЮТ TI-ПЛАТФОРМЫ

По мере расширения инфраструктуры организации назревает потребность

в автоматизации работы со сведениями об угрозах. На помощь приходят специализированные платформы киберразведки, которые агрегируют всю доступную информацию в единой базе, автоматизируют ключевые процессы, связанные с обработкой данных TI и, наконец, позволяют экономить временные и человеческие ресурсы. В качестве проактивной защиты платформы позволяют автоматически экспортировать индикаторы компрометации на СЗИ.

Помимо этого, TI-платформы используются в различных рабочих сценариях, самый распространённый из которых — реактивное реагирование на угрозы путём поиска индикаторов компрометации в инфраструктуре, а именно в событиях SIEM-систем. Также платформа киберразведки может участвовать в процессе реагирования на инциденты как своеобразная база знаний, предоставляя полный контекст по индикаторам, содержащимся в инцидентах.

Использование подобных платформ упрощает работу с данными TI в целом, позволяет быстро выявить скрытые угрозы в инфраструктуре, минимизирует ущерб благодаря своевременной блокировке угроз, а также ускоряет все ИБ-процессы организации.

ВЫБОР ПЛАТФОРМЫ АНАЛИЗА УГРОЗ

Компания «ДиалогНаука» долгое время поставляла заказчикам решения как российских, так и зарубежных вендоров. Когда компания Anomali, один из ведущих поставщиков платформ Threat Intelligence, ушла с российского рынка, было необходимо найти среди отечественных систем аналог, не уступающий в качестве западному продукту, который уже не один год был в портфеле решений компании.

При выборе подходящей системы компания концентрировалась на нескольких аспектах — архитектуре, модульности и интеграционных возможностях платформы. В ходе реализуемых проектов «ДиалогНаука» работает с разными типами инфраструктур заказчиков: территориально распределённые, гибридные, инфраструктуры с высокой нагрузкой и другие. Таким образом, одним из основных требований были

В R-Vision TIP реализована встроенная интеграция с ключевыми источниками данных TI, при этом поддерживается более 20 сервисов обогащения

масштабируемость решения и возможность архитектурно поддерживать инфраструктуру любого типа.

Заказчики «ДиалогНауки» неоднократно отмечали важность гибкости платформы, а именно возможность подключения различных поставщиков фидов. Кроме того, учитывая существующие сценарии применения систем киберразведки, одним из ключевых параметров при выборе была открытость платформы. Крайне важно встроить работу TI-платформы в текущие процессы информационной безопасности конкретной организации, такие как реагирование на инциденты, обнаружение событий ИБ, распространение информации об индикаторах компрометации на средства защиты информации и сетевые устройства организации.

Прежде чем предлагать заказчику решение какого-либо вендора, компания всегда проводит его предварительную проверку в своей тестовой лаборатории. R-Vision, в свою очередь, придерживается схожего подхода: сначала продукты проходят процесс тестирования в рамках инфраструктуры вендора, затем пилотирование в инфраструктурах заказчиков, а финальный процесс внедрения всегда индивидуален и проходит под контролем команды экспертов.

ПЛАТФОРМА R-VISION TIP

При проведении тестирования R-Vision Threat Intelligence Platform (TIP) «ДиалогНаука» отметила изобилие как коммерческих, так и открытых фидов, с которыми поддерживается работа. В их число входит АСОИ ФинЦЕРТ, а также R-Vision Threat Feed, который входит в состав платформы.

Помимо встроенных интеграций, возможно подключение других источников, при этом платформа поддерживает более 20 сервисов обогащения. За счёт ретроспективного и проактивного поиска релевантных индикаторов в потоке событий данное решение снимает

нагрузку с SIEM-систем и сокращает ресурсы на её настройку. Также R-Vision TIP поддерживает автоматическую выгрузку индикаторов для немедленной блокировки на такие средства защиты, как антивирусы, межсетевые экраны и решения класса EDR.

Поскольку ручной процесс обработки данных может занимать существенное время, для решения этой задачи в TI-платформах используются инструменты оценки качества источников и индикаторов, что позволяет аналитикам концентрироваться только на важных и актуальных вопросах. Эта функциональность также реализована в системе R-Vision TIP.

На более продвинутом уровне киберразведки R-Vision TIP позволяет формировать собственную базу данных: например, создавать уникальные IoCs и отчёты об угрозах, связывая при этом сущности друг с другом. Для получения целостной картины происхождения и проведения подробного анализа взаимосвязи между объектами можно отобразить в виде схемы. Кроме того, платформа позволяет осуществлять обмен данными между различными подразделениями организации путём создания бюллетеней о существующих в инфраструктуре угрозах и уязвимостях.

Тренд на импортозамещение коснулся и платформ Threat Intelligence — компании активно интересуются отечественными аналогами западных систем, при этом становясь всё требовательней в вопросе качества получаемых данных. По итогам сравнения различных TI-платформ система R-Vision TIP показала полное соответствие всем необходимым требованиям и уже получила положительные отзывы со стороны заказчиков в ходе ряда пилотов и полноценных внедрений.

**Иван ЧУРИЛОВ**аналитик данных
ООО «ЛАНИТ-ТЕХНОЛОГИИ», ЦК ДАТА**Иван МЕЛЕХИН**директор центра мониторинга и противодействия
кибератакам IZ: SOC, компания «Информзащита»

SOC + ML

КАК МАШИННОЕ ОБУЧЕНИЕ ПОМОГАЕТ АНАЛИТИКАМ SOC

Сегодня Центры мониторинга киберугроз или Security Operation Center (SOC) стали еще более востребованными. Помимо угроз со стороны злоумышленников необходимо также отслеживать техническое состояние контролируемых устройств, выявлять и исправлять неполадки, обнаруживать сбои и своевременно на них реагировать. Информационные системы, за которыми осуществляется контроль, обладают сегодня большим масштабом (десятки или сотни тысяч устройств). Сама структура этих систем, а также количество устройств динамически изменяются и работают они часто «в нескольких средах» (облака и ЦОД).

На практике это означает, что данные поступают из множества точек, и отслеживание всех возможных векторов атак, а также выявление важных событий, связанных с безопасностью, — комплексная задача, решать которую становится сложнее с каждым днем. Очевидно, что такое количество источников данных невозможно обрабатывать вручную. Каждую секунду центр мониторинга получает десятки тысяч событий — все эти горы данных необходимо сортировать и анализировать на предмет аномалий — представьте, сколько времени и ресурсов это может занять.

АВТОМАТИЧЕСКИЙ КОНТРОЛЬ

С другой стороны, за последние годы машинное обучение неоднократно применялось в индустрии кибербезопасности для решения различных задач, например, анализа и классификации пользовательской активности либо сетевого трафика, обнаружения компьютерных атак. Мы стараемся применять накопленный опыт и для анализа логов SOC, но в настоящей статье хотим поделиться базовой мерой контроля, целью которой является мониторинг потока файлов логов с каждого устройства исключительно по их количеству.

В случае сбоя, технической неполадки либо инцидента информационной безопасности, количество логов, поступающих с устройства, изменяется. А из-за большого количества устройств адекватной возможности контроля каждого устройства ресурсами аналитиков нет, выявить источник, который нарушает паттерн отправки событий вручную, невозможно, и, к сожалению, бывают случаи, когда отсутствие событий от источников обнаруживается не сразу. Таким образом, автоматический контроль наличия потока необходимого количества логов для своевременного обнаружения и предотвращения инцидентов является эффективной мерой, способной снизить финансовые, репутационные и иные риски.

МОНИТОРИНГ КОЛИЧЕСТВА ЛОГОВ

Для решения данной задачи было проведено исследование и разработан программный модуль, предназначенный для мониторинга количества логов, поступающих с контролируемых устройств. Если описывать задачу более формально, то здесь мы имеем дело с набором показателей, регулярно измеряемых через равные промежутки времени: количество логов на конкретном устройстве в единицу времени, например, 1 час. Такой показатель принято называть временным рядом, а задача в терминах машинного обучения представляет собой обнаружение аномалий во временных рядах (рис. 1).

Возникает закономерный вопрос: почему нельзя просто выставить определённые пороговые значения, выход за рамки которых свидетельствовал бы о критической ситуации и о необходимости создания нового инцидента. Это простое решение, имеющее право на жизнь. Но для его использования необходимо подбирать пороговые значения. Это можно попробовать сделать, ориентируясь на средние значения или другие характеристики ряда, но в действительности со временем поведение рядов часто может меняться. Более того, в определенное время суток, в разные дни недели или еще по какой-то

закономерности пороговое значение может отличаться. Так, для персонального компьютера отсутствие активности ночью может быть нормальным событием, в то время как в рабочий день вероятность такого мала. И, конечно же, всё это осложняется количеством устройств и большим объёмом информации, с которым приходится работать. И тут на помощь приходят технологии машинного обучения.

С УЧИТЕЛЕМ И БЕЗ

Для решения задачи средствами машинного обучения нам необходимо вначале обучить модель. Обучение может быть двух видов: с учителем и без. Разница в том, что при обучении с учителем у нас уже есть разметка (то есть множество ответов на тренировочных данных, которые учится прогнозировать модель), а при обучении без учителя разметки нет. Наш случай как раз второй, поскольку достаточного количества данных, соответствующих схожим инцидентам, которые мы хотели бы отлавливать, у нас нет. Даже при наличии достаточного числа задокументированных событий тем не менее сохраняется бы опасность большего числа незадокументированных инцидентов, которые потенциальная модель училась бы «считать» нормальными. Кроме того, рядов много, их поведение со временем меняется, поэтому делать разметку и периодически её обновлять было бы очень ресурсозатратно.

ТРИ ПОДХОДА

Для обнаружения аномалий во временных рядах с учетом отсутствия разметки тоже используются разные методы машинного обучения, которые, в свою очередь, можно разделить на следующие большие группы:

- ♦ **классические методы обнаружения аномалий** основаны на автоматическом установлении основных статистических закономерностей временного ряда в простом виде, как, например, одно нормальное распределение или смесь, или в более сложном — через аппроксимацию данных деревом решений;

- ♦ **методы на основе реконструкции** основаны на кодировании и последующем декодировании значений

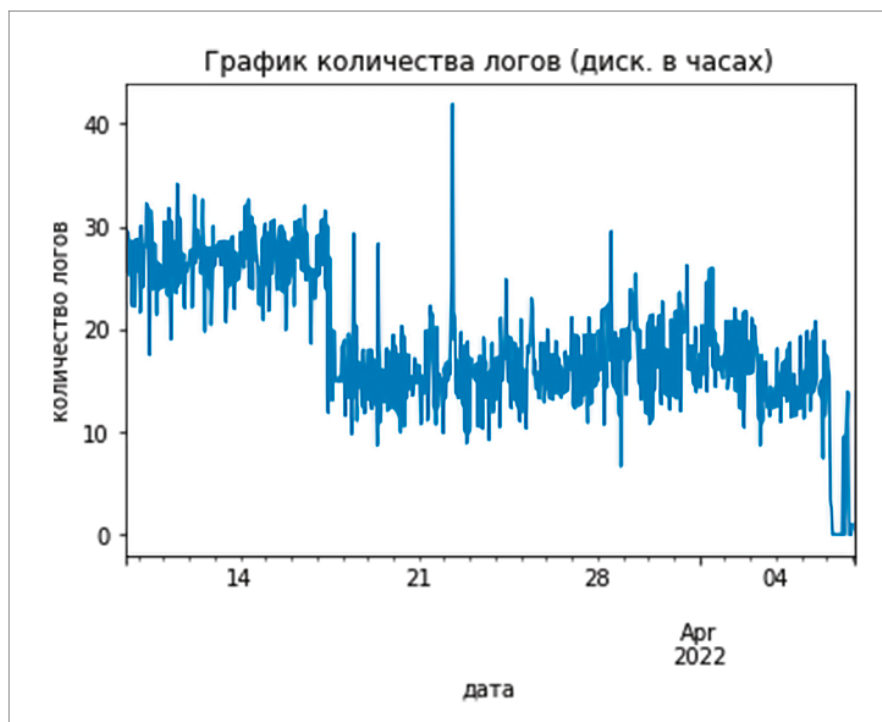


Рисунок 1. Пример временного ряда для конкретного источника

определённым способом, таким, что для нормальных значений ряда после декодирования получаются исходные значения, а для аномальных значения искажаются и таким образом происходит их детектирование;

- ♦ **методы на основе прогнозирования** основаны на создании прогнозной модели ряда и дальнейшем сравнении прогноза и фактической величины. Если прогноз сильно отличается от фактической величины, это говорит о том, что наблюдается аномалия. Данный подход лучше всего применим к временным рядам с выраженными периодами, циклами или сезонностью.

Первый подход хоть и не требует разметки для обучения, но нуждается в ней для тестирования результатов — иначе понять, успешно или нет получается решать задачу, невозможно. Вторым подходом помогает эффективно искать аномалии в многомерных временных рядах, где важна взаимосвязь показателей. Например, в кластере датчиков, в котором отклонение одного значения без знания других показателей не является критичным. Минусом такого подхода является концентрация на локальном промежутке времени, что

ограничивает взаимосвязи, которые можно было бы уловить из данных.

Поэтому мы выбрали подход по прогнозированию временных рядов, как наиболее подходящий в данной ситуации.

ТРИ ШАГА

Общий принцип работы этих методов можно разделить на несколько шагов.

В качестве подготовительного этапа обучается модель машинного обучения, прогнозирующая временной ряд. Следующие этапы происходят уже при работе по обнаружению аномалий.

Строится прогноз (на текущий момент горизонт прогнозирования составляет 1 час вперёд), для прогноза строится доверительный интервал.

Текущее значение временного ряда помечается аномальным, если оно выходит за рамки доверительного интервала.

При выборе такого подхода у нас появляется косвенная мера, позволяющая оценить, хорошо ли у нас получится решить целевую задачу — найти ошибку прогнозирования. И возникает вопрос — как мы могли бы измерить ее для 1000 рядов и понять, что у нас все получается. Самые

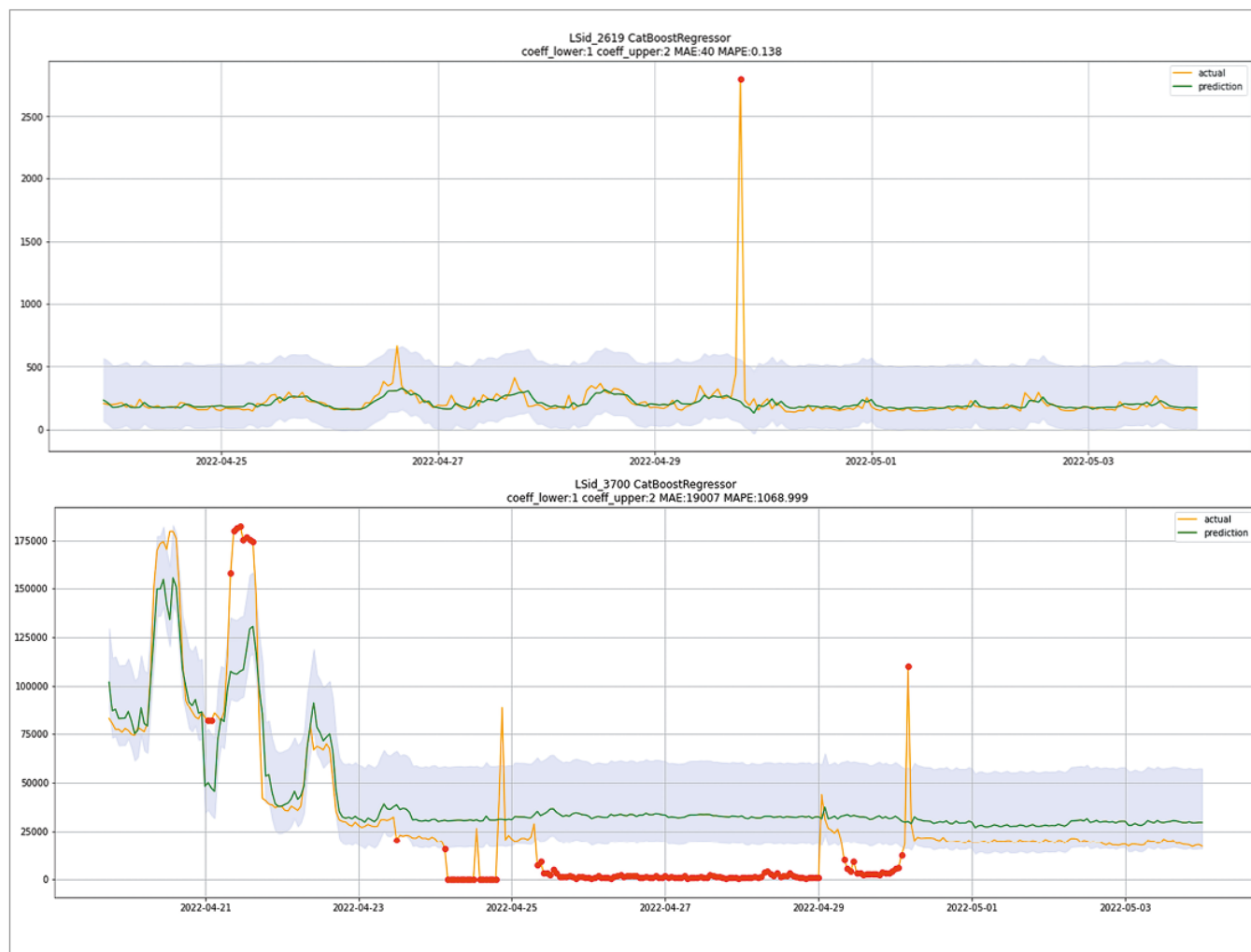


Рисунок 2. Примеры работы модуля. Жёлтым цветом показаны фактические значения ряда, зелёным прогноз, красным выделены аномальные значения

распространенные подходы — измерять модуль или квадрат разности фактического значения и прогнозируемого, чему соответствуют такие меры как MAE (mean absolute error) и MSE (mean squared error).

Тем не менее, для одного временно-го ряда может оказаться, что в момент загрузки он вполне может продуцировать до 1000 событий в час, и отклонение в 10 событий выглядит совершенно несущественным. Но логично, что присутствуют источники, для которых 20 событий это потолок, и, если количество падает в 2 раза, это о чем-то да говорит. Можно было бы нормировать (делить) на фактическое значение, чтобы ошибку считать в относительных единицах — это позволило бы сравнивать ошибки для разных источников и хотя бы посчитать среднее значение

ошибки на всех рядах для того или иного подхода, чтобы выбрать наиболее оптимальный.

Такая мера обозначается как MAPE или mean absolute percentage error. Но и тут кроется проблема: если текущее фактическое значение равно 0, что вполне нормально для персональных компьютеров, выключенных на ночь, то делить мы также будем на 0, а заниматься этим без разрешения взрослых мы не могли. Существует мера, исправляющая этот подход: SMAPE или symmetric mean absolute percentage error, в котором нормировка происходит не только на фактическое значение, а на среднее между фактическим и прогнозируемым значениями в этот момент времени. На эту метрику качества мы и ориентировались в своей работе. Существуют и другие

распространенные подходы оценить качество прогноза — измерение R2. Но специфика этой метрики такова, что по факту она сравнивает ошибку прогнозирования текущей модели с ошибкой прогнозирования единственным значением, иначе константой. Поскольку в данной задаче мы были нацелены на прогнозирование значительно более качественное, чем константное, эта мера нам также не подходила.

ТРЕНД И СЕЗОННОСТЬ

После того как мы определились, как же нам оценивать результаты прогноза, возникает следующая нетривиальная задача: выбор подхода, алгоритма машинного обучения, который бы универсально подходил для всех временных рядов. Какие же ингредиенты требуются для успешного

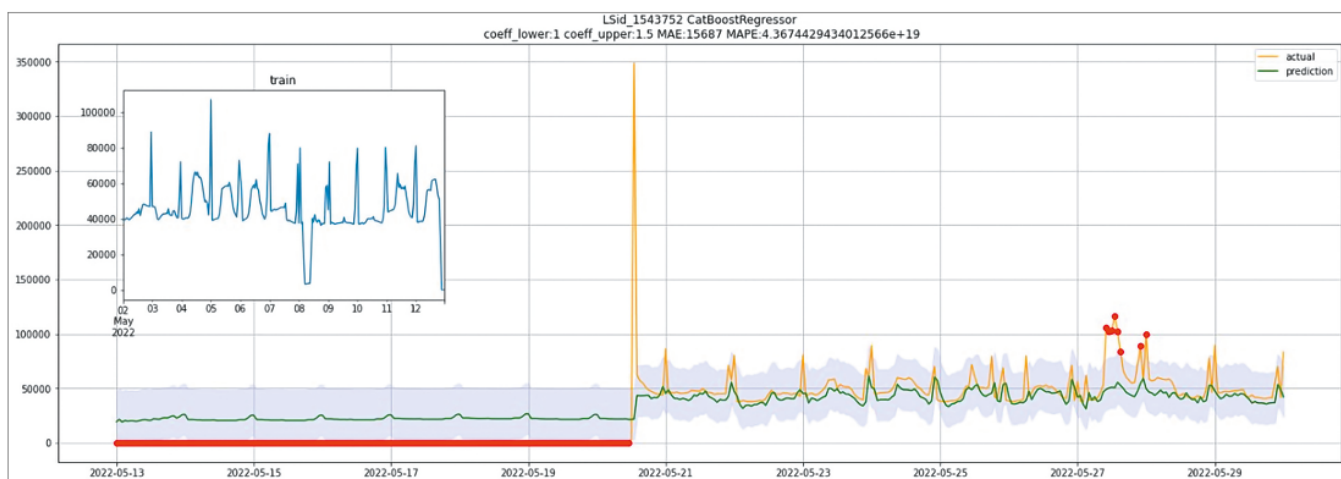


Рисунок 3. Результат работы модуля и временной ряд, на котором обучалась модель

прогнозирования? На самом деле самые базовые подходы, которых может оказаться достаточно для решения некоторых задач, основаны на скользящем среднем и его вариациях. Т.е. в таком случае следующее значение временного ряда, в данном случае число логов, которое мы ожидаем в следующий час, определяем как среднее число логов за последние n часов. Вполне валидный подход, но для наших целей совершенно не подходящий, поскольку при возникновении инцидента, приводящего к прекращению поступления логов, через эти самые n часов для нашей системы это отсутствие логов станет совершенно нормальным. Противоположной альтернативой является представление временного ряда на всем промежутке времени в виде двух составляющих: тренд и сезонность.

Тренд представляет собой постепенное изменение временного ряда. Например, при запуске сервиса нагрузка на него может быть 100 запросов в час, но впоследствии его востребованность растет.

Сезонность же представляет собой периодические закономерные изменения временного ряда. Например, увеличение числа событий днем и затухание ночью. Проблема такого подхода в том, что не все временные ряды настолько закономерны. Кроме того, подход предполагает оценку тренда и сезонности единожды при обучении, никак не опираясь на текущие показатели временного ряда.

КОМПЛЕКСНЫЙ ПОДХОД

Оптимальным же, как всегда, является подход комплексный, включающий как моделирование сезонных составляющих, так и учитывающий текущие наблюдения временного ряда. В качестве алгоритма, реализующего такой подход, возможно выбирать любую модель машинного обучения, подходящую для решения задачи регрессии — т.е. определения непрерывного показателя на выходе (в противоположность классификации-определению заранее определенных категорий). Здесь также есть два больших кластера подходов: нейросетевые и классические. Нами были опробованы оба и принято решение использовать модель на основе градиентного бустинга.

В качестве основных признаков, использовавшихся для прогноза значений временного ряда за следующий час, можно выделить следующие:

- ♦ лаговые значения (то есть значения временного ряда за предыдущие моменты времени);
- ♦ полиномиальные признаки от лаговых признаков (то есть их умножение, возведение в степень);
- ♦ порядковый номер текущего часа, дня недели, месяца (эти признаки закодированы);
- ♦ бинарный признак того, что текущий день является выходным;
- ♦ значения экспоненциального сглаживания ряда с различным коэффициентом сглаживания.

Примеры работы разработанного модуля приведены на рис. 2.

На рисунке 3 также приведён график с результатом работы модуля, а внутри графика ещё один, на котором изображён временной ряд, использованный для обучения прогнозной модели.

ОГРАНИЧЕНИЯ

На протяжении работы мы также столкнулись с определёнными ограничениями данного подхода. Особенно хочется отметить необходимость оценивать в целом прогнозируемость временных рядов. Описанный подход довольно успешно можно применять в тех случаях, когда ряды прогнозируемы, но на практике бывают случаи, когда ряды сами по себе плохо прогнозируемы и больше напоминают шум. Поскольку каждый ряд описывает количество логов с конечного устройства, а бывает и такое, что устройства постоянно меняют своё поведение (изменяется режим работы, сменяются пользователи этого устройства и т.д.). Необходимо отлавливать такие случаи и обрабатывать их отдельно.

* * *

Подводя итог, можно сделать вывод о том, что автоматический контроль количества логов с каждого устройства является дополнительным средством обнаружения инцидентов информационной безопасности. Таким образом, команды SOC могут использовать машинное обучение для выявления новых инцидентов, а значит, более оперативно устранять возникающие угрозы.



Антон ТИХОНОВ
эксперт решений
по защите от сложных угроз,
«Лаборатория Касперского»



Сергей ШТИН
эксперт решений для центров
мониторинга, «Лаборатория
Касперского»



Дамир ШАЙХЕЛИСЛАМОВ
руководитель группы развития
решений по защите от сложных угроз,
«Лаборатория Касперского»

АЛЬТЕРНАТИВА SOC?

РОЛЬ XDR В СОВРЕМЕННЫХ ЦЕНТРАХ МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

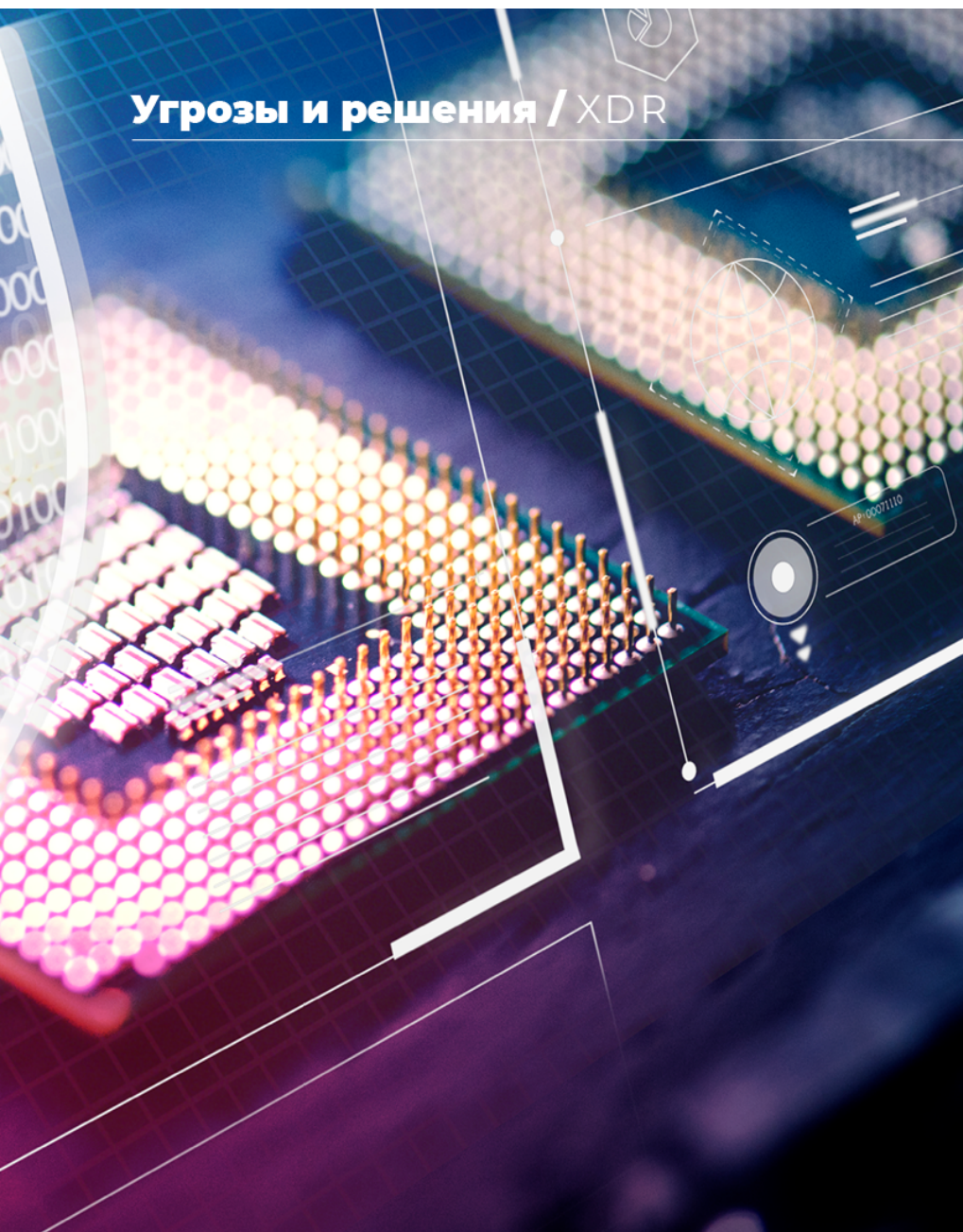
Задача автоматизации рутинных процессов обнаружения и реагирования на угрозы с целью минимизации затрачиваемого на них времени обозначена перед всеми современными командами и центрами информационной безопасности. Данная задача — своего рода вызов для индустрии ИТ и ИБ, ответ на которую компании-производители ищут не первый десяток лет, выпуская на рынок решения для

автоматизации задач сбора и обработки событий (SIEM), автоматизации и управления исполнением рутинных процессов реагирования (SOAR).

Очередным технологическим предложением, находящим всё большее распространение и включаемым в портфель вендоров кибербезопасности, являются платформы расширенного детектирования и реагирования (Extended Detection and Response — XDR). В первом

приближении концепция XDR в части сведения воедино и обработки в реальном времени событий безопасности с различных векторов может показаться крайне близкой по духу и функциональности SIEM-решениям, зарекомендовавшим себя технологическим ядром центров мониторинга.

С появлением на рынке новых продуктов закономерно встаёт вопрос востребованности и обоснованности инвестиций в них. Какую же добавленную



ценность может принести концепция XDR при решении современных задач Security Operations и насколько стоит вопрос замещения уже сложившегося инструментария?

Современные инфраструктуры генерируют нескончаемый поток событий и алертов безопасности в SIEM, так или иначе приводящий к переизбытку информацией команды аналитиков SOC. Недостаток контекста угрозы и детализации по алертам, формируемым независимо при помощи отдельных инструментов, усложняет задачу восстановления целостности картины инцидента за счёт необходимости дополнительных проверок и эскалаций и влечёт ухудшение показателей времени устранения угрозы.

Вывод на рынок концепции XDR как альтернативного подхода к повышению автоматизации и степени наглядности за счёт кросс-продуктовых сценариев и получения общего контекста для разных векторов атак (конечные точки, сетевой трафик и почта, облака, identity, etc.) рассматривается как явление эволюционное, особенно учитывая рост виришь продуктовых портфелей производителей систем безопасности. Стоит отметить, что разнородность продуктовых линеек последних вкпе с сильными и слабыми сторонами производителей ПО приводит к тому, что найти две одинаковые реализации XDR-концепции будет не так просто.

Возможность включения XDR-платформы для закрытия части функ-

ций SOC потенциально обоснована следующими тезисами и драйверами:

1. Уникальность практической экспертизы вендора. Готовый «из коробки» набор корреляционной логики, работающей в парадигме минимизации уровня ложноположительных срабатываний, учитывает даже «слабые» сигналы с источников в процессе выявления угроз. Принимая во внимание всю комплексность и уникальность процессов производства современных решений ИБ, очевидно, что описать внутреннюю поведенческую логику и продуктовую «обязку» точнее производителя этих решений невозможно.

Потенциально при наличии соответствующей технической возможности «сырые» события с сенсоров (к примеру, endpoint-агентов) можно отправлять в SIEM напрямую, однако насколько тяжёлой представляется для команды ноша в виде дополнительного объёма телеметрии, её нормализации и реализации на ней соответствующей детектирующей логики? Да и зависимость схем лицензирования SIEM-систем от потока событий никто не отменял.

Крайне удачной выглядит концепция предварительного обогащения телеметрии дополнительной информацией, углубляющей контекст, снижающей количество событий, отправляемых в SIEM, и уменьшающей требования к SIEM инсталляции. Данное обогащение может быть произведено как на уровне порождения события (APM, сеть, почтовый трафик, веб-трафик, облачные приложения), так и по пути следования к месту сборки в SIEM с использованием данных Threat Intelligence.

2. Повышенная степень автоматизации. Автоматизация тесно связана с интеграционными возможностями, а в XDR интегрированность уже как свойство встроено в архитектуру самой платформы.

При острейшей нехватке человеческого ресурса и экспертизы предоставление удобного механизма расследования, оркестрации и готовых сценариев реагирования на сложные угрозы является в своём роде спасательным кругом и элементом повышения общей эффективности команды. Классический SIEM, как правило, не

В XDR точка потенциального реагирования на условной временной шкале инцидента максимально приближена к точке выявления угрозы, при этом требуя минимальных усилий по настройке

имеет «из коробки» развесистой логики и планов реагирования, или же требуется дополнительная реализация реагирования в смежных системах класса SOAR. Работа с последними уже требует более серьезной аналитической зрелости и тюнинга, а следовательно, серьезных трудозатрат.

В XDR точка потенциального реагирования на условной временной шкале инцидента максимально приближена к точке выявления угрозы, при этом требуя минимальных усилий по настройке. Корреляция событий с нескольких источников и низкий уровень ложноположительных срабатываний позволяет более уверенно осуществлять реакцию на угрозу.

3. Доступность порога вхождения в технологию. XDR и SIEM/SOAR имеют отличающиеся друг от друга циклы интеграции: эффективная реализация SIEM/SOAR априори предполагает проектный и долгосрочный характер (может занимать годы), сильно зависит от планирования и отличается высокими требованиями к команде. Для отдельных организаций начать с реализации «коробочного» XDR-решения — значит оперативно выйти на уровень эффективности исполнения стоящих задач и сбалансировать показатель ROI.

4. Инструменты глубокого расследования. Даже обладая событиями, собранными со всех источников эшелонированной системы защиты, извлечь из них контекст, на основании которого аналитик мог бы оперативно принять обоснованное решение о выборе той или иной опции по реагированию, — непростая задача. Важным фактором здесь является требуемая высокая степень компетенции как минимум в двух обширных областях:

1) Применяемые решения ИБ. Данная область требует от эксперта четкого понимания тонкостей в работе

используемых решений, а также, возможно, навыков в пусконаладке и их администрирования.

2) Системное окружение, где выявлен инцидент, реагирование на который необходимо произвести. В эту область входит знание особенностей среды, понимание той инфраструктуры, мониторинг и защиту которой осуществляет аналитик, знание основных тактик, техник и процедур злоумышленников, а также методов реагирования на них.

Детектирующая логика SIEM-систем довольно часто строится на отдельных событиях или на связке нескольких корреляционных событий, что потенциально может дать представление о взаимосвязях событий в ходе атаки, однако для действительно сложных кейсов задача восстановления хронологии атаки не проста. В таких случаях, как правило, потенциальный масштаб атаки аналитик вынужден определить самостоятельно, формируя и проверяя собственные гипотезы, осуществляя поиск событий в «окрестностях» алерта (поиск подозрительных событий на хосте, включая работу легитимных утилит и др.) и добавляя новые подозрительные события в алерт вручную.

Предлагая к реализации концепцию XDR, вендоры безопасности поставляют не только технические средства защиты, но также и контекстные модели взаимосвязи разрозненных событий, проработанные сценарии реагирования на них и дополнительный аналитический инструментарий. В частности, в роли последнего может выступать хронологически выверенный визуальный граф связей.

Если же речь идет о сопровождении процесса поиска угроз, то в этом случае платформа XDR предоставит доступ к данным киберразведки (Threat Intelligence) своего или независимого производителя.

О ВАЖНОСТИ ИНТЕГРИРОВАННОЙ ИСТОРИИ

Вместе с описанными выше возможностями, на текущий момент гибкость SIEM-технологии в части реализуемых сценариев (use cases) и функций (лог-менеджмент, поведенческая аналитика и др.), подключения множества разнородных и сторонних источников, закрытия compliance-вопроса вкуче с уже состоявшимися инвестициями в проект (а внедрение SIEM — это всё же проектная активность) ещё остаются факторами, сдерживающими процесс полноценной замены SIEM как некой универсальной и централизованной платформы безопасности альтернативой в виде XDR.

Факт принадлежности продуктов-компонентов одному-единственному вендору средств защиты, присущих классическому представлению об XDR, также может навести заказчика на мысль о потенциальном закрытии лишь ограниченного спектра сценариев (для которых у производителя есть продукт и соответствующая экспертиза).

Крайне важно отметить, что производитель, в продуктовый портфель которого входят оба технологических решения, способен реализовать явное преимущество при построении так называемой открытой XDR-платформы (Open XDR), в которой компоненту SIEM отведена роль не только как точки сбора и обработки событий и инцидентов, но и как источника обогащённой телеметрии для того же XDR, реализовывая тем самым замкнутую циклическую систему по выявлению инцидентов без оглядки на производителя конечного устройства источника событий.

Всё это с уверенностью позволяет сказать, что оба класса технологий могут взаимно и органично обогащать друг друга за счёт свойственных им специфичных сценариев, адресуя всё больший фокус на автоматизацию и глубину процесса расследования и реакции на сложные и целевые угрозы, в то же время минимизируя объём требуемых ресурсов.



Павел ПУГАЧ
системный аналитик
«СёрчИнформ»

ПОЧЕМУ SIEM-СИСТЕМА БОЛЬШЕ НЕ РОСКОШЬ

И КАК ВНЕДРИТЬ ЕЁ БЫСТРО

S IEM-система из нишевого решения превратилась за последние годы в маст-хэв-продукт для многих компаний. Подстёгивал процесс ФЗ-187 о критической инфраструктуре и постоянный рост киберугроз, контролировать которые вручную в большой ИТ-инфраструктуре невозможно. Экстренное импортозамещение-2022 прибавляет проблем.

ЗАЧЕМ НУЖНЫ SIEM-СИСТЕМЫ И ПОЧЕМУ ИХ ЗНАЧЕНИЕ ВОЗРАСТАЕТ

С рынка ушли ключевые зарубежные вендоры (IBM, HP, Microsoft, Oracle, Fortinet), риск того, что какие-то разработчики ещё покинут рынок, сохраняется. Это создаёт российским компаниям множество рисков. Зарубежные поставщики могут отключать функциональность удалённо. Не дожидаясь конца истечения лицензий, предоставление услуг могут остановить. Может отказать железо. Растут инсайдерские риски. Актуальны проблемы контроля обновления ПО в сочетании с противоположным риском, что это же обновление сделает из оборудования бесполезный кусок «железа».

За что хвататься ИТ- и ИБ-специалисту? Сколько времени он должен тратить, переключаясь из консоли одного защитного решения в другое? SIEM-системы в этой ситуации приобретают совершенно новую актуальность, потому что позволяют работать со всеми

логами из одного окна, а также видеть взаимосвязи между этими логами, распознавая в их цепочке инцидент, оповещающая о нём ИБ-специалиста.

КАК ВНЕДРЯТЬ SIEM БЫСТРО

Несмотря на то что рынок SIEM зрелый, системы отличаются друг от друга, выбрать «просто любую» может быть большой ошибкой. Сюрпризы могут быть на моменте расчёта конечной стоимости, необходимости что-то докупать или нанимать отдельных специалистов.

«СёрчИнформ SIEM» может стать решением в ситуации, когда нужно внедрить систему быстро. Мы разрабатывали её «коробочной», с возможностью развернуть ПО за один день.

Легко начать работу. Интерфейс «СёрчИнформ SIEM» понятен любому, кто хоть раз открывал «Ворд» или «Эксель». Мы вынесли создание правил в графический интерфейс — это просто и понятно для пользователя. Для работы с системой не нужно выделять отдельного человека.

Универсальные предустановленные правила. Они дают точку опоры на первом этапе, чтобы можно было организовать работу с первого дня внедрения. Администратор SIEM сразу покажет результат руководству и дальше продолжит настройку под нужды своей компании. «Из коробки» доступно больше 350 правил.

Система имеет все самые нужные коннекторы, а также пользовательский Custom Connector, который позволяет

с помощью простых скриптов подключить любой источник. Образцы этих скриптов, написанные на PowerShell script, вы также найдёте в «коробке».

Не нужно докупать отдельные модули — весь заявленный набор функций доступен в одном решении. Часто заказчики сталкиваются с противоположной ситуацией и просчитываются на старте — в итоге рассчитанная сумма закупки оказывается гораздо больше.

Бесплатная помощь в настройке. Давние клиенты «СёрчИнформ» знают о нашем отделе внедрения — это специалисты с высокой квалификацией и опытом работы с сотнями клиентов. Поэтому они, как и инженеры техподдержки, берут на себя весомую часть забот. Это позволяет успешно внедрять решения, даже если у вас в компании есть дефицит специалистов в ИТ- или ИБ-отделе.

Лучший способ убедиться в том, что решение подходит, — проверить его на практике. У нас это бесплатно. Заполните заявку на сайте и получите «СёрчИнформ SIEM» в полном функционале на 30 дней:





Анастасия ЗУЕВА
старший менеджер
по продуктовому маркетингу
Positive Technologies

ДИСЦИПЛИНЫ В БАНКАХ БОЛЬШЕ

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ В КРЕДИТНО-ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ

Недавно мы провели опрос¹ специалистов по кибербезопасности, чтобы выяснить, как построен процесс управления уязвимостями (vulnerability management) в российских компаниях. Специально для читателей BIS Journal рассмотрим результаты опроса представителей ИБ в привязке к кредитно-финансовой отрасли.

В исследовании приняли участие эксперты из 42 компаний банковского сектора, из них 50% относятся к средним по размеру организациям (от 250 до 3000 сотрудников), 31% — к крупным (более 3000 сотрудников), 19% — к небольшим (до 250 сотрудников).

ИНСТРУМЕНТЫ VM В БАНКАХ

Для работы с уязвимостями специалисты по ИБ банковской отрасли исполь-

зуют в основном российские коммерческие VM-решения (50%) (рис. 1).

По сравнению с общей тенденцией по рынку, в банковской сфере выше доля тех, кто собирается перейти на российские решения (31% против 18%). Такой тренд можно объяснить тем, что к субъектам критической информационной инфраструктуры, к которым в большинстве своём относятся и финансовые организации, применимо требование о переходе со средств защиты информации из недружественных государств, согласно Указу Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Несмотря на это, доля тех компаний, которые готовы продолжать использование иностранных решений в кредитно-финансовой сфере, выше, чем по всему рынку (21% против 8%). При этом больше половины опрошенных используют иностранное решение вместе с open-source-сканерами (56%), а треть — вместе с российским VM-решением (33%). Оставаться на иностранных решениях всё сложнее для российских пользователей. Во-первых, они перестают получать официальные обновления, то есть информацию о новых уязвимостях. Во-вторых, российские компании сейчас переходят на отечественное ПО,

и нужно решать, как анализировать его защищённость, — и тут иностранные VM-решения не помогут с поддержкой сканирования отечественного ПО.

Треть специалистов отметили, что прибегают к решениям open source для выявления уязвимостей (31%). Однако рост интереса к open-source-решениям имеет нюансы. Во-первых, применение open source вызовет необходимость в высококвалифицированных специалистах — тех, кто знает, как самостоятельно поддерживать и развивать данное ПО в соответствии с запросами компании. Либо таких специалистов будут нанимать в штат, либо компании будут использовать сервисную модель, то есть платить сторонним организациям, которые будут дорабатывать и обслуживать исходно бесплатное ПО. Во-вторых, сейчас меняется подход к обеспечению безопасности. В банковской отрасли цена ошибки слишком высока: организация напрямую оперирует большими денежными потоками. Остро встанет вопрос надёжности и безопасности кода программы. Если раньше пользователи полагались только на вендора и аттестацию, сертификацию регуляторов, то теперь необходимо будет самостоятельно контролировать надёжность и безопасность решений: создавать карантин для обновлений и тестировать обновления на

¹ Ознакомиться с результатами опроса можно по ссылке:



наличие скрытых функций. Главное, ни в коем случае не обновлять напрямую ПО из интернета без проверки.

ОЖИДАНИЯ ОТ VM-РЕШЕНИЙ

Мы спросили участников опроса, какими возможностями должна обладать VM-система для решения задач компании. 71% респондентов из финансового сектора отметили, что нуждаются в интеграции VM-продукта с другими решениями для ИБ. 62% участников опроса отметили, что хотят получать уведомления о новых уязвимостях от вендора.

64% специалистов отметили учёт значимости активов сети. Это позволяет упорядочить работу, вовремя обращать внимание на активы, эксплуатация уязвимостей на которых может нанести больше всего вреда организации. В новой версии системы управления уязвимостями MaxPatrol VM можно автоматизировать присвоение значимости IT-активам. Например, задать высокий уровень значимости всем контроллерам домена. Также продукт информирует пользователя о новых, ещё не оценённых активах. Это позволит специалистам по ИБ тратить меньше времени на ручную обработку результатов сканирования (рис. 2).

ИЗМЕНЕНИЯ В ПАТЧ-МЕНЕДЖМЕНТЕ

За последние несколько месяцев изменения произошли и в подходах компаний к патч-менеджменту иностранного ПО и open-source-решений (рис. 3).

74% специалистов из банковской отрасли внесли изменения в патч-менеджмент после февраля 2022 года. На решение повлиял возросший риск получить недеklarированные возможности в новых обновлениях от иностранных вендоров. Специалистам по ИБ приходится делать сложный выбор: обновлять ПО с риском получить вместе с исправлением недокументированные возможности или не обновлять и копить известные и неизвестные уязвимости.

Большая часть респондентов (31%) выбрала подход, когда обновляются только критически важные узлы, 29% выбрали увеличить сроки проверки ПО в тестовой среде перед обновлением. Этот метод помогает отследить аномальное поведение системы в закрытой

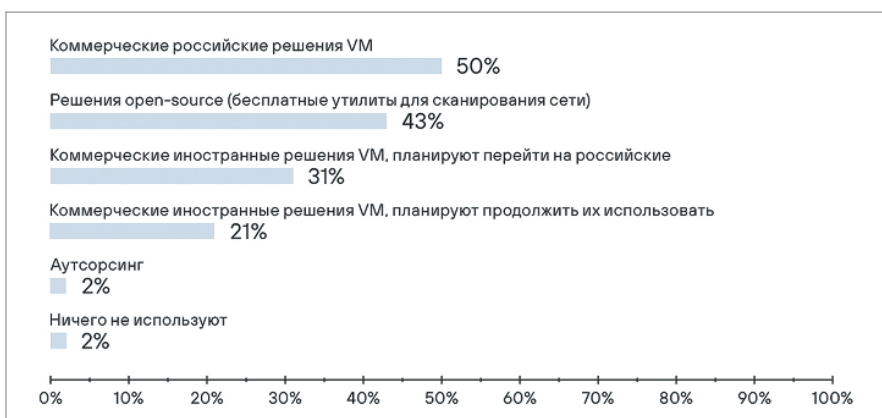


Рисунок 1. Какие продукты для управления уязвимостями используют в кредитно-финансовой отрасли

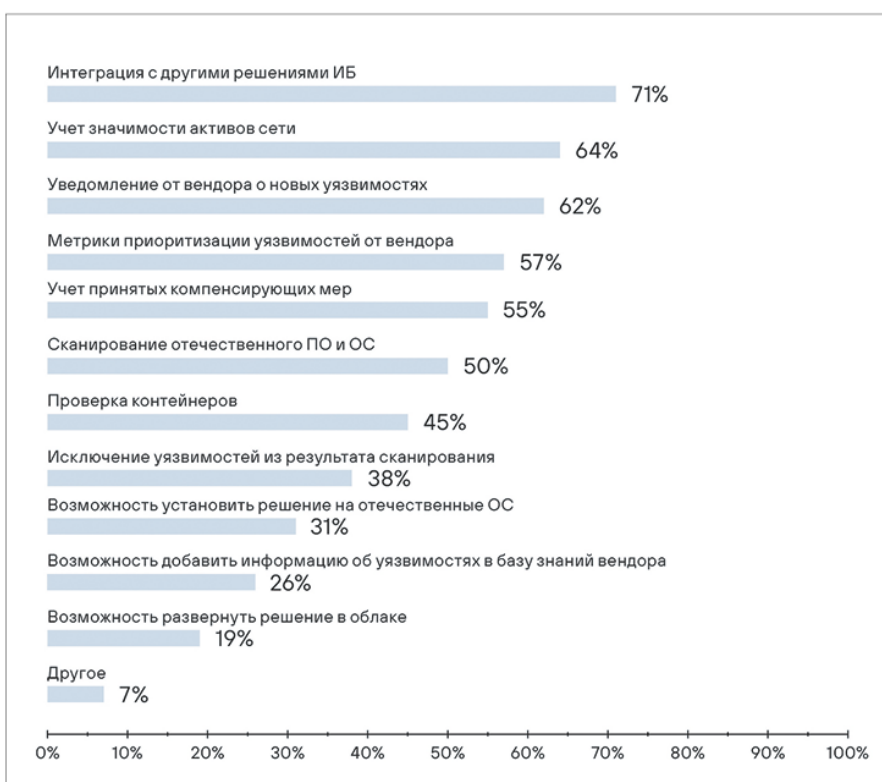


Рисунок 2. Какими возможностями должно обладать VM-решение, по мнению представителей финансовых компаний

среде и выявлять наличие скрытых функций. Доля компаний банковской отрасли, приостановивших обновления на всех узлах, существенно ниже (14%), в сравнении с тем же показателем для всех отраслей (26%). Это в том числе говорит о том, что представители банковской сферы оценили риск взлома системы через накопленные уязвимости выше, чем риск получения обновления с недокументированными возможностями.

Посмотрим на связь ответов с размером финансовой компании (рис. 4).

Представители крупных кредитно-финансовых организаций в большинстве случаев обновляют только критически важные узлы (46%), средний бизнес сделал ставку на увеличение сроков проверки ПО в тестовой среде перед обновлением (38%), а среди малого бизнеса нет явного перевеса на каком-то одном из подходов (25% уве-



Рисунок 3. Как в 2022 году компании финансового сектора изменили процесс патч-менеджмента

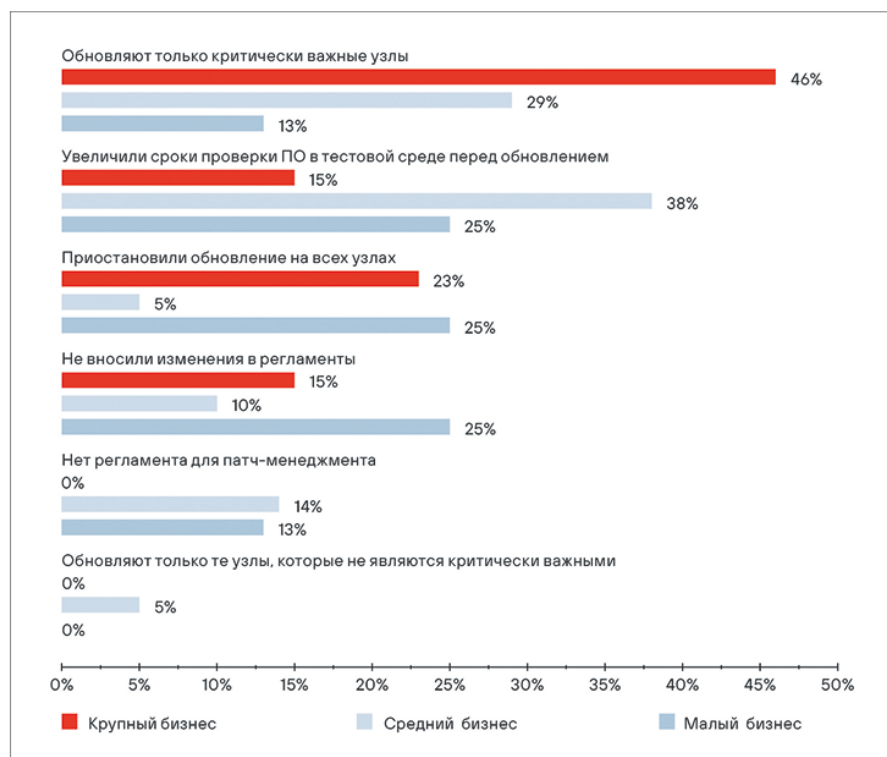


Рисунок 4. Связь ответов респондентов с размером финансовой компании

личили сроки проверки ПО в тестовой среде перед обновлением, 25% приостановили обновления на всех узлах, 25% не вносили изменения в регламенты).

СПЕЦИФИКА VM В КРЕДИТНО-ФИНАНСОВОЙ ОТРАСЛИ

Мы сравнили ответы респондентов из финансовой отрасли с ответами участников опроса из других отраслей. Ожидаемо банки уделяют больше

внимания управлению уязвимостями. Для сферы финансов характерно следующее.

♦ Гораздо ниже доля специалистов, которые не используют специализированные средства для выявления уязвимостей (2% против 15%).

♦ Отсутствие патч-менеджмента встречается реже, чем в целом по рынку (10% против 15%).

♦ Средний срок устранения критически опасных уязвимостей на приоритет-

ных для компании активах — один-два дня (38%), неделя (40%). Ни один из опрошенных специалистов банковской сферы не отметил вариант устранения критически опасных уязвимостей в течение полугода (0% против 10% специалистов других отраслей).

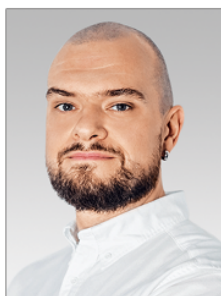
♦ В банковской сфере действует более четкое разделение ИБ и ИТ. Ни один из опрошенных не отметил, что устанавливает патчи самостоятельно (против 20%).

События 2022 года принесли специалистам по кибербезопасности новые вызовы, в том числе и службам ИБ банковской сферы.

Во-первых, мы отмечаем рост кибератак на российские компании². С одной стороны, это заставляет ответственно подходить к вопросам защиты — убедиться, что даже в нештатных ситуациях процесс vulnerability management работает и уязвимости инфраструктуры закрываются вовремя. С другой стороны, появился страх небезопасного обновления иностранного ПО, а соответственно, и невозможности закрытия в нём уязвимостей. Из-за этого компании вынуждены были вносить изменения в уже выстроенный процесс патч-менеджмента.

Во-вторых, на ситуацию влияет и массовый переход компаний с иностранного ПО на российские решения. Это обезопасит компании от риска получить недокументированные возможности через обновления, но при этом не снимает с компании задач проверки российского ПО на наличие уязвимостей. Тут нужно заранее думать о том, какие средства защиты поддерживают российские системы, а производители российского ПО, в свою очередь, должны корректно работать с уязвимостями — выпускать бюллетени безопасности, заводить уязвимости в БДУ ФСТЭК.

² Исследование Positive Technologies: в I полугодии 2022 года количество атак увеличилось на 16% по сравнению с 1-м полугодием 2021 года (<https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/>).



Сергей НЕЙГЕР
директор по развитию бизнеса
АО «Перспективный мониторинг»

ПОСТАВЩИКИ THREAT INTELLIGENCE УШЛИ

НО THREATS ОСТАЛИСЬ

В текущем году из России ушли или сократили своё присутствие большинство западных поставщиков средств защиты информации и сведений о киберугрозах. Однако число угроз и количество атак на российские информационные ресурсы кратно возросло, как вырос и объём ресурсов, которые используют злоумышленники. В этой связи особенно остро стоит вопрос своевременного получения сведений о киберугрозах и интеграции этих сведений со СЗИ. Это помогает оперативно выявлять компьютерные атаки, обогащать данными события безопасности и расследовать инциденты информационной безопасности.

ТИ

В России интерес к ТИ формируется примерно с 2016–2017 года. И за это

время многие отечественные компании научились правильно применять сведения о киберугрозах в своих процессах обеспечения ИБ. Для чего они, как правило, используют специализированные решения для накопления, хранения и систематизации ТИ — Threat Intelligence Platform (TIP) и решения, где эти данные могут применяться с наибольшей эффективностью, — SIEM, IRP и SOAR.

Одно из определений ТИ: «Threat Intelligence — это регулярно и системно собирать информацию об угрозах, улучшать и обогащать её, применять эти знания для защиты и делиться ими с теми, кому они могут быть полезны. ТИ — это не только базы сигнатур для IDS или наборы правил для SIEM. ТИ — это процессы, у которых есть владельцы, цели, требования и понятный и измеримый (насколько это возможно)

результат». Исходя из этого определения, справедливо считать, что потребителями ТИ могут быть как люди, так и машины.

Для людей полезными могут быть сведения в виде бюллетеней безопасности «Перспективного мониторинга» (рис. 1), НКЦКИ, FinCERT или других ИБ-вендоров, в виде публикаций в профильных СМИ, порталах, соцсетях. Даже простой обмен мнениями с коллегами на SOC-форуме можно рассматривать как ТИ.

ПМ ПОДСТАВЛЯЕТ ПЛЕЧО

В «Перспективном мониторинге» накоплен и постоянно обновляется большой объём экспертных данных об угрозах для применения в различных средствах защиты информации.

Одним из первых коммерческих продуктов АО «ПМ» стала так называемая

Информационный бюллетень Центра мониторинга АО «ПМ»

Название документа	Информация о ранее неизвестной кампании по распространению вредоносного ПО через скомпрометированный ресурс: infraads.ru
Разослан	2022-07-18
Идентификатор	AM-2022-ALE-0718-01
Описание угроз	Объект уязвимости: Компонент в браузере Google Chrome Требования к атакующему: Удаленный неаутентифицированный Максимальный результат атаки: Исполнение произвольного кода Источник уязвимости: Неизвестно

Рисунок 1. Подписаться на информационную рассылку бюллетеней безопасности ПМ можно путём обращения в произвольной форме на адрес электронной почты info@amonitoring.ru.

QR-код для обращения на почту:



Exploit-DB	Packet Storm Security	NVD CVE	Zero Day Initiative
Malware Traffic Analysis	DHS CISA	GitHub	FinCERT
FireEye Threat Research	CrowdStrike Research	Cisco Talos	McAfee Labs
Dr. Web	ESET WeLiveSecurity	Proofpoint Threat Insight	Positive Technologies
TrustWave SpiderLabs	ThreatPost	HackerNews	KrebsOnSecurity
Securelist	SecLists Full Disclosure	Fortinet Threat Research	Palo Alto Unit42
SecurityFocus	Trend Micro Research	Check Point Research	[...]

Рисунок 2. Система сбора данных о киберугрозах получает информацию из более чем 27 открытых источников

база решающих правил AM Rules, которая успешно применяется для обнаружения и предотвращения атак в сетевом трафике с использованием «движков» Snort, Suricata и решений на их основе. В текущих условиях, когда зарубежные СЗИ лишились технической поддержки и обновлений, ПМ может качественно заменить необходимую экспертизу. База AM Rules используется в линейке решений сетевой безопасности ViPNet производства ИнфоТеКС, продуктах других отечественных производителей, конечными пользователями сетевых сенсоров. В настоящий момент в базе 24 тысячи правил. База обновляется и пополняется ежедневно, постоянно актуализируется и тестируется на вредоносных объектах и трафике, накопленных за 10 лет работы компании.

В начале 2022 года разработчики «Перспективного мониторинга» поставили перед собой амбициозную цель — категоризировать Интернет. Решение этой задачи продолжается,

и на текущий момент в базе URL-фильтрации ПМ 81 категория доменов, 11 миллионов собранных доменных имён русскоязычного и англоязычного Интернета, 1,5 миллиона откатегоризированных доменов. Эти экспертные данные могут применяться ИБ- и ИТ-службами для ограничения доступа к веб-ресурсам, контентной фильтрации, мониторинга интернет-активности пользователей организации. Если в организации контролируется доступ в Интернет, то использование категорий позволит сконфигурировать гранулированные политики доступа к сайтам и веб-приложениям. Целевыми системами для интеграции базы данных URL-фильтрации могут быть межсетевые экраны (NGFW), прокси, сетевое оборудование, поддерживающее данную функциональность. Также существует и вариант поставки этих данных через обращение к API. Важно отметить, что речь идёт не о базе так называемых плохих доменов, которые злоумышленники используют для заведомо

вредоносной активности, а о базе легальных доменов, для которых необходимо определить тематику сайта.

Ещё одно направление «Перспективного мониторинга» — это TI-фиды. В настоящий момент мы предоставляем три типа данных: IP-адреса, домены и хеш-суммы вредоносных объектов. Подразделение исследования киберугроз еженедельно выпускает обновления базы с подробным описанием указанных индикаторов компрометации (IOC). TI-фиды формируются в стандартном формате STIX2 для удобной и быстрой интеграции с имеющимися средствами защиты информации. А благодаря собственной среде сбора и обработки сведений об IOC возможно предоставление фидов в любом необходимом виде, включая JSON и XML.

В АКТУАЛЬНОМ СОСТОЯНИИ

Все типы экспертных данных «Перспективного мониторинга» на постоянной основе обновляются и уточняются. Например, если первоначально у ПМ есть информация о конкретном эксплойте на уязвимость, то сигнатура на конкретный эксплоит будет добавлена в БРП. И если появляется дополнительная информация, позволяющая выявлять различные варианты её эксплуатации, то аналитики доработают имеющуюся сигнатуру или напишут новую. При этом старое правило удалят

На текущий момент в базе URL-фильтрации ПМ 81 категория доменов, 11 миллионов собранных доменных имён русскоязычного и англоязычного Интернета, 1,5 миллиона откатегоризированных доменов

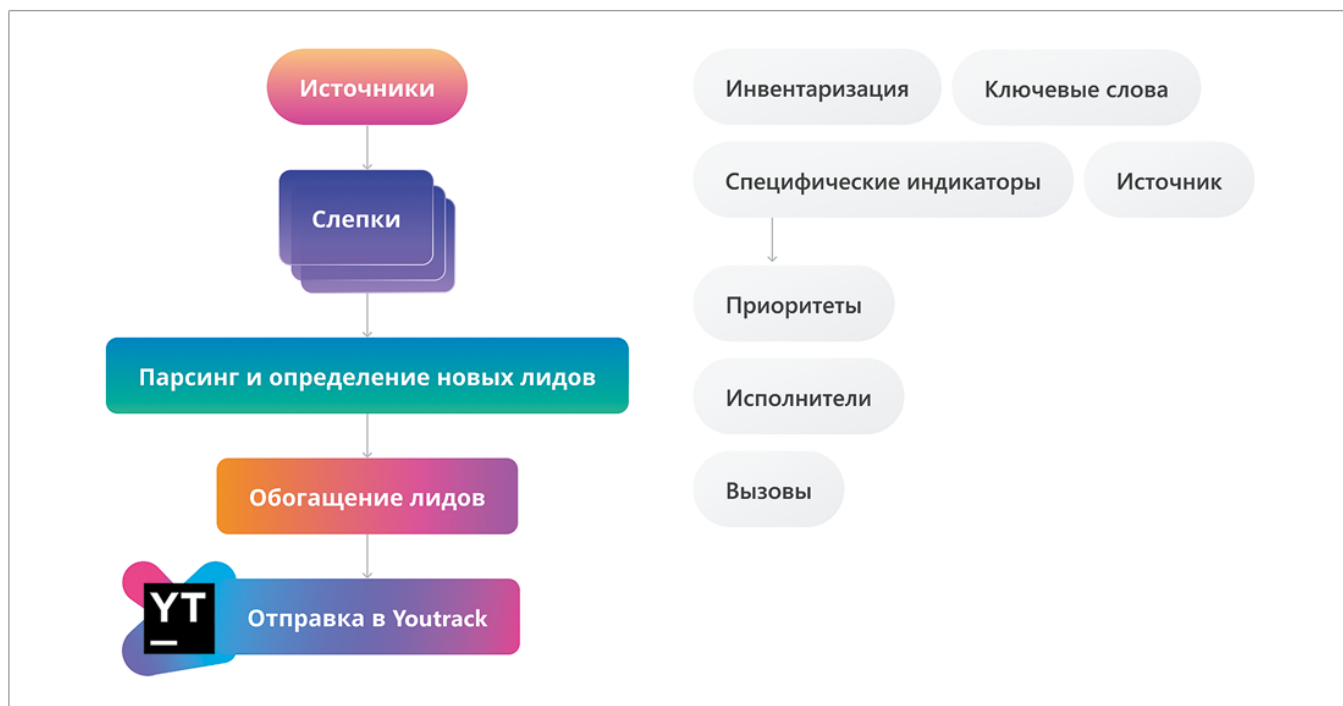


Рисунок 3. Схема сбора и обработки данных

из набора, чтобы оптимизировать производительность. Также отработываются и ложные срабатывания, которые мы получаем от пользователей.

ДЛЯ КАКИХ ЗАДАЧ ЦЕЛЕСООБРАЗНО ПРИМЕНЯТЬ ТИ-ФИДЫ

Первая, самая очевидная задача — обнаружение индикаторов компрометации в своей ИТ-инфраструктуре. Если в системе присутствуют файлы, соответствующие вредоносным образцам, или в журналах сетевого оборудования или прокси есть обращения к «плохим» адресам или доменам, то это повод подробнее разобраться в ситуации.

ТИ-фиды и сигнатуры можно применять и для блокирования вредоносной активности, если сетевые и хостовые IPS/IDS работают в режиме prevent.

Важная задача, которую решают компании с высоким уровнем зрелости обеспечения информационной безопасности, — это обогащение имеющихся данных о событиях и инцидентах ИБ. Если организация эксплуатирует SIEM-систему, IRP или ТИ-платформу, то из ТИ-фидов ПМ можно получить дополнительные сведения об индикаторах компрометации. К таким сведениям относятся: оценка

опасности, время обнаружения, связанные индикаторы, целевое ПО или системы, название и идентификатор вредоносной кампании.

Четвёртая задача — расследование и установление причин компьютерных инцидентов. Специалисты-форензики получают возможность получать дополнительные сведения об обнаруженных индикаторах компрометации.

КАК МЫ СОБИРАЕМ ЭКСПЕРТНЫЕ ДАННЫЕ

В настоящий момент система сбора данных о киберугрозах получает информацию из более чем 27 открытых источников (рис. 2).

Из этих источников мы забираем HTML и храним у себя. Потом происходит постобработка, каждый HTML превращается в набор логических единиц с помощью обработчиков (на каждый источник свой обработчик). Новыми единицами считаются те из момента N, которых не было в момент N-1. Далее происходят дообогащение и фильтрация. Общая схема представлена на рисунке 3.

Важным источником сведений для ТИ-фидов является многотысячный парк сетевых и хостовых сенсоров ViPNet, которые эксплуатируются у десятков

заказчиков коммерческого SOC «Перспективного мониторинга». Полученные события очищаются от любых чувствительных данных (вроде целевых адресов и доменов) и попадают в состав ТИ.

ВОЗМОЖНОСТИ ПИЛОТИРОВАНИЯ И ВАРИАНТЫ ЛИЦЕНЗИРОВАНИЯ

Для предоставления любой лицензии на доступ к ТИ-фидам возможен первоначальный пилотный проект. «Пилот» организуется по двум причинам. Первая — проверка технической совместимости и возможности интеграции с имеющимися или планируемыми к приобретению средствами защиты информации. Вторая причина — проверка полезности. Необходимо проверить, помогают ли новые данные в решении указанных выше задач.

Также у «Перспективного мониторинга» гибкая система лицензирования. Можно приобрести лицензию на произвольный период.

Компания АО «Перспективный мониторинг» также открыта к сотрудничеству с отечественными производителями СЗИ и провайдерами сервисов кибербезопасности.



Владимир УЛЬЯНОВ
эксперт по
кибербезопасности

СИЛЬНЫЙ КОНКУРЕНТ ЗАПАДНЫМ РЕШЕНИЯМ

ДСАР-СИСТЕМА ZECURION ДЛЯ УПОРЯДОЧЕНИЯ
ДАННЫХ В КОРПОРАТИВНОЙ СРЕДЕ

В 2022 году на рынок DСАР-систем вышел новый игрок — российская компания Zecurion, получившая мировое признание и высокие оценки Gartner, IDC и Forrester за собственную DLP-систему. Попробуем критически оценить новый продукт, на что способен, так ли он нов и какие преимущества перед конкурентами может предложить.

ВМЕСТО ВВЕДЕНИЯ — ДЛЯ ЧЕГО НУЖНЫ ДСАР-СИСТЕМЫ

ДСАР (Data-centric audit and protection) предназначены для решения проблемы безопасного хранения информации, а именно:

- ♦ составить полную карту хранения данных, включая почтовые системы и файловые архивы
- ♦ выявить документы, содержащие персональные данные, информацию, попадающую под действие регулирующих актов, сведения, составляющие коммерческую и банковскую тайну и другие типы информации ограниченного доступа.
- ♦ установить контроль над правами пользователей, избежать нерегламентированного и избыточного доступа к важной информации.
- ♦ вести мониторинг движения информации и выявлять потенциально небезопасные действия.
- ♦ оценивать риски, связанные с каждым объектом данных, местом хранения или пользователем.
- ♦ формировать отчетность, показывающую различные срезы данных и связанных с ними событий информационной безопасности.

Перечень широк, но в решениях класса Enterprise DLP уже имелись Discovery-модули, которые находили и

помогали защищать конфиденциальные данные компаний. Тогда зачем понадобился новый продукт?

Zecurion DСАР как элемент единой экосистемы информационной безопасности

Действительно, Zecurion смог использовать свои многолетние разработки в области DLP и хранения корпоративных данных для запуска нового продукта, и в целом DСАР — это один из элементов корпоративной платформы кибербезопасности для защиты от внутренних (DLP, Staff Control) и внешних (NGFW, SWG) угроз с единой консолью управления, общей базой событий и инцидентов, упрощающей расследование любых нарушений в сети. Помимо этого есть Zecurion Storage Security для шифрования данных на серверах и резервных носителях и DСАР. Последние два продукта повышают защищенность информации на этапе хранения, тогда как DLP и NGFW сокращают угрозы при обработке и передаче данных.

Совместная работа нескольких продуктов позволяет уменьшить количество ложных срабатываний за счёт взаимного обогащения данными. А единое хранилище снижает издержки на передачу данных и увеличивает скорость их обработки. Продукты имеют общие политики, обеспечивающие бесшовную защиту от разных угроз по всем каналам передачи данных.

Разработки Zecurion имеют сертификаты ФСТЭК и внесены в реестр отечественного ПО. Портфолио вендора выглядит как сильный вариант для построения полноценной системы безопасности данных на принципах реального, а не «бумажного» импортозамещения.

КАК РАБОТАЕТ ZECURION ДСАР

Ниже, краткий обзор функциональных возможностей Zecurion DСАР в разрезе методологии работы системы — от сбора первичной информации до формирования отчётности.

Сбор данных. Полнота и качество первоначальных данных имеют решающее значение для аудита и безопасного хранения информации. Zecurion DСАР способен контролировать данные находящиеся на файловых серверах, локальных хостах, и в папках общего доступа. Помимо этого, система работает с информацией из служб домена Active Directory и LDAP, а также получает данные о входящей и исходящей электронной почте с серверов Exchange.

Обработка. После сканирования очередного источника данных Zecurion DСАР проводит классификацию содержащейся в нём информации. Цель этого этапа — выбрать из всего массива данных те, что могут представлять ценность для компании.

В отличие от конкурентов, Zecurion применяет свыше 10 технологий контентного анализа, включая словари, морфологию, цифровые отпечатки, метод Байеса и др., которые позволяют очень точно классифицировать информацию.

Анализ угроз. Классификация — это лишь основа для сбора событий информационной безопасности и выявления киберугроз. Ещё на этапе сбора информации DСАР имеет возможность определить так называемые пассивные угрозы: документы с общим доступом, внегрупповые наборы прав, псевдоадминистраторские права. Здесь же определяются реальные

владельцы файлов, подсвечиваются регулярные пользователи тех или иных данных, находятся зоны избыточного доступа.

Однако наибольший эффект даёт динамический анализ данных. Изменение, перемещение, открытие объекта, содержащего критически важные данные, предоставление прав доступа к документу или папке, создание новых и изменение имеющихся наборов прав, а также десятки других событий не только фиксируются системой, но и оцениваются с точки зрения рисков информационной безопасности.

Технологии Zecurion заточены на работу в больших и очень больших организациях. DCAP может обрабатывать события со скоростью до 1 Тбайт в час, её архитектура специально разработана для работы с распределённой сетевой инфраструктурой.

Реагирование. Безусловно, выявлением инцидентов и созданием алертов возможности Zecurion DCAP не ограничиваются. При необходимости Zecurion DCAP может реагировать на обнаруженные нарушения.

Помимо стандартного для DCAP-систем набора функций реагирования, разработка Zecurion обладает расширенным набором возможностей, которые выделяют её среди аналогичных решений. К таким функциям относятся теневое копирование данных. В этом случае офицера безопасности получает в своё распоряжение не просто запись об инциденте, а полную копию данных, связанных с событием.

Zecurion DCAP в автоматическом режиме может заблокировать учётную запись пользователя. Это крайняя, но весьма эффективная мера противодействия утечкам данных. Если есть основания полагать, что сотрудником движут преступные намерения или же его аккаунт взломан, лучше просто лишить его доступа к системе, после чего спокойно разбираться с нарушением. При этом, для проведения дальнейшего расследования не требуется внешний инструментарий, Zecurion DCAP обладает собственным IRP-модулем, куда может быть отправлена информация об инциденте.

Отчёты и интерфейс. Важное преимущество Zecurion DCAP — мощная

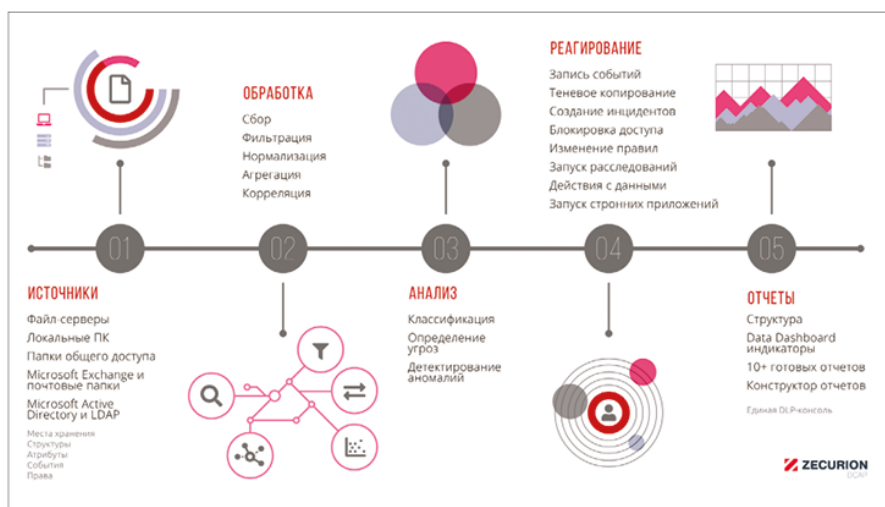


Рисунок 1. Функциональные возможности Zecurion DCAP в разрезе методологии работы системы — от сбора первичной информации до формирования отчётности

система отчётов. Помимо традиционного для продуктов вендора дашборда с таблицами и графическими виджетами, пользователю доступны несколько десятков готовых отчётов, раскрывающих все необходимые срезы собранной базы. Каждый шаблон можно дополнительно настроить, а если и этого окажется мало, отчёт можно собрать, используя удобный конструктор.

Отдельно отметим систему рекомендации Zecurion DCAP. Для большинства контролируемых объектов решение будет рассчитывать уровень риска. Подсистема должна охватить как файлы, папки и хранилища в целом, так и пользователей, группы, конкретного админа, а также структурные подразделения.

ИТОГИ

Безусловно, у Zecurion DCAP большой потенциал в своём сегменте. Функциональные возможности стартового релиза системы сразу выводят её в лидеры сегмента на отечественном рынке и, как минимум, сильного конкурента западным решениям для контроля и хранения данных. Перечислим ещё раз сильные стороны:

- ♦ Глубокая интеграция DCAP с Zecurion DLP и другими продуктам вендора. Системы используют единый массив данных, взаимно обогащая накопленную информацию.

- ♦ Zecurion DCAP использует весь стек фирменных технологий анализа

данных вендора, хорошо зарекомендовавших себя в Zecurion DLP, это позволяет точно классифицировать корпоративные данные.

- ♦ Работа через агенты позволяет Zecurion DCAP собирать максимальный объём данных с конечных точек, серверов и сетевых хранилищ. Кроме того, в ряде случаев агенты могут самостоятельно реагировать на потенциально опасные действия, пресекая возможные инциденты.

- ♦ Глубокий разбор событий Active Directory. Zecurion DCAP не только способен подробно расшифровывать стандартные события службы каталогов, но и может контролировать ещё более полноту десятков действий внутри AD.

- ♦ Помимо операционных систем Microsoft, Zecurion DCAP полноценно работает с серверами и рабочими станциями под управлением ОС на базе Linux.

Как встретит новинку рынок, покажет время. Однако первый взгляд на Zecurion DCAP даёт основание утверждать, что в этом сегменте появился очень серьёзный игрок. Система с архитектурой, заточенной под инфраструктуру Enterprise-заказчиков, обладающая богатым набором функций и технологий, многие из которых уникальны даже по сравнению с глобальными конкурентами. Решение, учитывающее особенности отечественного рынка и поддерживающее широкий стек операционных систем.



Константин ЮДИН
руководитель проектов,
«Доктор Веб»

DR.WEB FIXIT!

НОВЫЙ УРОВЕНЬ РАССЛЕДОВАНИЯ ИБ-ИНЦИДЕНТОВ

В августе 2022 года компания «Доктор Веб» представила широкой публике новый облачный сервис Dr.Web FixIt!¹ — функциональный инструмент, в основе которого лежат российские технологии и собственная многолетняя экспертиза компании «Доктор Веб». Сервис предназначен для дистанционного анализа вирусозависимых компьютерных инцидентов на платформе Windows и устранения их последствий. В его основе — обширная база знаний с информацией о различных типах заражений операционной системы, способах обнаружения признаков компрометации, а также набор алгоритмов выявления и лечения угроз.

С одной стороны, Dr.Web FixIt! — это отдельное многофункциональное средство борьбы с киберугрозами, дополняющее существующие на рынке антивирусные инструменты. С другой — мощное диагностическое решение, которое помогает оценивать состояние компьютеров и выявлять всевозможные неполадки системы и установленного в ней ПО.

ПОКАЗАНИЯ К ИСПОЛЬЗОВАНИЮ DR.WEB FIXIT!

- ♦ Есть подозрение на вирусную активность.
- ♦ Обнаружен аномальный трафик с компьютера в сети.

♦ Необходима проверка компьютера после обнаружения и нейтрализации атаки антивирусными средствами.

♦ Нужно найти отсутствующие обновления ПО/ОС, которые закрывают определённые уязвимости.

♦ Требуется устранить последствия заражения вредоносным ПО.

♦ Необходимо собрать данные при расследовании целевых атак на информационные системы.

♦ Нужно найти нарушения правил и политик ИБ компании.

♦ Нужно выяснить причины произошедших заражений и других инцидентов ИБ.

ОСОБЕННОСТИ СЕРВИСА

Dr.Web FixIt! можно сравнить с работой целой команды Digital Forensics-специалистов, которые шаг за шагом собирают улики киберпреступления и анализируют вектор заражения. Только здесь сбор сведений происходит автоматически, а благодаря фильтрам на анализ полученных данных затрачивается меньше ресурсов и человеко-часов.

Фильтры позволяют выполнять диагностику для выявления аномалий и потенциальных заражений, поиска следов проникновения злоумышленников, возможных уязвимостей и других угроз безопасности (например, отсутствия важных патчей и обновлений ОС). Таким образом, сервис помогает изучать целевую систему по целому ряду параметров и выявлять в ней наличие самых разных проблем. В том числе — присутствие новейшего

вредоносного ПО, включая программы, используемые для целевых атак и не обнаруживаемые никакими иными инструментами.

По завершении диагностики Dr.Web FixIt! позволяет производить лечение заражений, а также исправлять другие выявленные недочёты. Например, корректировать настройки системы или вносить изменения в реестр Windows.

ПРИНЦИП РАБОТЫ

Для первичной оценки состояния проверяемого компьютера (например, следов присутствия в нём неизвестных вредоносных программ или иных признаков компрометации) специалист генерирует диагностическую утилиту Dr.Web FixIt!. Пользователю исследуемой машины лишь необходимо запустить этот модуль — он автоматически сформирует отчёт со всей необходимой диагностической информацией.

Полученный отчёт передаётся в сервис, где оператор, ответственный за разбор инцидента, применяет необходимые фильтры для получения среза интересующих его данных. Существует возможность как использования предустановленных фильтров, так и создания собственных.

По окончании анализа отчёта оператор отмечает выявленные проблемы и выбирает действия и команды, необходимые для лечения целевого компьютера. На этом этапе формируется уникальный экземпляр лечащей утилиты Dr.Web FixIt!. В процессе

¹ <https://www.drweb.ru/fixit/>

работы она внесёт исправления, необходимые именно той конкретной машине, на которой проводилась первичная диагностика. Пользователю останется запустить её, а все действия по исправлению проблем она выполнит сама — в соответствии с заданным скриптом (сценарием) лечения (рис. 1).

После того как лечащая утилита заканчивает работу, она готовит новый отчёт, который также загружается в сервис. Оператор применяет к новому отчёту нужные фильтры и проверяет данные. Если проблемы устранены, задача закрывается. В противном случае формируется новая лечащая утилита, в которую при необходимости добавляются новые команды. Этот процесс повторяется до тех пор, пока инцидент не будет решён успешно.

Утилита Dr.Web FixIt! не требует установки, поэтому её использование не приведёт к конфликту с уже установленными сторонними антивирусами.

КОМУ НЕОБХОДИМ DR.WEB FIXIT!

В первую очередь Dr.Web FixIt! предназначен для специалистов, в чьи обязанности входит мониторинг безопасности компьютерной инфраструктуры и разбор ИБ-инцидентов. То есть специалистам SOC-центров (Security Operation Center). Особенно он актуален в случаях, когда к исследуемой машине нет физического доступа технического персонала соответствующей квалификации.

Кроме того, Dr.Web FixIt! полезен и частным специалистам в области информационной безопасности, и таким компаниям, где квалификация системных администраторов не позволяет грамотно анализировать компьютерные инциденты, связанные с действием вредоносных программ и атаками киберпреступников. Его использование даёт бизнесу возможность оптимизировать расходы на содержание технического персонала.

Dr.Web FixIt! может применяться и для общей диагностики компьютеров по широкому спектру критериев. Например, для поиска потенциального конфликта между установленным ПО, поиска ошибок в работе штатных

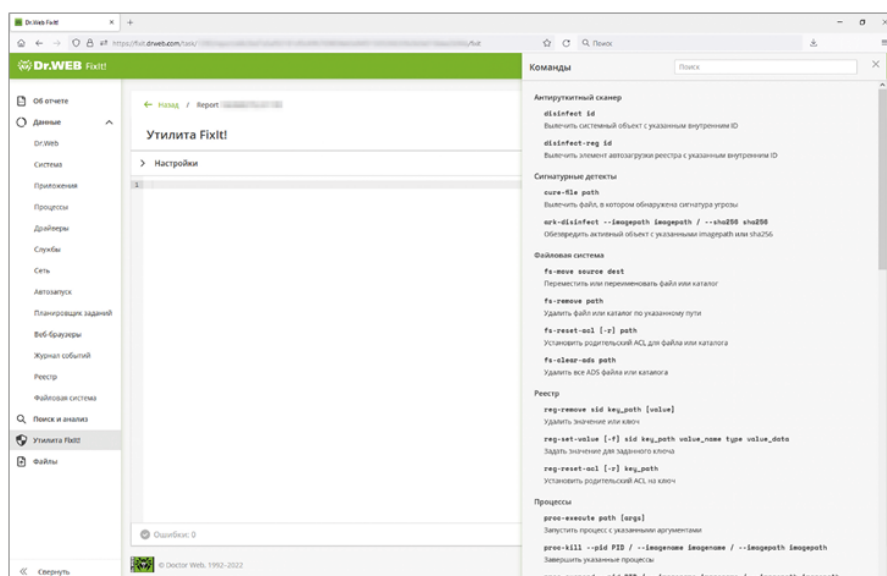


Рисунок 1. Создание лечащей утилиты Dr.Web FixIt! с применением необходимых команд

антивирусных продуктов Dr.Web, установленных на целевой машине, и многих других сценариев.

ОСОБЕННОСТИ ЛИЦЕНЗИРОВАНИЯ

Сервис Dr.Web FixIt! лицензируется по числу задач. Задача — это совокупность мероприятий, в рамках которых выполняется анализ и лечение компьютера. Задачи имеют ограниченный срок действия — 10 дней, по истечении которого все сформированные отчёты остаются доступными, но выполнение новых действий становится невозможным. Для того чтобы продолжить лечение компьютера, потребуется открыть новую задачу, куда можно будет загрузить созданные ранее отчёты. В настоящее время существует возможность приобрести пакеты по 1, 10, 20, 50 или 100 задач. При этом срок лицензии Dr.Web FixIt! — 1 год.

ЭКСПЕРТНОЕ СОПРОВОЖДЕНИЕ ЗАДАЧИ

Приобрести сертификат экспертного сопровождения можно через личный кабинет бизнес-пользователя. В отличие от стандартных, задачи с экспертным сопровождением не имеют ограничений жизненного цикла — они бессрочные.

Экспертное сопровождение задачи может потребоваться, если необходимо:

- ♦ проанализировать данные, полученные с помощью Dr.Web FixIt!;
- ♦ помочь в устранении последствий заражения;
- ♦ определить потенциальные масштабы ущерба на основе анализа обнаруженных вредоносных файлов;
- ♦ проконсультироваться по мерам минимизации потерь и исключению повторения атак.

Поступающая в рамках работы сервиса в «Доктор Веб» информация пользователей регламентируется политикой в области конфиденциальности. Компания обрабатывает её в соответствии с законами РФ и прилагает все возможные усилия для её защиты.

Облачный сервис Dr.Web FixIt! для удалённой диагностики инцидентов ИБ и устранения их последствий позволяет решать вопросы поиска и нейтрализации киберугроз на компьютерах под управлением Windows и улучшать ИБ-защищённость предприятий. Для более детального знакомства с сервисом вы можете запросить демодоступ², после чего принять решение о том, подходит ли Dr.Web FixIt! для решения ваших задач.

² <https://download.drweb.ru/fixit/>

**Максим СТЕПЧЕНКОВ**
RuSIEM

СТРАХОВАНИЕ КИБЕРРИСКОВ — СЕГОДНЯ И ЗАВТРА

ОБЪЕКТИВНЫЕ ОСНОВАНИЯ ДЛЯ РОСТА,
БЕЗУСЛОВНО, ЕСТЬ

В 2021 году спрос крупного бизнеса на страхование киберрисков в России вырос на 60%. По данным компании «АльфаСтрахование», это связано с учащением резонансных случаев атак вирусов-вымогателей в России и мире, а также возросшими требованиями крупных компаний к своим поставщикам по защите конфиденциальной информации. При этом сам рынок довольно небольшой: сегодня страхует киберриски всего 6% компаний. В первую очередь это организации финансового сектора, компании, занимающиеся электронной коммерцией и оказывающие ИТ-услуги, а также крупные промышленные предприятия, активно автоматизирующие свои бизнес-процессы.

Из безусловно положительных сигналов можно отметить следующее. Во-первых, 2/3 купивших полис организаций считают, что это способствовало повышению их привлекательности для клиентов, партнёров и сотрудников. Во-вторых, среди пострадавших от кибератак 9% жалуются, что у них не была оформлена киберстраховка, благодаря которой они

могли бы гораздо быстрее восстановиться. В-третьих, 21% организаций планируют воспользоваться услугой: по их мнению, наличие страховки поможет быстрее восстановиться после реализованной атаки и сделает компанию более защищённой (как правило, об этом говорят крупные компании и организации, обладающие значительными бюджетами и распределённой ИТ-инфраструктурой).

Тем не менее большинство респондентов пока не планируют страховать киберриски. Стоимость страхования определяется многофакторной моделью и сильно варьируется в зависимости от отрасли. В среднем суммы выплат находятся в диапазоне от 1 млн до 700 млн рублей, при этом, по некоторым данным, полис может увеличить бюджет расходов на ИБ на 10–20%. Для 33% опрошенных это либо слишком дорого, либо неочевидно с точки зрения финансовой целесообразности.

ПРОФИЛЬ СТРАХОВАТЕЛЯ

Малый и средний бизнес к страхованию киберрисков пока что просто не готов организационно. Стоимость полиса зависит от результатов аудита инфор-

мационных систем, однако, во-первых, такой аудит сам по себе удовольствие недешёвое, а во-вторых, при выявленных уязвимостях и рисках расходы на страхование часто оказываются сопоставимыми с выстраиванием эффективной ИБ.

Крупным компаниям страховщики часто не готовы предлагать достаточные ёмкости (страховые суммы), поскольку те не разрешают провести аудит по причине высокого уровня конфиденциальности. При этом они в принципе готовы рассматривать страхование киберрисков, если для них будет очевиден смысл подобной страховки.

И те, и другие правы. Вложения в обеспечение информационной безопасности и расходы на страхование должны быть просчитаны и гармонизированы. Иначе финансовый смысл этого инструмента управления риском не будет оправдан. Вопрос в том, как это сделать.

СТЕПЕНЬ ВИНЫ

Ещё один существенный вопрос — насколько сложно будет получить выплаты при наступлении страхового случая (нарушение работы информационных

систем клиента в результате DDoS-атак, взлома сайта компании, взлома инфраструктуры, почты, бизнес-приложений), когда неочевидно, на чьей стороне вина за допущение инцидента. Наличие правил, зафиксированных во внутренней нормативной документации и подтверждённых в правоустанавливающих документах работодателя и работника, может минимизировать эту неопределённость, но на практике ответственность работников за киберинциденты встречается в России крайне редко.

Аналогию можно поискать в страховании киберрисков физических лиц (в части ущерба, возникшего вследствие операций по переводу денежных средств без согласия клиента кредитной организацией). По данным кредитных организаций, агрегируемым и регулярно публикуемым Банком России, порядка 60% таких случаев происходит в результате использования злоумышленниками приёмов социальной инженерии. Формально клиенты добровольно передают конфиденциальную информацию или самостоятельно переводят денежные средства, что даёт банкам законные основания не возмещать ущерб. Однако регулятор

планирует сформировать новые правовые подходы к снижению ответственности потребителей финансовых услуг и развитию страхования их рисков и потерь. Иными словами, Банк России заговорил о балансе ответственности клиента, банка и страховой компании, в том числе в части соразмерности покрытия риску.

По подсчётам страховщиков, убыточность страхового полиса, покрывающего риски социальной инженерии, может быть в 8–10 раз выше, чем без них. Поскольку стоимость риска может быть статистически размыта на большом страховом портфеле, страховка, включающая защиту от социальной инженерии, будет на 25–30% дороже. Разумеется, для корпоративных клиентов цифры будут другие, но возможный порядок разницы очевиден.

ПЕРСПЕКТИВЫ

Число и интенсивность кибератак в краткосрочной перспективе не снизятся. Из в лучшем случае полукриминальной активности хактивизм перешёл в статус крестового похода за справедливостью и праведным отмщением. О прогосударственных акторах СМИ не только пишут, но уже и цитируют

их представителей, что, без сомнения, легализует эту часть жизни в массовом сознании. В России на фоне роста интереса к ИТ-профессиям это будет способствовать росту популяции «белых хакеров», что, в свою очередь, неизбежно спровоцирует наращивание сил «противника».

В этой связи, возвращаясь к причинам низкого спроса, можно предположить, что объективные основания для его роста, безусловно, есть. А вот конкретика будет определяться либо разработанными Банком России для финансовой отрасли и впоследствии адаптированными другими отраслями подходами, либо способностью компаний найти тот самый баланс расходов на ИБ и на страховку рисков, не закрываемых штатными средствами защиты информации.

Как вариант, решением может быть модель конструктора, когда компания сможет самостоятельно выбирать наиболее актуальные для себя риски, а также объём страхового покрытия. Для малого и микробизнеса можно зафиксировать предустановленный максимальный объём страхового покрытия, для крупного бизнеса — проводить индивидуальный андеррайтинг.

В основе любой системы анализа и управления киберриском лежит соотнесение реализованных инцидентов с моделью угроз и взвешивание их по степени опасности для непрерывности производственных и бизнес-процессов, соответствия требованиям законодательства и регуляторов, финансовой безопасности организации, прав и интересов её клиентов и сотрудников и так далее. Концепция управления риском включает как его предотвращение и парирование, так и «принятие риска», когда предотвращение инцидента обходится компании дороже, чем ликвидация его последствий.

Например, многим знаком непростой выбор между внедрением сложных СЗИ и уплатой штрафа. И хотя закон не имеет обратной силы и штрафовать за то, что до его принятия нарушением

не являлось, никто не будет, незакрытая «дыра в безопасности» может стать основанием для принятия мер реагирования по итогам проверки, проведённой по новым правилам. Поэтому, даже принимая такой риск, компаниям, с учётом разработки и вероятного усиления отраслевых требований по информационной безопасности, есть смысл как минимум сохранять события и телеметрию, анализ которых может выявить уязвимости и принять меры по их устранению спустя 1–2 года после инцидента, который было решено проигнорировать. Существующие SIEM-системы позволяют это делать благодаря функции архивирования и кластеризации хранилищ.

Другой пример — риск социальной инженерии. Человеческий фактор — сущность вообще трудно пред-

сказуемая. Точнее, методики есть (например, HRA — Human Reliability Assessment), но для построения прогноза нужно такое количество факторов, сбор которых сопоставим со стоимостью социального исследования методом прямого наблюдения. Гораздо проще составить алгоритм внедрения мер безопасности по принципу «светофора» и последовательно применять его по мере возникновения угроз соответствующего уровня (разумеется, с определённым запасом). И здесь тоже крайне важна правильная настройка в SIEM работы с активами, в частности, мониторинг изменения их свойств при наступлении определённых условий и сведение статистики: 1, 2, 3 однотипных инцидента в неделю — зелёный уровень, 4–7 — оранжевый, 8 и более — красный.



Сергей ПАРФЕНОВ
технический директор
«Фаззи Лоджик Лабс»

СОВРЕМЕННЫЙ АНТИФРОД

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ПРОТИВ МОШЕННИКОВ

Еще в недалеком 2016 году эксперты-практики не прекращали спор о том, заменит ли революционный концепт «машинного обучения» традиционное написание «правил антифрода», и какой метод эффективнее выявляет мошенничество: тот или другой, или оба метода

в комбинации¹. Рассмотрим подробнее эти методы.

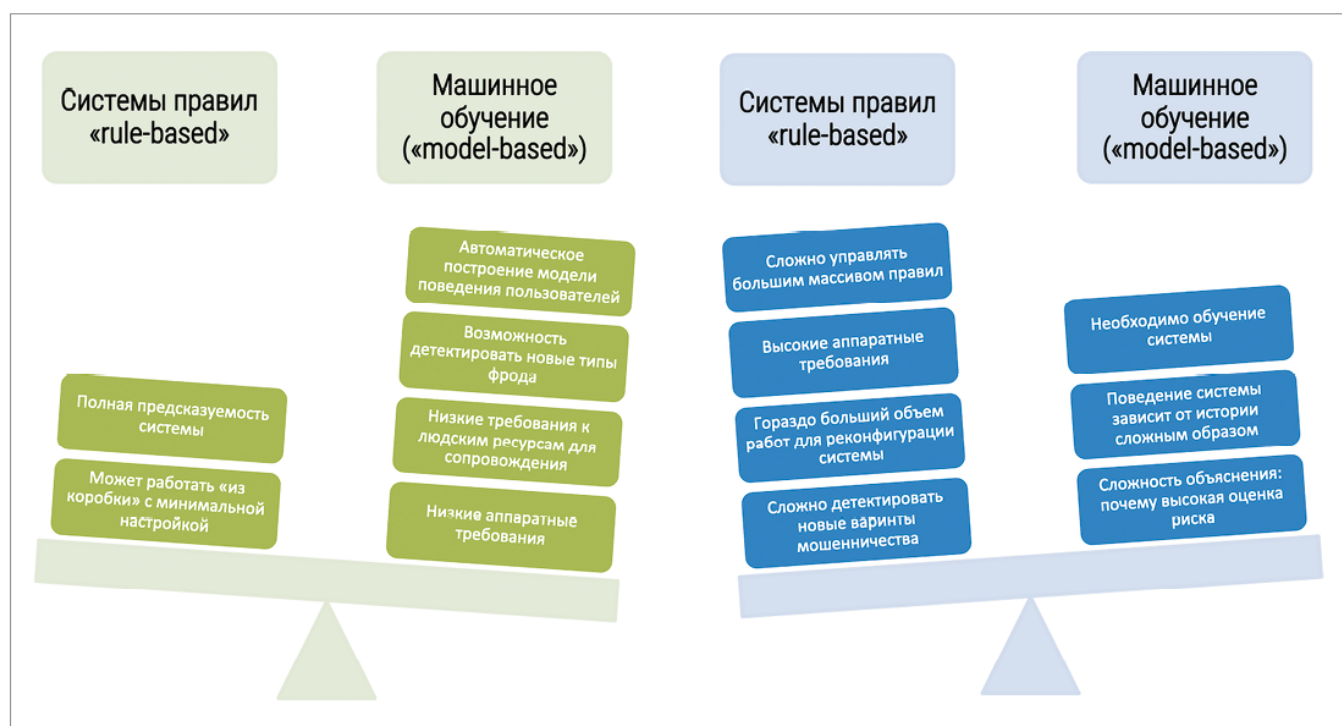
Итак, если ядром антифрод системы мы считаем механизм оценки риска каждой совершаемой транзакции, то все

¹ <https://merchantriskcouncil.org/news-and-press/mrc-blog/2016/is-machine-learning-changing-the-face-of-fraud-prevention>

существующие системы оценки рисков мы делим на два класса:

♦ «rule-based» — оценка рисков на основе правил, примененных ко входным данным;

♦ «model-based» — оценка рисков с применением самообучающихся систем принятия решения.



Кейс	Правило	Условия срабатывания правила	Действия	Управляющее воздействие
Социальная инженерия	Крупный перевод новому получателю	Оценка риска Больше или равно 750 И Срок (в днях) связи получателя с клиентом Меньше или равно 1 И Кумулятивная сумма операции за 1 часа по клиенту получателю Больше или равно 10000000	Review	Добавление атрибутов в список: transactionData.payee в 'Карта получателя: черный список'
Социальная инженерия	Перевод с нового устройства новому получателю	Оценка риска Больше или равно <X> И Срок (в днях) связи получателя с клиентом Меньше или равно 1 И Сумма транзакции Больше или равно <X> И Срок (в днях) с первого использования данного мобильного устройства Меньше или равно 1 ИЛИ Срок (в днях) с первого использования данного интернет устройства Меньше или равно 1	Deny	-

Сейчас, многие современные системы скрининга (фрода, или, например, кредитные системы) совмещают эти два подхода следующим образом:

- ♦ совмещение путем генерации человеко-читаемых деревьев (правил) из натренированных ML-моделей и
- ♦ использование результатов скоринга ML-моделей в правилах, которые создаются вручную.

В нашей компании, развивая кросс-канальную антифрод систему Smart Fraud Detection, мы используем оба подхода — комбинацию методов машинного обучения и методов на основе правил.

Каждый из этих подходов имеет свои преимущества: метод машинного обучения дает возможность обновлять параметры для создания профилей и параметры транзакций в процессе работы (квази-real time) и детектировать новые типы фрода.

А на основе метода правил можно создавать единую модель для разных

категорий клиентов, минимизируя «ручные» процессы.

Приведем пример использования правил «Крупный перевод новому получателю» и «Перевод с нового устройства новому получателю» для выявления одного из типов социальной инженерии.

Сначала полученные данные по клиенту аккумулируются в модуле оценки риска. Это динамическая самообучаемая модель оценки риска, которая позволяет дополнять модель при изменении данных и оперативно реагировать. Так, система собирает большое количество информации и оценивает риск для каждого события в диапазоне от 0 до 1000, чтобы снизить коэффициент ложных срабатываний. Чем больше у события признаков, отличных от модели типичного поведения, тем выше балл риска.

В первом случае возможная оценка риска 750 и более, правило срабатывает при условии минимального срока связи с получателем (меньше одного дня) и максимальной суммарной сумме

денежных средств более или равно 10 млн руб. Здесь требуется проверка оператором легитимности транзакции, а карта получателя (возможно мошенника) отправляется в черный список.

Во втором случае, при заданной оценке риска проходит проверка по нескольким правилам, в результате которой система без оператора отклоняет сомнительную транзакцию.

Далее возможно выполнить оптимизацию правил по социальной инженерии: система по результатам работы предложит новые правила для лучшего нахождения таких операций при минимальном параметре ложных срабатываний.

Таким образом, сочетание методов машинного обучения и метода правил позволяют решать более сложные, комплексные задачи защиты от мошенничества, в том числе от «социальной инженерии».

UserGate SUMMA

ЭКОСИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Иван ЧЕРНОВ
менеджер по развитию
UserGate

Информационная безопасность — это особая сфера, где специалист по защите непрерывности бизнес-процессов всегда должен действовать оперативно: быстро обнаружить угрозу, локализовать ее, не дать распространиться и ликвидировать последствия. Например, COVID-19 так изменил нашу жизнь, что и сейчас удаленный формат работы остается нормой и массовым явлением, при этом любые цифровые устройства сотрудников компании — и ноутбуки и гаджеты — могут быть выведены из строя или скомпрометированы, что может привести к самым печальным последствиям. Утрата доступа к важным данным или их утечка сделают дальнейшую работу организации невозможной. Кроме того, киберугрозы постоянно эволюционируют, меняются модели поведения злоумышленников, а также их цели и инструменты: атаки становятся более совершенными, а их тактики — разнообразнее.

Увеличение нагрузки на безопасность информационных систем и объекты критической инфраструктуры, а также уход из России иностранных вендоров привели к тому, что именно российские решения для обеспечения безопасности пользовательских устройств становятся все более востребованными.

UserGate, в первую очередь, рекомендует комплексные меры защиты, а не отдельные функции в области информационной безопасности. Это именно то, чего ожидают сегодня от российских производителей решений бизнес и государство: не просто средств защиты и услуг мониторинга безопасности, а комплексного обеспечения киберустойчивости, непрерывности всех бизнес-процессов.

Опыт UserGate показывает, что залог обнаружения и успешного отражения атак — а особенно сложных, целевых — заключается в экосистемном подходе к обеспечению контура безопасности. Именно такая комплексная концепция позволит обеспечить главное условие защищенности — абсолютную видимость всех событий безопасности внутри корпоративной сети. В UserGate для решения этих задач разработали экосистему продуктов безопасности UserGate SUMMA. К ключевым аспектам ее работы относятся:

♦ 100% видимость. Технологии UserGate SUMMA позволяют идентифицировать абсолютно всех пользователей сети, определить все приложения и расшифровать до 98% всего неизвестного трафика.

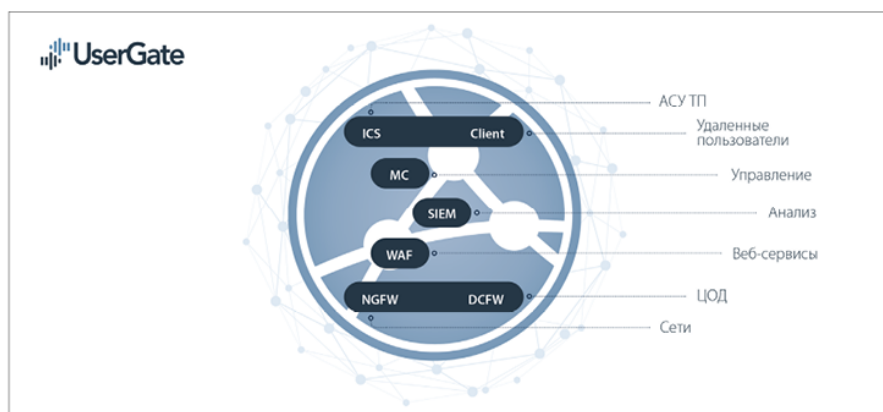
♦ Широкая область применения. Продукты UserGate SUMMA контролируют сетевой трафик на всех рубежах сетевого взаимодействия. Пользовательские рабочие места, локальная сеть, интернет, облачные сервисы и приложения, территориальные филиалы и удаленные сотрудники — везде можно уста-

новить продукты экосистемы UserGate SUMMA для комплексного сбора данных и защиты инфраструктуры.

♦ Агрегация. Единые дашборды, сводные отчеты, централизованная консоль управления — это то, что позволяет экосистеме UserGate SUMMA функционировать сплоченно и слаженно. А экспертиза Центра мониторинга и реагирования UserGate дополнит технологический стек экосистемы и в совокупности с ним обеспечит максимальный уровень безопасности.

♦ Реагирование. Совокупность продуктов и технологий экосистемы UserGate SUMMA, а также экспертизы MRC дает синергетический эффект и позволяет решать ключевые задачи для бизнеса — сокращать скорость реакции на инцидент, а значит снижать последствия от кибер-инцидентов и время простоя бизнес-процессов.

♦ Автоматизация. Продукты экосистемы безопасности UserGate SUMMA интегрированы друг с другом, а набор механизмов автоматизации позволяет настраивать мгновенное реагирование на события безопасности.



UserGate SUMMA — слагаемые безопасности



Kaspersky Unified Monitoring and Analysis Platform

Центральный элемент единой платформы безопасности

- Мониторинг и анализ инцидентов ИБ
- Поточковая корреляция в режиме реального времени
- Автоматическое обогащение данными об угрозах
- Масштабируемая архитектура и низкие системные требования
- Тесная интеграция с решениями «Лаборатории Касперского» и сторонних производителей
- Обеспечение соответствия законодательству в сфере безопасности объектов КИИ

kaspersky АКТИВИРУЙ
БУДУЩЕЕ

kaspersky.ru/enterprise

ДиалОгНаука

СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

dialognauka.ru



XX РКІ-ФОРУМ РОССИЯ

НАСТОЯЩЕЕ И БУДУЩЕЕ ЭЛЕКТРОННОЙ ПОДПИСИ

С 13 по 15 сентября в Петербурге состоялась юбилейная, двадцатая, Международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи: «РКІ-Форум Россия 2022». Мероприятие в очередной раз подтвердило статус одного из самых крупных и представительных отраслевых событий на российском рынке, собрав более 300 участников — представителей регуляторов и ИТ-вендоров, экспертов в области электронной подписи, документооборота, ИБ и криптографии, ведущих сотрудников аккредитованных удостоверяющих центров.

Юбилейный РКІ-Форум прошёл в период глубинных изменений на рынке электронной подписи: продолжается масштабная модернизация законодательства, удостоверяющие центры (УЦ) осваивают новые правила работы, активно разрабатываются отраслевые стандарты и соответствующая нормативная база. Развиваются новые технологии: мобильные электронные подписи, доверенная третья сторона,

машиночитаемые доверенности, архивные документы с электронной подписью. Одновременно с этим российская экономика находится перед лицом новых вызовов. Все эти нюансы отразились на программе РКІ-Форума.

«События, разворачивающиеся с февраля 2022 года, поставили ребром вопрос обеспечения безопасности и независимости страны в сфере ИТ. В этих условиях нужно быстро реагировать, принимать и реализовывать решения. В изменившемся мире вопросы безопасности и доверия звучат по-особенному остро. Подтверждается дальновидность решения отстаивать необходимость применения отечественной криптографии, поддерживать развитие российских производителей. Это даёт нам возможность сегодня смотреть вперёд с оптимизмом, хотя возникшие ограничения и барьеры требуют активной совместной работы отечественных специалистов в поисках непростых ответов. Отрасль электронной подписи и её участники уже неоднократно доказывали своё умение адаптироваться, учитывать меняющуюся обстановку,

сообща и с полной отдачей подходить к обсуждению наиболее насущных проблем», — выразил уверенность председатель Программного комитета РКІ-Форума Владимир Матюхин.

С приветственными словами к участникам форума также выступили заместитель генерального директора компании «ИнфоТеКС» Дмитрий Гусев и заочно — президент Федеральной нотариальной палаты Константин Корсик. Они отметили, что профессиональное сообщество, сложившееся вокруг РКІ-Форума, сохраняет преемственность и выносит на обсуждение наиболее важные вопросы.

ЭП В АТМОСФЕРЕ ДОВЕРИЯ

В первый день мероприятия состоялась ключевая дискуссия «Доверенные электронные услуги: лидеры о будущем в условиях стратегических изменений». Цель данной части деловой программы — обсуждение главного вопроса для отрасли: как регуляторы, законодатели и участники рынка видят актуальные стратегические цели отрасли, каковы критерии качества результатов,

получаемых в результате проводимых преобразований. «Наша отрасль решает задачу обеспечения инфраструктуры и применения базовых, системных компонентов доверия в информационных системах, пронизывает все сферы цифровой экономики. Фактически мы перешли от низкоуровневой, криптографической нацеленности РКІ к сквозной, фундаментальной и системообразующей технологии», — отметил член Совета Ассоциации РОСЭУ, генеральный директор компании «ГАРАНТ Электронный Экспресс» Алексей Пауков.

В дискуссии приняли участие: начальник управления ЭДО ФНС России Фёдор Новиков, вице-генерального директора, руководитель направления «Эффективное регулирование» АНО «Цифровая экономика» Дмитрий Тер-Степанов, директор Фонда «Центр инноваций и информационных технологий» Федеральной нотариальной палаты Михаил Веселов, начальник Управления режима секретности и безопасности информации Федерального казначейства Вячеслав Бражко. Участники сошлись во мнении, что ответ на главный вопрос ключевой дискуссии о том, кто же консолидирует тенденции и определяет стратегию развития отрасли, к сожалению, не радует: хотелось бы, чтобы это было Минцифры, но это, к сожалению, не так.

УЦ: ПЕРВЫЙ ГОД ПО НОВЫМ ПРАВИЛАМ

Далее участники форума подвели итог первого года работы удостоверяющих центров, аккредитованных по новым требованиям. Член Академии криптографии Российской Федерации Александр Баранов, обосновывая вывод о сложности и значительной финансовой ёмкости обеспечения ИБ в больших УЦ, сравнил эту ситуацию с безопасностью системы Госключ (не в пользу последнего). Павел Смирнов, директор по развитию компании «КриптоПро», познакомил слушателей с архитектурой единой цифровой платформы УЦ ФНС России и способами подключения к ней доверенных лиц. Начальник Управления режима секретности и безопасности

информации Федерального казначейства Вячеслав Бражко рассказал о современном состоянии и перспективах развития информационной системы «Удостоверяющий центр Федерального казначейства». Максим Букин, исполнительный директор Департамента по работе с государственным сектором Блока «Корпоративно-инвестиционный бизнес» ПАО Сбербанк, поделился опытом Сбера в роли доверенного лица УЦ ФНС. Начальник управления «Государственные услуги и сервисы для бизнеса» — вице-президент Банка ВТБ Светлана Дементьева завершила сессию докладом «Путь становления банка доверенным лицом УЦ ФНС России».

ДЕЛАЕМ РКІ ПО СТАНДАРТАМ

Финальная сессия первого дня конференции была посвящена вопросам стандартизации в области ЭП, РКІ, криптографии и ЭДО. Отраслевые эксперты оценили уровень стандартизации в отрасли. Модератор сессии, профессор МГТУ им. Н.Э. Баумана, заместитель генерального директора компании «Алладин Р.Д.» Алексей Сабанов обозначил проблемы стандартизации в области РКІ и ЭП. Одна из них — отсутствие стратегического планирования с чётко обозначенными целями и задачами. Выступление руководителя обособленного подразделения «ИнфоТеКС» Михаила Грунтовича было посвящено стандартизации OpenID Connect на базе отечественных криптографических алгоритмов. Представители компании «КриптоПро» познакомили слушателей со схемой подписи вслепую. Наталья Храмцовская, ведущий эксперт по управлению документацией компании ЭОС, посвятила доклад незакрытым проблемам стандартизации ЭДО. Выступление представителей Академии криптографии РФ было посвящено созданию и стандартизации постквантовых криптографических механизмов.

МОБИЛЬНАЯ ЭП

В рамках РКІ-Форума прошёл круглый стол на тему «Мобильная электронная подпись: проблемы и решения». Участники дискуссии обсудили нюансы реализации и сценарии применения мобильной электронной

подписи. Ведущий сессии, заместитель генерального директора «КриптоПро» Станислав Смышляев, указал на то, что именно в части технической реализации мобильной подписи сильно продвинулись все участники профессионального сообщества — разработчики, интеграторы и пользователи. С другой стороны, остаются трудные вопросы, связанные с порядком применения таких средств. Антон Мелузов, заместитель генерального директора «РТЛабс», в докладе «Масштабирование Госключа. Особенности массового внедрения средств электронной подписи» выступил от лица потребителя информационных систем, которые встраивают технологии мобильной подписи в свои решения, системы ЭДО. О совмещении классической и мобильной парадигм работы с квалифицированной электронной подписью говорил директор по развитию компании «Актив» Владимир Иванов. В выступлении «Банковская идентификация в мобильной электронной подписи» Алексей Дегтярёв, руководитель единой цифровой платформы «Тинькофф Банка», представил позицию клиента мобильного банковского сервиса. В рамках дискуссии прозвучало мнение о том, что для решения различных задач потребителей востребованными останутся все ранее существовавшие и новые варианты ЭП: мобильные, облачные, локальные, квалифицированные, неквалифицированные и другие.

ДОВЕРЕННОСТИ. ДОВЕРЯЕМ ИИ

Сессия «МЧД и документы о полномочиях: поиск решений» была посвящена вопросам нормативного обеспечения, технологического развития и практического применения машиночитаемых доверенностей. О МЧД и других машиночитаемых юридических действиях в системе машиночитаемого права рассказала старший научный сотрудник Сектора предпринимательского и корпоративного права Института государства и права РАН Нина Соловяненко. Директор фонда «Центр инноваций и информационных технологий» Федеральной нотариальной палаты Михаил Веселов пояснил, каким образом должно быть оформлено

передование доверенности, в каком виде в машиночитаемом формате оно будет передаваться. Начальник управления ЭДО ФНС России Фёдор Новиков рассказал о том, что цикл разработки форматов электронных документов в ФНС позволяет прогнозировать, что единый для органов власти в РФ формат МЧД может быть разработан к февралю 2023 года. Президент РОСЭУ Юрий Малинин поделился новостями о формировании «дорожной карты» внедрения МЧД и результатами опроса бизнес-сообщества. Оказалось, что уже больше половины опрошенных РОСЭУ организаций готовятся к внедрению: разработали ТЗ, сформировали внутреннюю команду или даже утвердили бюджет. Координатор Некоммерческого партнёрства ECR-Rus Елена Ткаченко и руководитель управления АО «ПФ „СКБ Контур“» Наталья Никитина представили взгляд бизнеса на МЧД — совместный доклад, посвящённый актуальной теме проверки МЧД и классификатора полномочий.

ПРОДУКТОВЫЕ КЕЙСЫ

Второй день РКИ-Форума завершился сессией «РКИ: технологии, продукты, проекты, решения» — с докладами о новых продуктах, широко востребованных в отрасли, а также перспективных проектах. О сложности работы бизнеса с документами, подписанными откреплённой ЭП, рассказал генеральный директор «НТСсофт» Игорь Белоцерковский. Выступления начальника отдела разработки компонентов инфраструктуры открытых ключей «ИнфоТеКС» и управляющего партнёра ООО «Клируэй Текнолоджис» Константина Леонтьева были посвящены решениям по реализации отечественного TLS (Transport Layer Security) в условиях санкций. Особенности выполнения требований приказа ФАПСи № 152 в компаниях, использующих значительное количество СКЗИ, отметил исполнительный директор Spacebit Хияс Айдемиров. Варианты построения отечественной инфраструктуры eSIM предложил технический директор ООО «Системы практической безопасности» Сергей Александров в докладе с подзаголовком «РКИ или симметричная криптография?». Спикер

уверен, что оптимальным вариантом для отечественной инфраструктуры eSIM всё-таки является архитектура на основе РКИ. Коммерческий директор Sign Me Тимур Алексеев представил СКЗИ для мобильной электронной подписи. Финальное выступление было посвящено кейсу по реализации кадрового ЭДО на базе собственной инфраструктуры РКИ в компании Gazprom International GP. Проект представляли начальник отдела автоматизированных систем управления Информационно-управляющих систем и связи Gazprom International Егор Соколов и профессор факультета безопасности информационных технологий ИТМО Илья Лившиц.

РКИ НА ПИКЕ: НАИБОЛЕЕ ОСТРЫЕ ТЕМЫ

Третий день форума открыли участники сессии «Острые аспекты обеспечения РКИ в 2022 году, проблемы, поиск путей решения». Дмитрий Кольцов, ведущий руководитель продуктов «Астрал-Софт», поделился опытом обеспечения удалённой идентификации в коммерческих УЦ. Руководитель департамента развития услуг и продуктов АО «Инфотекс Интернет Траст» Никита Вылегжанин продолжил обзор способов идентификации в УЦ, их преимуществ и недостатков. Директор Фонда «Центр инноваций и информационных технологий» Федеральной нотариальной палаты Михаил Веселов рассказал подробнее о новых практиках применения РКИ в нотариате. Ведущий инженер компании «Газинформсервис» Екатерина Ермина представила систематизированный обзор существующих проблем при проверке цепочки сертификатов в соответствии с требованиями руководящих документов. Ведущий менеджер продуктов «ИнфоТеКС» Римма Бадмаева продемонстрировала взгляд вендора на реализацию требований 171-го приказа — использование средств ЭП класса KB2 доверенными лицами УЦ ФНС России. Советник «КриптоПро» Владимир Простов говорил о применении российских программно-аппаратных криптографических модулей (HSM) при обеспечении безопасности платёжных систем. Заместитель директора НИИ «ВОСХОД» Андрей

Пьянченко — о проекте Национального удостоверяющего центра по обеспечению TLS-сертификатов в домене доверия России. Директор по развитию бизнеса и работе с партнёрами «КриптоПро» Павел Луцук продолжил эту тематику в своём докладе о том, как обеспечить защищённый доступ к веб-сайтам и корпоративным ресурсам в условиях санкций и ухода с российского рынка иностранных поставщиков TLS-сертификатов.

ЭП ПРЕОДОЛЕВАЕТ ГРАНИЦЫ

На сессии «Трансграничное пространство доверия электронной подписи» руководитель проекта «СберКорус» к.э. н. Анна Рыбалко рассказала об экономических преимуществах, которые могут быть получены при реализации взаимного признания электронной подписи; директор Правового блока ВЭБ.РФ Александр Плахов — о мировом опыте правовых основ взаимного признания электронной подписи; заместитель начальника удостоверяющего центра Национального центра электронных услуг Республики Беларусь Дмитрий Москалев — о месте в данной правовой модели договоров между операторами ДТС; представитель Оперативно-аналитического центра при Президенте Республики Беларусь Станислав Кутузов — о существующих подходах к подтверждению эквивалентности уровней надёжности ЭП при трансграничном взаимном признании; руководитель группы технического развития ООО «УЦ ГИС» Александр Малахов — об опыте практической деятельности операторов трансграничного доверия электронной подписи.

ЭЛЕКТРОННЫЕ АРХИВЫ КАК ДОЛГИЙ ТРЕНД

Тематике длительного архивного хранения электронных документов с электронной подписью была посвящена завершающая сессия Форума. Здесь были представлены доклады ведущего эксперта по управлению документацией компании ЭОС Натальи Храмцовой «Практика и основные тенденции создания и использования электронных архивов». Согласно выводам Натальи Храмцовой, «текущий момент по развитию темы архивного



хранения электронных документов очень интересен и требует коллективной работы айтишников, юристов, архивистов... Законодательная база носит лоскутный характер... до сих пор не решена ключевая задача обеспечения сохранения правовой и юридической силы электронных документов и информации при их длительном хранении... нет концептуальных документов об этом, а мы начинаем регулировать в этом частные вопросы». В докладе заместителя директора по экспериментальным правовым режимам направления «Эффективное регулирование» АНО «Цифровая экономика» Дмитрия Соболева на тему «Законопроект об электронном архиве: текущее состояние, проблематика и перспективы» был представлен текущий этап и проблемы работы над законопроектом, уже рассмотренном Государственной думой в первом чтении, а также прозвучало, что, согласно актуальному статусу этой работы, до конца сентября 2022 г. работа над поправками будет завершена на уровне органов власти и проект будет передан в АНО «Цифровая экономика». В докладе ведущего инженера ООО «Газинформсервис» Александры Жильцовой на тему «Архивное хранение документов с ЭП, или почему пользователям не нужны пятилетние сертификаты» рассмотрено недавнее

(от 25 августа 2022 г.) поручение межведомственной рабочей группы высокого уровня по ЭДО под руководством вице-премьера Д. Н. Чернышенко о проработке вопроса по увеличению сроков действия пользовательских сертификатов до 5 лет. В докладе сделан вывод о необоснованности выбора этого единственного, неоднозначного подхода, необходимости учитывать имеющиеся технологии и сложившуюся организационную практику отечественной и мировой PKI, позволяющую решить задачу долговременного архивного хранения электронных документов на основе использования архивных форматов электронных документов с метками доверенного времени и сервисов валидации электронной подписи доверенной третьей стороны.

ПРЕМИЯ РКІ-ФОРУМА

В первый день конференции состоялось традиционное для PKI-Форума событие — вручение дипломов за выдающиеся достижения в области электронной подписи. «Проектом года» была названа технология выдачи SSL-сертификатов Национального удостоверяющего центра, стартовавшая в НИИ «Восход» в 2022 году. Победителем номинации «Удостоверяющий центр года» стал УЦ ФНС России. «Продуктом года» в 2022 году стал «Рутокен ЭЦП 3.0 NFC».

В номинации «Эксперт года» чествовали Евгения Лахаткина, сотрудника дирекции «Цифровые решения для государственного сектора» ПАО «Сбербанк». Звание «Организации года» программный комитет PKI-Форума присудил в 2022 году Академии криптографии РФ. Номинация «За вклад в развитие отрасли» в этом году была посвящена памяти Илларио Лаврентьевны Бачило (1926–2017) — советского и российского юриста, специалиста по информационному праву, доктора юридических наук, профессора, заслуженного юриста РФ.

Ещё две награды в рамках премии были приурочены к юбилею конференции. За неоценимый вклад в деятельность Форума, бережное сохранение его традиций и правил, самоотверженную работу на благо отрасли Сергею Кирюшкину вручили диплом «Хранитель традиций», а Сергею Дуднику — «Ветеран отрасли».

Конференцию «PKI-Форум Россия 2022» организовала Медиа Группа «Авангард» при поддержке Минцифры и ФСБ России, при участии ФНС России, Федерального казначейства, Банка России, Федеральной нотариальной палаты России. Официальным партнёром PKI-Форума выступила ГК «ИнфоТеКС».

МАСТЕР-КЛАСС ШКОЛЫ УПРАВЛЕНИЯ СКОЛКОВО

«НОВАЯ ПОВЕСТКА БИЗНЕСА: ОТ КИБЕРБЕЗОПАСНОСТИ
К КИБЕРУСТОЙЧИВОСТИ»

В последнюю декаду лета Школа управления Сколково анонсировала «образовательную программу по управлению кибербезопасностью бизнеса для топ-менеджеров». В комментариях к онлайн-представлению этой программы обещалось обсуждение того, «какие знания и компетенции нужны топ-менеджерам, чтобы сформировать эффективную стратегию кибербезопасности компании, организовать процессы и команду, обеспечивающие цифровую устойчивость бизнеса». Интересно, что ни в анонсе, ни в ходе мастер-класса спикеры, говоря о топ-менеджменте, не использовали устоявшийся и хорошо понятный «ибэшникам» термин «CISO». Хотя довольно часто звучал термин «уровень „топ-менеджер минус один“».

ПОМОЖЕТ ТОТ, КТО МЕШАЕТ

Похоже, в этом контексте Школа управления Сколково вкупе с компанией «РТК-Солар» намерена предложить своё решение проблемы выстраивания диалога между CISO и высшим руководством компании. Подход этот сформулирован в к/ф «Кавказская пленница»: «Тот, кто нам мешает, нам поможет!»

Действительно, сколько можно обсуждать унизительное положение CISO! Он, в дополнение к своим ИБ&ИТ компетенциям и умению руководить подчинёнными, должен и экономикой овладеть, и русский язык с ораторским искусством оттачивать, чтобы донести прописные истины до забронзовевшего капризного «бизнеса». И если этот «бизнес» желает жить в «цифре», то и фэйрволы у него должны быть Next Generation, и деньги на проверку опенсорса выделять надо, и людей в службе ИБ должно быть столько, чтобы обеспечить её работу в режиме

24×365, а не так, что «отработал ЧОП свой восьмичасовой день, закрыл объект и явился на работу следующим утром, которое начнётся, скорее всего, с разгребания завалов, накопившихся за ночь». Такое образное сравнение привёл Игорь Ляпунов, генеральный директор «РТК-Солар».

В озвученной на мастер-классе актуализированной концепции той многогранной деятельности, которая пока описывается лишь двумя стандартизованными понятиями — «Информационная безопасность» и «Защита информации», Школа управления Сколково и «РТК-Солар» предлагают возглавить управление кибербезопасностью «стейкхолдерам» и отказаться от «спихивания» ответственности за соответствующие процессы на уровень профильных руководителей — тех самых CISO.

А для организации управления кибербезопасностью по-новому топ-менеджерам для начала предлагается приобрести (на занятиях в Сколково) знания и компетенции, которые потребуются, чтобы сформировать эффективную стратегию кибербезопасности компании, организовать процессы и команду, обеспечивающие «цифровую устойчивость бизнеса» (этот набор слов, в отличие от понятий «информационная безопасность» и «защита информации», пока лишь художественный образ).

КИБЕРБЕЗОПАСНОСТЬ И ДАРВИНИЗМ

В ходе изложения этой идеи Игорь Ляпунов кратко рассказал и об эволюции концепций защиты бизнеса от угроз, исходящих из киберпространства, в которое этот самый бизнес отчасти смело, отчасти безрассудно погрузился.

На начальном этапе этой эволюции господствовал принцип «нулевого

доступа» извне — все выстраивали «цифровые крепости». Далее в какой-то момент произошёл переход от идеи изолированной «крепости» к квазиоткрытому пространству, но с развитыми возможностями выявления внутренней нелояльности и внешних посягательств. Сегодня происходит переход на тот уровень, когда кибербезопасность — это не только выявление и пресечение угроз, но и технологии и процессы «быстрого восстановления бизнеса» (и это вновь скорее художественный образ, чем стандартизованное понятие. И в контексте слова «быстрое», и с точки зрения понимания слова «восстановление»).

При взгляде «с земли» последний эволюционный переход привлекателен не только с позиции решения местечковой проблемы бесконфликтного (в контексте борьбы за ресурсы компании) встраивания «ибэшной» деятельности в общую канву бизнес-процессов. Подобные воззрения могут оказаться весьма плодотворными и для развития разных аспектов методологии того, что называют то «цифровизацией», то «цифровой трансформацией».

О ЦЕЛЯХ, НАРРАТИВАХ И ПЕРВОПРИЧИНАХ

Спикеры мастер-класса, представившие себя «ибэшниками», работающими «на земле», с иронией упоминали о существовании и потугах тех, кого называли «теоретиками ИБ». Эту иронию можно понять в суетных условиях отражения сиюминутных вызовов нынешней кибервойны, но не стоит поддерживать. Ведь история развития общества содержит ряд примеров потерь и темпа, и средств из-за нечёткости или ошибок в принципиальной постановке целей. Самый свежий из них — призрачная гонка за эффективностью инвестиций в производство и иной бизнес через



Школа управления Сколково. Фотография: skolkovo.ru

глобальное разделение труда. Сегодня она пришла к финишу, на котором дана отмашка новой гонке — за реиндустриализацию и диверсификацию экономик регионов и отдельных стран.

Отечественная «цифровизация» — это ещё одна проекция нарративов о целях общественного развития («эффективность») и приоритетах общественных интересов («интересы бизнеса»). Проекция на технологии в оболганной и на этой основе нравственно и профессионально оболванной стране.

Спикеры мастер-класса были единодушны во мнении о первопричине нынешнего непростого состояния с кибербезопасностью в России. Единодушны, но не оригинальны, ибо в мае на RNDays 11 на профильной дискуссии «Кибербезопасность для цифровой трансформации» было признано наличие ошибок в фокусах и приоритетах процессов отечественной «цифровой трансформации», признано наличие «фундаментальных проблем, которые недооценили».

АНТИКОВИДНЫЕ АНАЛОГИИ

И тут уместно вспомнить, что и мировые процессы «цифровизации» не

безупречны, что отмечалось, например, в ходе мероприятий на Киберполигоне Сбера 2021 года.

В тот год модным было рассматривать проблемы через призму медицинских «антиковидных» аналогий, и г-н Шваб, президент Всемирного экономического форума, не преминул заявить, что для комфортности и безопасности цифрового образа жизни одних «масок» недостаточно, нужна будет и «вакцинация»! И критическая информационная архитектура должна будет иметь встроенные «антитела» уже на этапе её внедрения.

СНАЧАЛА БОЛЬНО, ПОТОМ ХОРОШО

Тема о «вакцинации» ИТ и «антителах» в ней нашла продолжение на конференции киберполигона Сбера 2021 в дискуссии об устойчивости так называемых supply chains, к которой были привлечены топ-менеджеры ведущих ИТ-компаний, работающих в сфере защиты информации. Конечные выводы этой дискуссии в обобщённом виде звучали приблизительно так: «Информационным технологиям пора отдавать свои долги. Безопасность должна быть встроен-

ной. В ближайшей перспективе будет хуже, прежде чем станет лучше».

КАЧЕСТВО И ПОРЯДОК В ИТ

Природа же нынешнего «сейсмоактивного» состояния отечественного «кибербеза» лишь отчасти обуславливается чисто технологическими проблемами в контексте так называемого импортозамещения, но главной причиной является тот принцип «цифровизации» бизнеса, когда ИБ переведена в арьергард процессов «цифровой трансформации». Тогда как, по мнению генерального директора РТК-Солар, ИБ — это «качество и порядок в ИТ».

А имеет ли смысл «цифровизация» бизнеса без процессов управления качеством ИТ и качеством внедрения ИТ?

Выправить ситуацию призван помочь подход, продвигаемый Школой управления Сколково и компанией «РТК-Солар». Его суть в том, что ответственность не только за деловые и производственные процессы, но и за их безопасную «ИТзацию» возлагается на Центр — высшее руководство, которое наряду с де-юре делегированной ему компетентностью в сфере управления бизнесом должно будет овладеть де-факто и компетенциями в сфере ИБ.

BIS SUMMIT — 2022

АДАПТАЦИЯ К НОВОЙ РЕАЛЬНОСТИ КАК СЛЕДСТВИЕ ПРОВАЛОВ В ИСТОРИЧЕСКОЙ ПАМЯТИ

В IS Summit — 2022 продолжил свою традицию облекать актуальную повестку в организационно разнообразные формы. Пленарная дискуссия «Новая старая модель угроз и предстоящие изменения»; тематические треки — технологическая секция «Ландшафт и стратегия ИБ голосами практиков»; круглый стол «Технологическая независимость. Взаимодействие ИТ и ИБ»; информационно-дискуссионные секции «Прорывные технологии в ИБ» и «Цифровой след»... И последнее в этом перечне, но отнюдь не наименее важное — кулуарное неформальное общение.

Хотя в названии BIS Summit — 2022 отсутствует прямое указание на «международность» (за исключением латинского шрифта), уместно отметить интересные выступления гостей из Киргизии и Казахстана.

БЕЗ БУМАЖКИ ТЫ БУКАШКА

Ещё в ходе музыкально-информационной подводки к началу конференции обнадёживающе прозвучал призыв к стиранию барьеров между «бумажной» и «практической» ИБ. Эта тема

не только поднималась в явном виде на секции «Ландшафт и стратегия ИБ голосами практиков», но и пронизала сквозной нитью ряд комментариев «пленарки». На последней, кстати, регуляторы браво рассказали о том, что созданные в «дофевральский период» рекомендации по оценке модели угроз и типовые сценарии противодействия этим угрозам в целом оказались правильными (за исключением недооценки фактора «предательства вендора») и помогли большинству служб ИБ отразить первые атаки «постфевральского» периода.

Заместитель директора ФСТЭК также анонсировал утверждение и передачу для применения методик оценки критичности уязвимостей и тестирования обновлений (если таковые окажутся возможным получить тем или иным способом).

Виталий Лютиков также проинформировал об изменениях в требованиях к сертификации, призванных ускорить и удешевить процессы внедрения нового оборудования и продуктов. Эта новость вызвала большой интерес у аудитории, оказавшись, похоже, нежданной и неизвестной доселе даже для

модератора, который не только руководит целой «айтишной» группой компаний, но и является председателем правления одной из «айтишных» отраслевых ассоциаций.

ВОПРОСЫ ЯЗЫКОЗНАНИЯ

Год за годом конференции BIS Summit отличает не только актуальность повестки, но и креативность формулировок. В этом контексте интересно проанализировать название темы ключевой дискуссии — «Новая старая модель угроз и предстоящие изменения».

В этом наборе слов обращает внимание провокативность сочетания эпитетов «Новая старая...» и временная неопределённость определения «предстоящие». А что касается модели угроз, можно предположить, что организаторы конференции намекают на несостоятельность разговоров о чём-то новом в этих самых как бы «нынешних» угрозах.

Действительно, как раньше информация в отечественных информационных системах на базе аппаратных платформ и ПО от иностранных вендоров была под угрозой утечек, так и осталась в том же состоянии и ныне. И как раньше существовала угроза целостности и доступности информации через обновления ПО, так и сейчас эта угроза остаётся, а если и не реализуется, то благодаря «параноидальной» осматрительности руководства служб ИБ и заботам ФСТЭК (см. главу «Без бумажки ты букашка»).

Некоторую новизну можно найти лишь в вероятностях реализации упомянутых угроз, по большей части выросших.

В связи со сказанным о повышении вероятностей реализации «старых новых угроз» обескураживающе выглядит использование аморфного определения «предстоящие» по отношению к изменениям, которые должны проводиться если не с 2010, то с 2014 года точно.



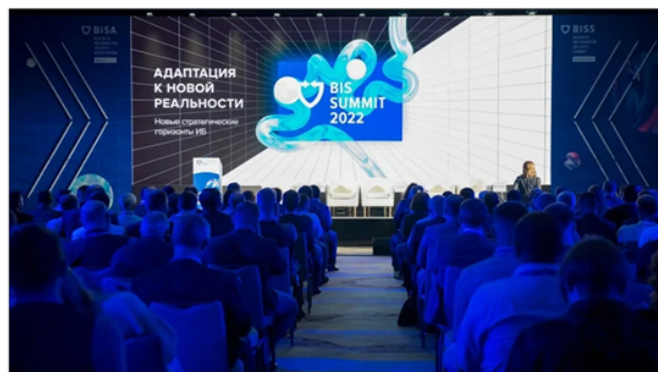


Фото: bissummit.ru

ПРОДОЛЖАЕМ ГОВОРИТЬ ПО-РУССКИ

Тема BIS Summit — 2022 — «Адаптация к новой реальности. Новые стратегические горизонты ИБ» — это ещё один повод поговорить о формулировках.

«Новые стратегические горизонты ИБ» — это как бы намёк на наличие старых стратегических предшественников у этих «новых горизонтов». Однако зачин темы «Адаптация к новой реальности» раскрывает секрет Полишинеля об этих старых и новых стратегиях. Этот секрет заключается в том, что отечественные компании, специализирующиеся на ИБ в сфере применений ИКТ, всегда лишь адаптировались к той реальности, что им задавали «сверху».

Уже в начале так называемой «усиленной пленарной дискуссии в двух частях с ключевыми регуляторами и цифровыми лидерами страны» (эта цитата анонса похожа на смешение двух реклам — санатория и театральной постановки) прозвучала мысль о том, что у экспертов «иллюзий не было никогда». Речь в этот момент шла об исходе иностранных вендоров с российского рынка, сопровождающемся недобросовестностью в отношении своих теперь уже бывших подопечных, которая в отечественных словарях обозначается термином «вредительство».

Но если «иллюзий не было никогда», то почему же владельцы многих информационных инфраструктур пытались доказать, что эти угрозы не актуальны и не реализуемы (это отметил на «пленарке» представитель ФСТЭК), а «отрасль ИБ» не соорганизовалась для проактивного реагирования на вполне вероятное развитие ситуации?

Тем более что, как отмечалось на всё той же «усиленной пленарке», в

руководстве отечественных компаний, специализирующихся на ИБ в сфере применений ИКТ, подобрались люди, которые в своей массе по своей квалификации и интеллекту превосходят средний уровень того руководства, что «подмяло» под себя работы в сфере цифровизации и цифровой трансформации в стране.

Что же до уместности применения термина «стратегия» к формированию и работе отечественного рынка средств обеспечения ИБ, то эксперты «усиленной пленарки» отметили, что нынешняя ситуация высветила готовность к работе лишь в тактической перспективе, а говорить о готовности решать стратегические задачи оснований пока нет.

КОМУ ВОЙНА, А КОМУ МАТЬ РОДНА

Коснулась пленарка и вопроса о «внезапно» обозначившемся повышении цен на российскую продукцию «отрасли ИБ». И если обывателю это повышение вполне понятно — желание «срубить бабла по-лёгкому», то вызывают недоумение попытки некоторых представителей регуляторов дать объяснение этому явлению на основе аргументации из известного анекдота: «нефть дорожает, и поэтому бензин дорожает; цена нефти стабильна, но бензин дорожает из-за инфляции; нефть дешевеет, но бензин дорожает, ведь главная цель бизнеса — рост прибыли».

А ЧТО НА МЕСТАХ?

BIS Summit — 2022, наряду с вниманием к новостям и мнениям с регуляторного уровня, традиционно предоставил место (и трибуну, и кулуары) для выступлений и дискуссий экспертов «полевого» уровня.

Круглый стол «Технологическая независимость и взаимодействие ИТ с ИБ» стал местом встречи представителей «отрасли ИБ» с вендорами российских ОС: Astra Linux, Ред Софт, Base ALT.

На секции «Прорывные технологии в ИБ» под новым соусом было подано уже начинающее набивать оскомину «блюдо» в виде «искусственного интеллекта».

Секция «Цифровой след», в отличие от прошлого года, выложила в открытый доступ некоторую толику информацию о том, что частная приватность — это в первую очередь не ИБ, а разумное увиливание от социальных сетей и прочей «цифровой трансформации» личного поведения. Но и тогда многое о вас станет известно благодаря прорехам в ИБ информационных систем госорганов и госсервисов. А возникают эти прорехи по вине программистов эпохи квалифицированного потребительства и благоприобретённого пофигизма (пароли adminadmin и 123), программистов, уповающих на лоскутный Open Source, собранный на живую нитку, и рефлекс DevOps вместо осознанного «безопасного программирования». Об этом интересно и много рассказал Олжас Сатиев, представлявший казахский Центр анализа и расследования киберпреступлений (TSARKA).

Уже упоминавшаяся секция «Ландшафт и стратегия ИБ голосами практиков» была, пожалуй, наиболее приземлённой из всех мероприятий и включила в свою повестку, помимо обсуждения стирания граней между «бумажной» и «практической ИБ», ещё и полемику вокруг таких нарративов, как «дефицит кадров» и «виртуальный CISO».

OFFZONE 2022

ПРЕДЕЛЬНО ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

ОFFZONE2022 — это в некотором смысле актуализированный релиз конференции, «продюсируемой» компанией BI.ZONE. Её «драфт» был продемонстрирован в 2018 году в интервью, которые по мысли организаторов должны были ассоциироваться с постапокалипсисом. Зампред правления Сбербанка Станислав Кузнецов отметил тогда, что подобный дизайн интересен молодым ребятам. Он же тогда признался, что «одна из задач, которая стоит перед подобного рода конференциями, — это кадровые вопросы... Несколько кадровых агентств работают на площадке и внимательно отслеживают активности и потенциальных кандидатов, которых мы, в том числе, отбираем на работу».

ЕДИНОГО КАДРА РАДИ ТЫСЯЧИ «ТОНН» ИГРОВОЙ ЕРУНДЫ

В этом году откровений об охоте за головами на OFFZONE громко не звучало, но что-то подсказывает, что ситуация не изменилась. Тем более что особое место тут занимала секция CTFFone для проведения соревнований по практической кибербезопасности.

Работали также секции HACK in 15 min (тут решались задачи по «взлому за 10 минут» с возможным продлением этого лимита до 15 минут, но с игровым штрафом) и Jock Wars (для проведения соревновательных «битв» между программами в компьютерной сети с последующим определением рейтинга игроков). ИМХО очевидно, что эти «активности» позволяют, помимо

заявленных целей, также провести ещё и первичный отбор потенциальных кандидатов для приглашения на собеседование.

БЕРЕГИ ЧЕСТЬ СМОЛОДУ

Чтобы обеспечить и упростить переход молодёжи от восприятия мира компьютерных уязвимостей в игровом формате к взрослому отношению к этой проблеме и одновременно направить эту «взрослость» не по «кривой дорожке», компания BI.ZONE представила на OFFZONE2022 платформу для проведения «цифrofизеющими» компаниями и организациями программ bug bounty.

Эксперты и разработчики BI.ZONE разработали и уже эксплуатируют своеобразный хаб для связи бизнеса и госучреждений, заинтересованных в объективном тестировании своих рабочих ИТ-инфраструктур, с независимыми исследователями уязвимостей мира ИТ — багхантерами. Анонсированная на конференции платформа позволяет запускать публичные программы bug bounty (с привлечением «неопределённого круга» исследователей уязвимостей) и программы закрытые (когда для работы приглашаются лишь избранные эксперты).

ЗОНЫ ОСОБОГО ВНИМАНИЯ

Нынешняя OFFZONE прошла в условиях «тектонических сдвигов» в отечественном кибербезе, поэтому атмосферу постапокалипсиса уже не нужно было формировать интерьерно. Да и ИТ&ИБ-молодёжь 2018 года повзрослела на 4 года и вышла на кибертектонику года 2022, пройдя ещё

и через кибершторм ковидных вызовов. Поэтому если повестка дня OFFZONE2018 наводила на мысль о проведении своеобразного коллоквиума с элементами «дня открытых дверей», то OFFZONE2022 стал богаче форматами мероприятий, а сами форматы — более насыщенными.

Открыл конференцию доклад Дмитрия Евдокимова (компания Luntry) об изменениях ландшафта информационных систем и о связанных с этим проблемах обеспечения кибербезопасности. В целом же на конференции были предложены два потока докладов «общего» назначения (основной трек и трек кратких сообщений на актуальные темы про взломы), доклады на специализированных секциях и практикумы.

В числе «секций по интересам» были организованы AppSec.Zone (для интересантов в сфере защиты приложений), Finance.Zone (для тех, кто работает или намерен заняться безопасностью финансовых систем и банковской инфраструктуры), DC&HW.Zone (для экспертов по «железу» и участников сообществ DEF CON).

Очевидной фишкой тут является культивирование внимания и интереса к «железу». Эту социальную функцию можно было ощутить сразу, при регистрации, получая комплект батареек и бейдж на основе печатной платы с работающей по определённому алгоритму светодиодной системой, а позже — посетив секцию Craft.Zone, где работают и с паяльником.

Внимание к Open Source, в отличие от интереса к «железу», не было столь акцентировано внешне. Тем не менее нельзя не отметить, что тема «открытого ПО» засветилась и на центральном треке докладов, и на AppSec.Zone, и на воркшопе, где была проведена серия практических занятий по возможностям эксплуатации ошибок ядра Linux в современных дистрибутивах этой ОС для 64-разрядной архитектуры x86.

Нынешняя OFFZONE прошла в условиях «тектонических сдвигов» в отечественном кибербезе, поэтому атмосферу постапокалипсиса уже не нужно было формировать интерьерно

ПРЫЖОК ВЕРЫ ИЛИ РОСТ НА ОСНОВЕ ЭКСПЕРТИЗЫ?

ОБ ИМПОРТОЗАМЕЩЕНИИ В ИТ НА КОНФЕРЕНЦИЯХ
GLOBAL INFORMATION SECURITY DAYS 2022
И «РОССИЙСКОЕ ПО: ВЫЗОВЫ НОВОГО ВРЕМЕНИ
И ПОИСК НОВЫХ РЕШЕНИЙ»

ТОЩИЙ СДОХНЕТ, ПОКА ТОЛСТЫЙ СОХНЕТ

Доклады на GIS Days 2022 можно считать одним из подтверждений преимуществ экономики на основе крупных корпораций. Именно наличие в Российской Федерации таких компаний, как Газпром, РЖД, Росатом, и других в этой весовой категории позволило разработать методологии замещения «зарубежных ИТ» на отечественные.

Превращению госкорпораций в центры компетенции по импортозамещению способствовали достаточные для инвестирования ресурсы, возможность и культура планирования таких инвестиций на большую глубину, а также культура технологического партнёрства, при которой в контексте ИТ не ставится вопрос о выборе между «инхаусом» и «аутсорсингом». «И то, и другое, и можно без хлеба».

В результате вокруг крупнейших корпораций с госучастием сформировался пул ИТ-компаний, которые относительно комфортно развивали свои продукты в ходе долгосрочных проектов и которые подошли к сегодняшним временам готовыми к масштабированию своих поставок.

СЕГОДНЯШНИЕ ВРЕМЕНА

Как отметили на GIS Days 2022 заместитель министра РФ А. Шойтов и сенатор А. Шейкин, профильные государственные и отраслевые структуры решили сегодня на тактическом

уровне вопросы противодействия киберугрозам и параллельно разработали стратегию исправления ошибок, накопленных в сфере ИКТ за последние несколько десятилетий. И главное сейчас — это навести надёжные мосты между мерами тактического характера и стратегическими замыслами. Очевидно, что одним из инструментов наведения таких мостов является взаимопонимание российских ИТ-вендоров и того, что принято называть «бизнесом».

Так получилось, что о том же говорили и на конференции «Российское ПО: вызовы нового времени и поиск новых решений». Там также было отмечено, что отечественное «софтверное» достигло наибольших успехов в сфере информационной и кибербезопасности, где российские решения обеспечивают импортозамещение на уровне, близком к 100%. Пусть пока и не самым эффективным путём с точки зрения цены решений.

Резюмируя вопросы, поставленные перед экспертами на этой конференции, можно собрать следующий их ключевой пул:

- ◆ Какие из российских ИТ-компаний оказались в наиболее выигрышной ситуации из-за кризиса?

- ◆ Смогли ли отечественные ИТ-компании предложить достойную замену зарубежным программным продуктам?

- ◆ Готов ли российский бизнес переходить на отечественное ПО?

- ◆ Готовы ли разработчики дорабатывать свои продукты под нужды заказчиков?

- ◆ Какую помощь может оказать и уже оказывает государство?

Хотя по первому вопросу модератор высказал некоторые собственные предположения о бенефициарах нынешней ситуации, представитель АПК ИТ на это философски заметил, что говорить о выигрышных позициях какой-либо компании в кризис, когда на кону судьба страны, не приходится.

Отвечая на вопрос о «достойной замене», эксперты предпочитали говорить о приемлемых заменах части зарубежных решений уже сегодня и о готовности создать недостающие приемлемые решения за несколько лет.

Вполне ожидаемо была отвергнута постановка вопроса о «готовности или неготовности» российского бизнеса переходить на отечественное программное обеспечение. Речь велась лишь о путях развития диалога между вендорами и заказчиками для оптимального распределения ресурсов при переходе на отечественное ПО в установленные сроки. Этот диалог также предусматривает и решение вопросов доработок продуктов под нужды заказчиков.

Единодушно эксперты конференции дали высокую оценку мерам господдержки «ИТ-отрасли», хотя и посовещались на то, что эти средства и процессы не были задействованы в начале 2000-х или хотя бы 2010-х.

BIS Journal открывает новую рубрику «ИБ + ИИ», посвящённую бурно прорастающему в нашей жизни направлению искусственного интеллекта (ИИ) в аспектах информационной безопасности (ИБ).

Конечно, можно говорить об инфернальной сущности ИИ, видеть в нём Левиафана, намерившегося пожрать человеческие души. А можно смотреть на него с рационально-утилитарной точки зрения. И куда тут денешься: проникновение ИИ в повседневную жизнь за последние годы очевидно.

Тем из нас, кто пользуется системами машинного перевода, весьма заметен существенный прогресс в его точности. Качество перевода, например, Google.Translate уже вполне сопоставимо с качеством перевода человеком — носителем языка. И видно, как это качество растёт с каждым годом.

ИИ, обученный на текстах Набокова, недавно написал новый рассказ в набоковском стиле.

ИИ может создавать рисунки, иллюстрирующие представленный ему текст.

ИИ уже пишет стихи и музыку. Правда, пока хорошо получается только рэп.

Системы ИИ могут анализировать данные с камер видеонаблюдения и распознавать различные инциденты.

ИИ управляет беспилотным транспортом.

И многое, многое другое.

Наша жизнь без ИИ вот-вот станет такой же непредставимой, как без водопровода и электричества.

А как обстоит дело с ИИ в отрасли ИБ? Для решения каких задач будут востребованы эти новые технологии?

Отдельной задачей является обеспечение безопасности собственно самих систем ИИ, анализ возможных нападений на такие системы и способов защиты от них. Важной темой является оценка достоверности систем ИИ, особенно тех, которые работают в критически важных областях. К этой теме вплотную примыкает проблематика интерпретируемости ИИ.

Открывает новую рубрику статья В.А. Окулесского, в которой обсуждаются вопросы использования ИИ в системах антифрода.

Нельзя решить проблему, находясь на том же уровне мышления, на котором она была создана. Чтобы её решить, нужно выйти на новый уровень мышления.

А. Эйнштейн

ОДНОМУ БАНКУ НЕ ПО СИЛАМ

НЕОБХОДИМ ОБМЕН ИНФОРМАЦИЕЙ С ИСПОЛЬЗОВАНИЕМ ИИ

Мошенники в сфере электронных платежей непрерывно совершенствуют свой бизнес: используют новые способы воздействия на системы банков, средства проведения платежей, применяют технологии дипфейков, глубокого психологического воздействия на клиентов и прочая, прочая, прочая... Каждый день мы обсуждаем всё новые и новые сценарии противодействия, вносим изменения в законы, ужесточаем требования к банкам, но ситуация в лучшую сторону не меняется. И есть основания полагать, что вряд ли

изменится, если подход к решению этой проблемы не будет изменён принципиально.

Сейчас для борьбы с мошенничеством практически все платёжные системы вооружены антифрод-системами, набором инструментов, с помощью которых анализируются и вычисляются подозрительные проводки денег. Это позволяет банкам останавливать и предотвращать хищения денежных средств клиентов со счетов. За одним маленьким НО. Огромное число (до 90%) мошенничеств совершается с явного согласия клиентов, т.е. формально антифрод-систе-

ма рассматривает такие платежи как легитимные.

Методика работы большинства антифрод-систем основывается на аналитике параметров платежа и параметров профиля клиента. Есть определённый набор параметров, который нам приходит «сверху», есть набор параметров, передаваемый нашими коллегами по цеху, есть наши собственные уникальные параметры. На основе этих параметров можно сформировать набор правил, который поможет принять решение — «хорошо/плохо». Но всегда остаётся серая зона (иногда до 20% платежей), в которой система не



**Василий
ОКУЛЕССКИЙ**
эксперт
информационной
безопасности,
кандидат
технических наук



Рисунок 1. Приблизительная схема одного из видов мошенничества

может принять решение без глубокой аналитики (или без хорошего аналитика): платёж ещё пока похож на настоящий, но уже имеет признаки отклонения от нормы. В центре принятия решения находится фрод-аналитик — человек, у которого перед глазами инструкция, позволяющая анализировать дополнительные признаки, и на их основе отличать одни финансовые схемы от других, то есть одни определять, как подозрительные, а другие — как не вызывающие сомнений. При небольшом потоке платежей задача вполне решаемая, но при многомиллионном потоке транзакций такая работа становится невероятно трудозатратной. В наиболее продвинутых банках на помощь приходит система машинного обучения, которая позволяет построить более сложную модель данных, чем просто использование правил, и, исходя из неё, принимать те или иные решения. Причём чем больше объём платежей и чем плотнее аналитик работает

с системой, тем больше точность работы системы.

Машинное обучение трудно назвать искусственным интеллектом. В основе здесь по-прежнему труд аналитика, который формулирует правила отсева мошеннических операций. Тут мы всё равно оглядываемся назад — проводим оценку операции на основе анализа прошлых транзакций, признанных ранее фродовыми. При этом не надо забывать, что число контролируемых параметров платежа также растёт по мере совершенствования программных и технических средств в системах ДБО и антифрода.

На самом деле реальные системы защиты от фрода должны иметь гораздо больше «слоёв» сбора и анализа различных данных. Для простоты рассмотрения глубины проблемы представим себе сильно упрощённую «модель» мошеннической операции (рис. 1).

Даже беглый взгляд на эту схему показывает, что классическая антифрод-

система в отдельном банке даже при наличии особо интеллектуальной системы анализа платежей может анализировать только один или два блока из этой схемы на транзакционных данных и данных профиля клиента. Может ли такая система пресечь социальную инженерия, когда банк получает от клиента все необходимые признаки согласия клиента на проведение платежа?

В такой мошеннической схеме для выявления проведения платежа с согласием «под давлением» в самом простом случае в число участников взаимодействия по минимуму должны входить (рис. 2):

- ♦ другие банки, на счета которых переводятся средства;
- ♦ операторы связи, которые могут иметь информацию об истории звонков клиенту и истории звонков номеров, с которых производится обзвон;
- ♦ Центральный банк, который имеет обобщённую информацию об обстановке в банковской системе;

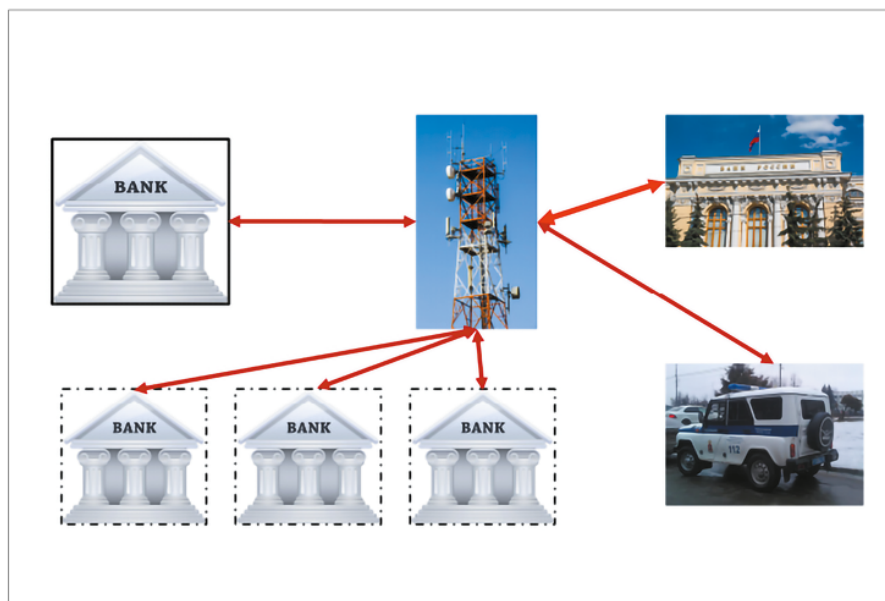


Рисунок 2. С кем обмениваться информацией

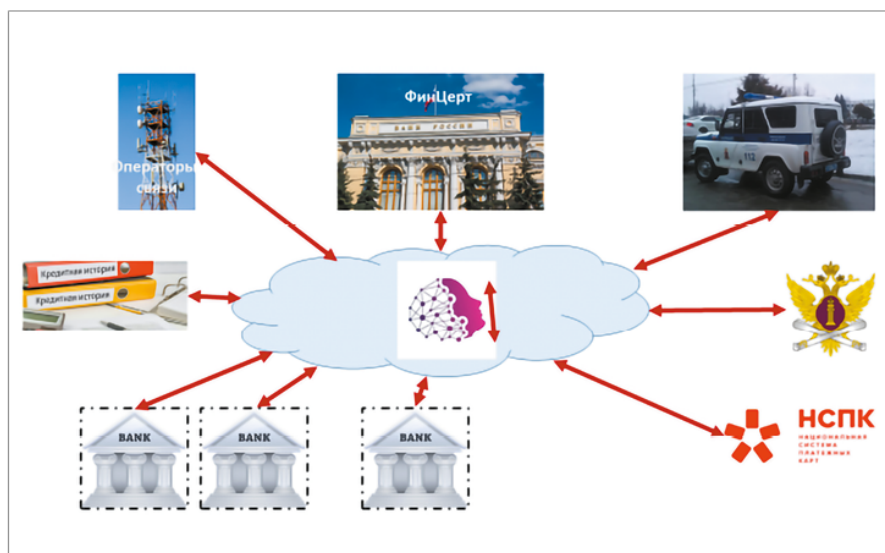


Рисунок 3. Минимальный набор участников обмена с сервисом

- ♦ Бюро кредитных историй;
- ♦ различные государственные реестры;

♦ силовые структуры — только они имеют право непосредственного «воздействия» на мошенников.

Кроме того, необходима информация из массы внешних источников для ТИ и т.д.

Становится понятным, что объём информации для обработки и принятия решения о «хорошести» платежа колоссальный, число параметров может исчисляться несколькими сотнями. Для такого информационного обмена

просто физически необходимо применять высокоинтеллектуальные высокотехнологичные системы. И здесь роль искусственного интеллекта (ИИ) просто невозможно переоценить.

Применение ИИ ставит ещё одну задачу. Стоимость реализации системы не под силу большинству банков. Кроме того, требует решения вопроса владельца такой системы, правовой основы обмена персональными данными и банковской информацией между участниками обмена.

Возможным решением могла бы стать независимая компания (не регу-

лятор), которой банки могли бы доверять. Основной деятельностью такой компании должно быть предоставление банку-участнику скоринговой оценки платежа в онлайн-режиме с учётом целого ряда параметров:

- ♦ значение параметров из списка ФинЦент и НСПК;
- ♦ данных операторов связи об истории звонков клиенту и клиента с аналитикой по клиенту и по номерам абонентов;
- ♦ данных из бюро кредитных историй;
- ♦ данных из налоговой инспекции;
- ♦ данных об истории входящих и исходящих платежей;
- ♦ данных об имуществе клиента;
- ♦ и т.д. и т.п.

Такая компания должна бы создать облачный сервис (рис. 3), имеющий взаимодействие со всеми участниками обмена. Получение информации банками возможно на основе возмездного обмена информацией. В такой конструкции банки могли бы предоставлять в это облако данные своих транзакционных и антифрод-систем. Это потребует какой-то стандартизации и унификации обмена, которыми также должны руководствоваться операторы связи, бюро кредитных историй и остальные.

Без применения ИИ создать такой сервис невозможно.

Риторический вопрос — кто или что это будет?

ПОДВОДЯ ИТОГИ

♦ Борьба с социальной инженерией можно.

♦ Создание и совершенствование собственных систем защиты информации — антифрод-систем — остаётся базовой задачей банков.

♦ Для этой борьбы необходимо объединение усилий самых разных участников на основе оперативного обмена информацией.

♦ Необходимо решить юридические проблемы законности такого обмена информацией.

♦ Организатор обмена должен иметь безусловное доверие участников взаимодействия.

♦ Построение облачного сервиса возможно только с использованием ИИ.



Павел БЫЛЕВСКИЙ
доцент Департамента
информационной безопасности
Финансового университета при
Правительстве РФ

ФУТУРОЛОГИЯ УГРОЗ БОЛЬШИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

АХИЛЛЕСОВА ПЯТА РОССИЯН НЕ ЗАЩИЩЕНА ЗАКОНОМ

Защиту обычных персональных данных Роскомнадзор курирует уже свыше полутора десятков лет, а безопасность больших данных россиян, всех вместе каждого, пока вообще целенаправленно не обеспечивается. Между тем глобальные цифровые корпорации и недружественные страны уже давно используют «большие персональные данные» наших граждан вразрез с их интересами, а не в национальных интересах России. Необходима игра на опережение, а не «креститься, когда гром грянет», как в случае с \$5 млрд штрафа Марку Цукербергу по делу Cambridge Analytica.

1 + 1 = «БОЛЬШОЙ ОДИН»

Внешний сбор и обработка в режиме 24×7 самого широкого перечня данных о каждом россиянце создают огромные преимущества для зарубежных субъектов. Начиная с оперативной детализированной статистики и аналитики по широкому перечню параметров и заканчивая высокоточным деструктивным воздействием на социальные группы.

Государственное регулирование пока касается лишь некоторых видов персональных данных и осуществляется по разрозненным, мало скоординированным направлениям. Обычные персональные данные, в большинстве своём буквенные, цифровые и буквенно-цифровые комбинации (не считая биометрической информации), защищаются под эгидой Роскомнадзора на

основании закона Ф3-152. Наказания за нарушения в этой сфере соразмерны оценке угроз: налагаемые штрафы просто мизерны, особенно для юридических лиц.

Отличие «больших» персональных данных от обычных «документационных» сведений граждан качественное, угрозы им сопутствуют намного более масштабные. В критически важный ресурс превращаются такие «новые» виды персональных данных, как пользовательская активность и «цифровые образы», формируемые без прямого участия граждан. Заслуживают внимания новые, пока недостаточно учитываемые угрозы новых видов персональных данных — пользовательской активности и автоматизированно собираемых о пользователях датчиками сетевых устройств для технологий искусственного интеллекта.

Термина «большие персональные данные» в законодательстве пока нет, но должен появиться, по убеждению автора этой статьи. Выглядит как обычное механическое приплюсовывание хорошо всем известных персональных данных к столь же распространённым big data, большим данным. Однако здесь 1 + 1 в сумме даёт не 2, а «большой один», как при слиянии капель дождя. Потому что этот вид конфиденциальной информации заслуживает выделения для его целенаправленной защиты, возможно, в ещё большей степени, чем обычные персональные данные. Об этом говорит футурология угроз «больших персональных данных» — прогноз

и предвидение, предупреждение и профилактика реализации сопутствующих им информационных уязвимостей.

ЗАЩИТА КУРАМ НА СМЕХ

Действующая в России система защиты персональных данных (ПДн) характеризуется диспропорцией значительных ресурсов и усилий, которые затрачиваются на её обеспечение, и малозначительными результатами. В данной области существует развитая нормативно-правовая база: Федеральный закон «О персональных данных» от 27 июля 2006 года № 152-ФЗ (ФЗ-152), Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (принятая ФСТЭК России в 2008 году), Приказ ФСБ РФ № 378 о шести классах СКЗИ для защиты ПДн и другие акты нормативно-правового и технического регулирования.

Защиту персональных данных в России осуществляют государство, компании — разработчики и поставщики решений в области информационной безопасности, операторы персональных данных и, конечно, их субъекты — сами граждане. Однако ответственность за нарушения в этой сфере всего лишь административная, штрафы незначительны. Максимум в 75 000 рублей штрафа выглядит не слишком суровым даже для граждан, не говоря об организациях. В таком контексте, с учётом всё большего развития и применения технологий больших данных и искусственного интеллекта,

предпринимаемые защитные меры выглядят одновременно и избыточными, и... недостаточными.

Эффективность противодействия нарушениям в сфере ПДн показывает официальная статистика уполномоченного органа федеральной исполнительной власти — Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). За 2021 год было зафиксировано 3,7 млн мошеннических телефонных звонков с неправомерным использованием персональных данных. По результатам рассмотрения 38 тыс. жалоб граждан на неправомерную обработку их ПДн составлено более 220 протоколов. В 80% из 3,9 тыс. контрольных мероприятий выявлены нарушения операторов. С сентября до конца года в Центр правовой помощи гражданам в цифровой среде обратились 450 граждан.

Насколько значительны указанные успехи, можно судить по статистике Следственного департамента МВД России. В том же 2021 году за 11 месяцев каждый седьмой россиянин становился мишенью телефонных мошенников, общий ущерб от этого вида правонарушений достиг 45 млрд рублей. Результаты противодействия Роскомнадзора и других государственных органов нарушениям в области персональных данных трудно оценить как достаточно эффективные. Анализ понятийно-терминологического аппарата в данной области показывает, что деятельность по защите рассматривается лишь в отношении достаточно узкого перечня видов ПДн.

ФЗ-152 (ч. 1 ст. 3) определяет персональные данные как «любую информацию, относящуюся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных)». В настоящее время это определение практически применяется в отношении электронных буквенно-цифровых сведений, воспроизводящих гражданско-правовые статусы и характеристики личности, традиционно фиксируемые в официальных документах. Отдельным видом ПДн обозначены фотография или видеозапись, позволяющие идентифицировать человека, а также его биометрические

данные. Некоторые виды информации, связанной с гражданином, относятся к ПДн во взаимосвязи с другими данными (номер мобильного телефона, адрес электронной почты и т.п.).

ОБНОВЛЕНИЕ КЛАССИФИКАЦИИ

Выделение защиты персональных данных в отдельное направление обеспечения информационной безопасности, включая государственное регулирование, было во многом обусловлено следованием «мировой практике», в первую очередь европейской. Наряду с положительными результатами, проявились и негативные моменты: обособление одного из видов персональных данных, а в отношении других — недооценка специфики угроз, взаимодействия и координации для обеспечения безопасности.

Несколько подвидов персональных данных защищаются другими федеральными законами, государственными органами, нарушения здесь могут подпадать под более серьёзную правовую ответственность вплоть до уголовной. Персональные данные высокопоставленных государственных служащих, сотрудников спецслужб и ряда других категорий граждан могут относиться к государственной тайне. Отдельно регулируется и осуществляется защита медицинских, финансовых сведений о гражданах, информация об их личной жизни, содержание переписки и непубличного общения посредством дистанционных сервисов и др. Защита перечисленных видов персональных данных, личной информации граждан осуществляется по отдельным самостоятельным направлениям, редко соотносясь с ФЗ-152.

Вместе с тем вне специального целенаправленного государственного регулирования пока остаются новые, всё более значимые виды персональных данных, соответствующие их общей характеристике в ФЗ-152. Это виды личной информации, которые используются в технологиях «больших данных» и «искусственного интеллекта». Речь идёт об активности пользователей в публичных сетях, в первую очередь в интернете, включая социальные сети, и о цифровых профилях граждан,

формируемых вне зависимости от их согласия и других действий.

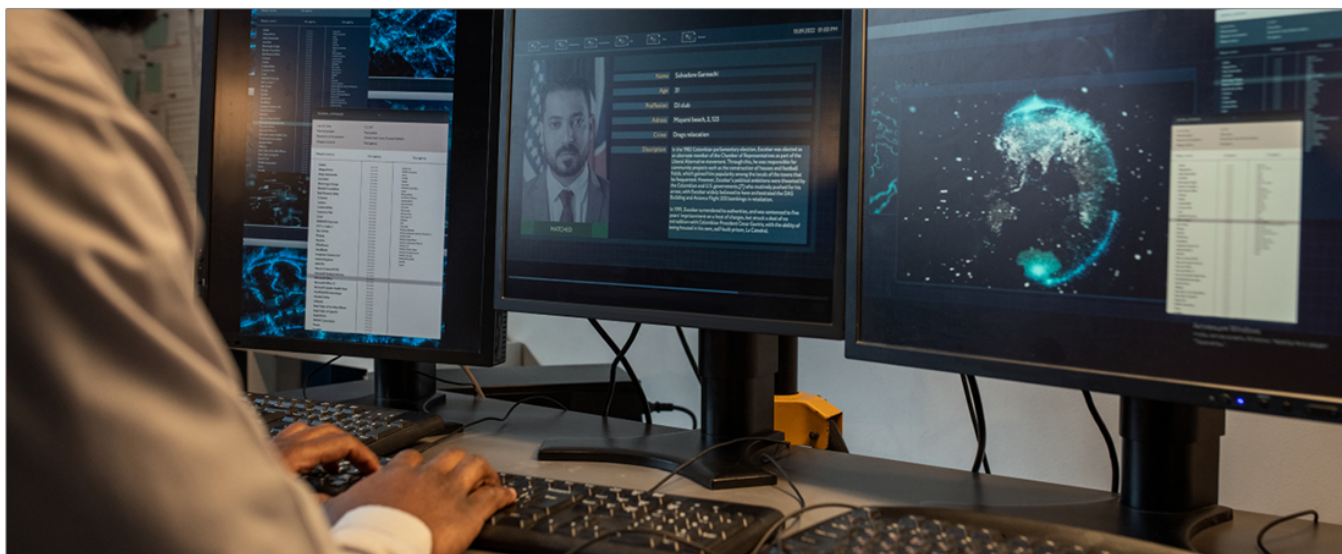
В современном мире практически для всех граждан персональные данные такого типа генерируются и собираются многими устройствами различных типов онлайн, в постоянном режиме «24×7» (24 часа в сутки семь дней в неделю). Данные о пользовательской активности владельцев персональных настольных компьютеров и мобильных устройств (гаджетов), казалось бы, чисто технические. Однако они включают индивидуальные параметры использования этих программно-аппаратных средств и операционных систем и другого программного обеспечения.

ПРОГНОЗ УГРОЗ

Персонализированы могут быть cookie, IP-адреса, посещённые веб-ресурсы и использованные мобильные приложения, продолжительность просмотра и данные о других действиях пользователей. Такие персональные пользовательские данные собирают и обрабатывают глобальные информационные платформы, а также другие дистанционные сервисы. Большие персональные данные (big personal data) могут как использоваться их сборщиками для оптимизации сервисов, так и продаваться.

Важный подвид больших персональных данных составляют сведения о пользовательской активности в социальных сетях и на других информационных платформах (торговых, развлекательных и т.п.). Это не только собственно персональные данные (в обычном узком смысле) владельцев аккаунтов, но и сведения об их социальных связях — наличии «френдов» и членстве в группах и сообществах, о просмотрах и времени пребывания на других ресурсах, о совершаемых действиях: постах (авторских публикациях), оценках, комментариях и т.п. Эти большие персональные данные — та самая «новая нефть» для владельцев глобальных информационных платформ, средство совершенствования собственных сервисов и товар для продажи.

Ещё более значительный по разнообразию параметров и всеохватности вид больших персональных данных — следы, которые оставляет в современной цифровой социальной среде почти



каждый гражданин. Разнообразные программно-аппаратные устройства и сетевые решения наполняют производство, досуг и быт, автомагистрали и улицы, места отдыха и т.д. Данные о гражданах вне зависимости от их участия и согласия собираются посредством видеокamer на искусственных спутниках Земли и в публичных местах, включая парковки автомобилей, датчиков экологического состояния окружающей среды, терминалов дистанционной оплаты, бытовой умной техники и т.п. История местоположений, привязанная ко времени, определяется данными регистрации в системах сотовой связи SIM-карты мобильного телефона.

Большие персональные данные позволяют моделировать цифровых двойников практически любого человека, автоматизировать аналитику предпочтений и совершенствовать методы влияния на поведение, личность в целом и социальные группы разных масштабов. Международное и национальное государственное правовое сознание отстаёт от стремительных темпов возрастания роли больших персональных данных и сопутствующих угроз, способных приобретать критический характер.

ПОКАЯНИЕ ЦУКЕРБЕРГА

Отсутствие удовлетворительного нормативно-правового регулирования этих персональных данных предоставляет простор произволу и возможным злоупотреблениям со стороны их

операторов — транснациональных корпораций, глобальных информационных платформ. Признавая проблему, недостаточно сводить её к «сохранению конфиденциальности» и искать решение исключительно среди технических средств, пусть даже методом глубокого обучения.

Законодательное регулирование защиты «больших персональных данных» не в интересах глобальных информационных платформ, поскольку ограничивает и ставит под контроль государства их возможности. Значительные потенциальные угрозы попадают в публичное поле тогда, когда наносят ущерб тем, кто привык бесконтрольно манипулировать этим видом персональных данных в своих корпоративных интересах. О чём свидетельствует дело о сотрудничестве Facebook с компанией Cambridge Analytica в 2014–2017 годах, из-за которого Марку Цукербергу (пока ещё не запрещённому в РФ) пришлось давать показания в конгрессе США и Европарламенте, а также выплатить рекордные \$5 млрд штрафа.

Были вскрыты неожиданные уязвимости традиционной практики прибыльной торговли «большими персональными данными» пользователей, включая допуск партнёров к непосредственному сбору. Работавшая в партнёрстве с Facebook компания Cambridge Analytica на основании изучения политических предпочтений пользователей оказала воздействие на победу Дональда Трампа на

выборах Президента США и на результаты Brexit — референдума о выходе Великобритании из Европейского союза. Учитывая негативные последствия, Марк Цукерберг обязался впредь более тщательно относиться к партнёрству Facebook в области больших персональных данных.

Для транснациональных корпораций главное — собственная безопасность и прибыли, а национальное регулирование не является необходимым руководящим фактором, с ним просто приходится считаться. В России проблема защиты больших персональных данных (пользовательской активности и прочих данных о пользователях) пока чётко не сформулирована. Защита российских граждан от злоупотреблений зарубежными субъектами в этой сфере носит фрагментарный и косвенный характер.

Результаты выступают побочными следствиями противодействия зарубежным санкциям, обеспечения цифрового суверенитета, локализации информационной инфраструктуры и достижения независимости от импорта высоких технологий. Целенаправленная формулировка задачи, разработка и осуществление мер защиты больших персональных данных российских граждан является практической футурологией близкого будущего.



Андрей ЖАРКЕВИЧ
редактор
ООО «Антифишинг»

ПОБЕДИТЬ НЕЛЬЗЯ ЗАЩИТИТЬ

ПОНИМАНИЕ ЗАКОНОВ ПСИХИКИ
ЗАСТАВЛЯЕТ ВНОСИТЬ КОРРЕКЦИЮ
В МЕТОДЫ БОРЬБЫ С СОЦИНЖЕНЕРИЕЙ

Непримируемое сражение с мошенниками незаметно превращается в борьбу с обычными людьми, с теми самыми потенциальными жертвами — доверчивыми, сомневающимися, готовыми помочь. Даже бывалые борцы с фишингом в определённой жизненной ситуации могут пострадать, потому что не в состоянии победить самих себя. У каждого найдётся слабость, за которую могут зацепиться мастера социальной инженерии в ходе разработки сценария очередной цифровой атаки.

В этой статье мы разберём особенности человеческой психики, которые во многом превращают борьбу с фишингом и мошенниками в фарс, а затем попробуем сформулировать меры противодействия, которые действительно будут работать на широкой аудитории.

МОЗГ-ОБМАНЩИК

Первая причина, по которой люди настолько уязвимы к профессионально подготовленным мошенническим схемам, состоит в том, что мозг часто обманывает нас. Когда мы попадаем в критические ситуации или оказываемся в непредвиденных обстоятельствах, мозг стремится выдать ответ «на скорую руку», поскольку на поиск идеального решения нет времени. Ему приходится искать кратчайшие пути и довольствоваться допущениями.

В этом нет ничего криминального: такой обман в большинстве случаев вполне допустим и

даже полезен, но это также ведёт к вполне предсказуемым ошибкам. Например, мы воспринимаем огромное количество информации, но быстро её забываем, потому что мозг отбрасывает большую часть данных, как только решает, что они не нужны.

Помимо отбрасывания лишней информации, мозгу также приходится решать, стоит ли делать выводы «по-быстрому». Решение он принимает, отталкиваясь от того, что важнее в конкретной ситуации: скорость или точность. Разумеется, в большинстве случаев мозг выбирает скорость, опираясь на сформированные в ходе эволюции эмпирические правила, которые далеко не всегда подчиняются законам логики.

Представим, к примеру, ситуацию, когда сотрудник получает фишинговое письмо с напоминанием сменить пароль для входа в сеть. Если письмо выглядит как привычные системные уведомления, никаких сомнений в его подлинности, скорее всего, не возникнет.

Поскольку логическое или рациональное мышление требует больших усилий, мозг выбирает более простой в реализации интуитивный ответ, поскольку знает, что в большинстве случаев такого ответа вполне достаточно. Даже если он ошибочен.

Таким образом, мозг весьма избирательно обрабатывает информацию из окружающего мира, выбирая ту, которая, по его мнению, наиболее важна для выживания, и в связи с этим уделяя особое внимание неожиданным событиям. При этом мозг редко говорит нам правду, сообщая лишь то, что, по его мнению, нам необходимо знать.

ПРИНЯТИЕ РЕШЕНИЙ — ПУТЬ НАИМЕНЬШЕГО СОПРОТИВЛЕНИЯ

Вторая причина уязвимости человеческой психики — особенности работы системы

Даже бывалые борцы с фишингом
в определённой жизненной ситуации
могут пострадать, потому что
не в состоянии победить самих себя

самоконтроля и принятия решений. Система самоконтроля сформировалась в человеческом мозге постепенно, дополнив древнюю систему желаний и инстинктов.

Эволюция сохранила нам все инстинкты, которые когда-либо приносили пользу, но в современном мире некоторые из них могут создавать проблемы. Один из таких инстинктов — «бей или беги». Его смысл в том, что, когда мозг перегружен, мы принимаем решения, руководствуясь импульсами, а не долгосрочными целями или рациональными рассуждениями.

Вот что происходит на физиологическом уровне, когда мы видим угрозу. Информация от глаз передаётся в зону мозга, которая называется миндалевидным телом и действует как система оповещения о тревоге. Она находится в глубине мозга и распознаёт возможные опасности. В момент угрозы такое расположение помогает ей быстро связываться с другими участками мозга и тела.

Получив информацию от сетчатки, на которой фиксируется опасность, система оповещения посылает серию сигналов в мозг и тело, запуская реакцию «бей или беги». Надпочечники выделяют гормоны стресса. Из печени в кровоток подаётся энергия в виде жиров и сахаров. Дыхательная система активизирует работу лёгких, чтобы дать организму больше кислорода. Кровеносная система работает на полную мощность, чтобы энергия из кровотока поступала в мышцы, которые и отвечают за бегство или борьбу.

Пока тело готовится защищать жизнь, в мозге система оповещения о тревоге старается, чтобы наш рассудок не помешал телу. Она привлекает наше внимание к опасности и внешней среде, чтобы не возникало посторонних мыслей, которые отвлекли бы от близкой угрозы. Параллельно система оповещения запускает сложные реакции в мозге для подавления префронтальной коры, отвечающей за контроль над импульсами. В режиме «бей или беги» организм переключается в импульсивный режим. Рассудительная и рациональная префронтальная кора засыпает, чтобы мы не труслили перед боем или не передумали бежать.

Реакция «бей или беги» спасала людей в течение миллионов лет эволюции, бросая все силы на то, чтобы спасти нас в случае опасности. Однако это значит, что все процессы в организме, не направленные на выживание, функционируют «на минималках». Нам просто не дают потратить ни капли физической или душевной энергии на то, что не поможет выжить.

Теперь в свете сказанного попробуем представить сотрудника, получившего письмо с

уведомлением о компрометации пароля и требовании немедленно сменить его в течение 15 минут под угрозой увольнения. Обострим ситуацию: допустим, что у этого сотрудника жена в декрете, кредит на машину и ипотека. С большой вероятностью угроза увольнения станет тем самым угрожающим фактором, который вызовет реакцию «бей или беги», а значит, подавит рациональную часть мозга и активизирует импульсивные реакции.

ХРУПКИЙ САМОКОНТРОЛЬ

Третьим фактором, который затрудняет борьбу с мошенниками, является, как это ни удивительно, ещё одна инстинктивная реакция, которую можно назвать «остановись и подумай».

Главная задача этой системы — сдерживать нас от совершения поступков, которые могут нам навредить на рациональном уровне. Именно эта система сдерживает нас, когда мы готовы нагругить начальнику, напоминает о неуплаченных налогах и просроченных платежах по кредиту. Мозг распознаёт подобные угрозы, и префронтальная кора активизируется, чтобы помочь сделать правильный выбор. Но реакция «остановись и подумай» не отправляет энергию в мышцы. Её цель — мозг, а точнее, префронтальная кора, которая включает самоконтроль.

Ответ «остановись и подумай» далеко не всегда ощущается столь же инстинктивным, как реакция на опасность. Причина в том, что самоконтроль ослабляется из-за недосыпа, неправильного питания, недостаточной физической активности и множества других факторов.

Так, если сахар в крови упадёт, мозг получит сигнал об опасности, снизит уровень самоконтроля и перейдёт в режим краткосрочного планирования и импульсивного поведения, примерно как в известной рекламе «ты не ты, когда голоден». Мозг будет искать способы поесть, а не раздумывать над далёкими стратегическими целями. Именно поэтому перед обедом биржевые трейдеры могут неожиданно для себя вложиться в безнадёжные акции, люди на диете покупают лотерейными билетами и берут ненужные кредиты, а забывшие позавтракать руководители отправляют свой пароль мошенникам.

УДИВИТЕЛЬНЫЙ КОНТЕКСТ ИЛИ ПАРАДОКС СТАРШЕГО ПОКОЛЕНИЯ

Недавнее исследование ВТБ показало, что люди старшего поколения (55+) более устойчивы к фишингу, чем более технически продвинутые люди в возрасте от 35 до 50. Они реже переходят по вредоносным ссылкам, реже нажимают

на кнопки и практически никогда не передают свои логины и пароли преступникам.

Причина такого, на первый взгляд, парадоксального явления в том, что люди 55+ привыкли к живому общению. Электронные уведомления не являются привычным элементом их жизни, поэтому либо игнорируются, либо становятся событием и поводом для обсуждения с кем-то, кто понимает. Фишинговые письма и сообщения просто находятся вне привычного для этой категории людей контекста, создавая видимость особой устойчивости.

Важность контекста объясняется уже рассмотренными выше режимами работы мозга. Находясь в рациональном режиме, например, размышляя на рабочем месте, люди с лёгкостью распознают уловки мошенников, не верят телефонным аферистам и с удивлением читают новости об очередном мошенническом инциденте, отмечая про себя, что они-то точно на такую ерунду не повелись бы. Но в другом контексте, например во время решения серьёзных проблем, те же самые люди совершают необдуманные поступки — вводят данные банковской карты на сайте мошенников или сообщают пароль от корпоративной сети на вредоносном ресурсе.

НРАВСТВЕННАЯ ПОБЛАЖКА

Ещё одна особенность психики, которая, пусть и косвенным образом, но помогает мошенникам обманывать людей, — эффект нравственной поблажки. Смысл этого эффекта состоит в том, что человек, совершивший какое-то правильное действие, настолько доволен собой, что позволяет себе совершить что-то неправильное, отпуская контроль.

Типичный пример: девушка на диете после двухчасовой тренировки на беговой дорожке идёт в кафе и заказывает пирожное. Она доказала себе, что она молодец, разве она не заслужила маленького послабления?

Представим теперь сотрудника компании, который только что прошёл курс по информационной безопасности или прочитал памятку о безопасной работе с почтой от отдела ИБ. Потратив время на безопасность, он чувствует себя молодцом и позволяет себе перейти по ссылке в письме или открыть вложенный в письмо документ. Конечно, он знает, что это может привести к проблемам, он же только что прошёл курс. Но ещё он помнит, что он молодец, а значит, с ним ничего такого произойти не может.

Худшее в нравственных поблажках — не их сомнительная логика, а то, что они обманом вовлекают в совершение вредных или даже опасных действий. Они убеждают, что любое

отступление от правильного поведения — диеты, бюджета, правил работы с почтой — это поощрение, которого мы заслужили.

А КАК ЖЕ РЕКОМЕНДАЦИИ И ОБУЧЕНИЕ?

Реальная эффективность информирования и рекомендаций примерно такая же, как в случае с правильным питанием и регулярной физкультурой. Все знают, что это полезно, но крайне мало людей последовательно выполняют эти рекомендации и тем более превращают их в образ жизни.

По данным исследований «Антифишинга», через год после прохождения обучающих курсов без практических тренировок всего 9% сотрудников ведут себя безопасно. Но несмотря на это, заблуждение о том, что путём информирования можно научить людей противостоять фишингу и телефонным мошенникам, демонстрирует неожиданную популярность на всех этапах власти.

Возможно, такая популярность информирования объясняется простотой реализации и возможностью наглядно продемонстрировать выполненное: «Вот мы сделали сайт, сняли ролик, напечатали плакат и листовку, теперь фишинг не пройдёт, а про мошенников можно забыть...»

К сожалению, реальность далека от оптимистичных отчётов сторонников массированного информационного наступления на злоумышленников. В некоторых случаях мошенники используют растиражированные правила безопасного поведения в своих сценариях. Например, в одной из компаний телефонные аферисты предлагали жертве не называть код голосом, поскольку это небезопасно, а ввести его в режиме тонального набора на клавиатуре телефона. Результат тот же — защитный код попал к преступникам, но с точки зрения жертвы всё нормально, ведь она же никому ничего не сказала.

ЧТО ДЕЙСТВИТЕЛЬНО ПОМОЖЕТ?

Эффективность мошеннических сценариев напрямую зависит от того, насколько изучена целевая аудитория, в адрес которой отправляются фишинговые сообщения или поступают телефонные звонки. Знание организационной структуры, бизнес-процессов и традиций организации позволяет разработать практически безотказные варианты воздействия на сотрудников. Аналогичным образом в случае с физическими лицами наличие информации о счетах, остатках, картах и других персональных сведений позволяет агрессивно манипулировать жертвой, принуждая её к нужным преступникам действиям.

Таким образом, важнейшей мерой для защиты граждан и организаций от мошеннических



атак должна стать борьба с утечками на государственном уровне. Нужно максимально затруднить доступ преступников к конфиденциальным данным.

Ужесточить ответственность за утечки персональных данных ранее предлагал глава Минцифры Максут Шадаев. По его мнению, дополнительная ответственность в виде оборотных штрафов должна побудить бизнес инвестировать в развитие инфраструктуры информационной безопасности и защиту персональных данных пользователей.

Свой вклад в борьбу с мошенниками должны внести и социальные сети. Сейчас социальные платформы представляют собой отличное место для проведения информационной разведки (Open Source INTelligence, OSINT). Причина этого состоит в максимальной открытости настроек пользовательских профилей по умолчанию. Простое изменение настроек профилей в соцсетях на приватные по умолчанию может стать ещё одним шагом к защите от мошенников.

Критически важным фактором повышения уровня безопасности людей является тренировка навыков. Как мы уже говорили в предыдущих публикациях, никакие лекции, видеоролики и плакаты не дают долговременного эффекта.

Наглядная агитация с третьего раза превращается в белый шум, который уже не воспринимается сознанием.

Чтобы победить реакцию «бей или беги», нужна тренировка навыков в условиях, максимально приближенных к реальным. С учётом влияния контекста такие тренировки должны проводиться в случайные моменты времени, поскольку человек, находящийся в рациональном режиме, успешно пройдёт тренировку, но не получит закрепления навыка.

Ещё один навык, который поможет противостоять мошенникам, — это развитие самоконтроля, той самой реакции «остановись и подумай». Добиться этого можно путём длительной фиксации внимания на каком-то несложном повторяющемся в течение дня действии. Например, для правши можно открывать двери или чистить зубы левой рукой.

Несмотря на кажущуюся бессмысленность, эти относительно простые действия вырабатывают у людей привычку осознанно следить за тем, что они делают, и выбирать то, что правильнее (хотя иногда и труднее), а не то, что легче. Прокачанный с помощью такого упражнения самоконтроль в итоге позволит в критической ситуации выбрать рациональный, а не импульсивный вариант поведения.

**Михаил ЛЕВАШОВ**кандидат физико-математических наук,
старший научный сотрудник

- Звонок в бухгалтерию:
- Вышлите мне, пожалуйста, расчётный листок.
 - Приезжайте и получите.
 - А можете выслать на корпоративный email?
 - Не могу. Это персональные данные.
 - Но это же мои данные, и я разрешаю вам их выслать мне на мою корпоративную почту.
 - Нам запретили. Обращайтесь к ректору...

БЛЕСК И НИЩЕТА ИБ-ОБРАЗОВАНИЯ

РОССЫПЬ ПРОБЛЕМ ГЛАЗАМИ ПРЕПОДАВАТЕЛЯ ВУЗА

Сейчас специалистов по информационной безопасности готовят во многих российских вузах. Это стало модно и престижно, в том числе и потому, что в эпоху цифровизации и цифровой трансформации защита информации в бизнес- и других процессах стала важнейшим условием успешной деятельности.

О достижениях ИБ-образования нам периодически докладывают министерские и вузовские чиновники, этим вопросам посвящены различные публикации. Например, в BIS Journal в статье А. Курило¹ отмечаются реальные достижения Минтруда, Минобрнауки и других ведомств в части подготовки ФГОС, профессиональных стандартов, различных рекомендаций, выполнение которых контролируется министерскими кураторами, департаментами образования и вузовскими чиновниками. Действительно, в этой части реализуется большой объём работ. Вместе с тем остаётся и множится значительное количество проблем, которые либо не решаются в принципе, либо решаются робко и непоследовательно.

Эти многочисленные вопросы образовательного процесса вообще и процесса подготовки специалистов по ИБ в частности оказывают заметное влияние на качество специалистов,

востребованных на рынке. Часть проблем давно известна, их даже пытаются решать, а часть можно определить как либо новые, либо глубинно скрытые. Попробуем для начала их обозначить.

СРАВНЕНИЕ С МЕДИЦИНОЙ

Информационная безопасность объединяет в себе много научных, технических, юридических, психологических, социальных и других направлений исследований и относится практически к каждому физическому и юридическому лицу, а также любым другим формам объединения людей, пользующихся компьютерами. По области охвата, значимости и разноплановости ИБ сегодня сродни медицине¹, у которой, на минуточку, имеется собственная Академия наук и своя разветвлённая система подготовки специалистов и обмена опытом. Думается, что ИБ также заслуживает особого к себе отношения в части обеспечения, включая и обеспечение кадрами.

НАЧНЁМ С БУХГАЛТЕРИИ

Так что же нас беспокоит в вузовской ИБ? В эпиграфе к статье представлен типичный, взятый из жизни диалог между преподавателем и работником бухгалтерии. Он, собственно, и показывает местоположение ИБ в общественном сознании. Из диалога следует, что квалифицированный работник вуза (бухгалтер) не знает (не понимает) азов ИБ, связанных с понятием

«персональные данные» и их защитой. Он даже не представляет себе, что субъект персональных данных может делать с этими своими данными всё, что ему угодно (конечно, в рамках Закона). Поэтому и отказывается выслать ПД преподавателя, касающиеся его заработной платы, по его личной просьбе! То есть по запросу самого субъекта эти данных.

Хотя возможна и другая субъективная причина, а именно весьма незначительная зарплата, указанная в расчётном листке...

ПРО ТЕРМИНЫ

В серии образовательных стандартов, как федеральных, так и вузовских, периодически меняются термины, обозначающие результаты, которые должен получить студент по завершении обучения. Это и знания, и компетенции, и умения, и навыки, и взятые из иностранных документов дескрипторы и индикаторы. Эти нововведения не внесли ничего нового в образовательный процесс, зато само по себе переписывание стандартов обеспечило занятость армии специалистов по учебно-методической работе на всех уровнях образовательной бюрократии.

ПРО МЕТОДИКИ

Ничуть не преуменьшая важности методической работы, замечу, что легла эта нагрузка в значительной мере на плечи преподавателей. Не обладая знаниями в

¹ А. Курило. «Куда идти? Три первых шага». BIS Journal, 2022, № 1.

предметной области, специалисты-методологи оказались не в состоянии самостоятельно создавать необходимые методики. Казалось бы, вот оно — плодотворное сотрудничество, синергия! Но сотрудничество это оказалось с каким-то дискриминационным оттенком: преподаватели разделяют с методологами их работу (по сути, работают за них) без какой-либо компенсации.

ПРО «НАВЫКИ»

Ещё несколько слов о терминах. Речь о «навыках», вырабатываемых у студентов за время обучения. Некоторые преподаватели трактуют этот термин по «Википедии»: «способность деятельности, сформированная путём повторения и доведённая до автоматизма». В таком понимании термин явно не подходит для выпускников вуза, тут речь идёт скорее о работниках конвейера. Но если слова «доведение до автоматизма» заменить на «приобретение опыта каких-либо работ», то в таком случае термин «навыки» вполне применим.

О НАУЧНОЙ ДЕЯТЕЛЬНОСТИ

Следующий аспект связан с научной деятельностью профессорско-преподавательского состава (далее — ППС). Тут явно смешиваются два разных понятия. Преподаватель и исследователь — разные профессии. Научные, практические и другие исследования проводятся в академических и отраслевых институтах и организациях, а преподавание — в учебных заведениях. Но ситуация складывается парадоксальным образом: преподаватели не вовлечены в исследовательские процессы, фактически дискриминированы с точки зрения работы и оплаты труда. Им не всегда продлевают контракты, и они каждый год вынуждены бороться за своё рабочее место и небольшую зарплату.

О ПУБЛИКАЦИЯХ

В сфере ИБ очень мало специализированных журналов. Поэтому многие ППС вынуждены публиковаться в других, не тематических, изданиях, где их труды не достигают целевой аудитории и не могут быть адекватно оценены. При этом перечень журналов, рекомендованных вузами для публикаций по тематике ИБ, весьма ограничен, а хорошо известные

Сплочённая вузовская «тусовка», возможно, ни разу в жизни не работавшая «на земле», ревниво следит за чистотой своих академических рядов и даёт практикам очень мало шансов на продвижение на ниве преподавания

отраслевые тематические журналы (тот же BIS Journal) не учитываются в публикационной активности преподавателей. И это при том что большинство известных в отрасли ИБ специалистов публикуется именно в этих, не входящих в перечень, отраслевых журналах, и именно через них идёт идейное формирование основных направлений развития отрасли. В результате вузы живут своей жизнью, в значительной степени оторванной от реальной жизни и процессов, идущих в отрасли.

О СПЕЦИАЛИСТАХ-ПРАКТИКАХ

Единственная нить, связывающая эти два мира (вузы и отрасль), — это опытные специалисты-практики, которые без отрыва от основной деятельности преподают по совместительству в вузах. Однако таких преподавателей любят только на словах. Их важнейший труд оценивается весьма скромно. Сплочённая вузовская «тусовка», возможно, ни разу в жизни не работавшая «на земле», ревниво следит за чистотой своих академических рядов и даёт практикам очень мало шансов на продвижение на ниве преподавания. Основные «печеньки» в виде госзаказов на исследования с дальнейшей публикацией в «хороших» журналах чужакам практически не достаются.

Такое положение вещей противоречит разумным рекомендациям, связанным с привлечением в учебный процесс специалистов-практиков, имеющих опыт реальной ИБ.

О ФОРУМАХ И КОНФЕРЕНЦИЯХ

С обозначенной выше темой связан вопрос участия ППС в многочисленных тематических форумах и конференциях, где принимают участие специалисты-практики и озвучиваются самые

последние вызовы и достижения в области ИБ. Вузовские работники, преподаватели и учёные мало вовлечены в эти мероприятия. Да их там не очень-то и ждут, так как они, во-первых, как правило, не могут оплатить участие в этих форумах, а во-вторых, не приносят с собой каких-либо прорывных идей. Связь между вузами и этими форумами весьма призрачна.

О СТАЖИРОВКАХ

Важными представляются и вопросы повышения квалификации ППС путём делегирования их в компании, специализирующиеся на информационной безопасности. Эта тема неоднократно обсуждалась, но эффективного решения до сих пор не найдено. Организуемые стажировки преподавателей в таких компаниях, как правило, эпизодичны и краткосрочны.

ПРО АДМИНИСТРАЦИЮ ВУЗА

Важным аспектом является и отношение к ППС со стороны администрации вузов. Срочные трудовые договоры, заключаемые вузами с ППС, не дают последним уверенности в завтрашнем дне. Необходимо полностью изменить эту систему и сделать эти договоры бессрочными — такими же, как и у административного персонала. Только в этом случае ППС перестанут быть в вузе работниками второго сорта с соответствующим к ним отношением. Ярким примером такого отношения является распространённая практика заключения договора на срок до 30 июня (то есть до отпуска — июля и августа), видимо, чтобы не переплачивать. Это, конечно, унижительная практика. В этом направлении уже проводятся определённые действия по законодательному установлению минимального срока трудового договора с ППС. Однако результаты пока неочевидны.



Василий ОКУЛЕССКИЙ
эксперт ИБ,
кандидат
технических наук

СМЕЩЕНИЕ АКЦЕНТОВ

АЛЬТЕРНАТИВОЙ ВЫСШЕЙ ШКОЛЕ
В СФЕРЕ ИБ МОЖЕТ СТАТЬ СРЕДНЕЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАНИЕ.
ЧТО ДЛЯ ЭТОГО НУЖНО?

Дефицит специалистов ИБ — это, наверное, самая набившая оскомину тема. И вроде делается в этом направлении много, и вузов, которые готовят таких специалистов, не счесть, а проблема менее острой не становится. Так, может, проблема не в количестве вузов и даже не в их программах обучения?

ПЛЯСАТЬ ОТ ПЕЧКИ

Давайте зададимся простым вопросом: кто они, самые востребованные рынком специалисты? На первый взгляд, ответ вроде бы очевиден: существуют стандарты специальностей в некоторых предметных областях, формулируются

портреты выпускников, существуют пожелания заказчиков. Но если в вузовских документах логика образования ещё прослеживается, то в типичных требованиях, в том числе и нормативных, звучит примерно такое: «*Высшее техническое образование в области ИТ или ИБ, опыт работы в области ИБ такой-то, а для руководителей такой-то*». Уловка-22 состоит в том, что на должность даже просто специалиста можно взять только человека, имеющего опыт работы, то есть не выпускника вуза. Откуда в таком случае такие специалисты берутся изначально?

Мой достаточно продолжительный опыт руководства разными

подразделениями ИБ позволяет классифицировать эти источники на житейском уровне.

Во-первых, небольшие организации ищут, как правило, «универсальных» специалистов и наименее требовательны к наличию первичного опыта. Это и есть своего рода инкубаторы будущих настоящих ибэшников.

Во-вторых, в средних и крупных организациях уже важна специализация по разным направлениям ИБ, но, главное, тут нужны те, кто знает, ЗАЧЕМ нужно что-то делать, ЧТО нужно делать, и те, кто не только знает, но и умеет, КАК делать. Очевидно, первую и вторую категорию (ЗАЧЕМ и ЧТО



Андрей КУРИЛО
кандидат
технических наук,
доцент

BIS-КОММЕНТАРИЙ

ОПТИМАЛЬНЫЙ ПУТЬ — ОБЛАЧНАЯ ПЛАТФОРМА

НЕОБХОДИМО СКОНЦЕНТРИРОВАТЬ
НЕМАЛЫЕ ВЫДЕЛЯЕМЫЕ,
НО РАСПЫЛЯЕМЫЕ СЕЙЧАС ФИНАНСОВЫЕ
СРЕДСТВА В ОДНУ ТОЧКУ

Хочу поблагодарить автора за то, что он снова взялся за проблему подготовки специалистов в области информационной безопасности. Да, вполне закономерно возникает вопрос о стратегическом пути обучения новых кадров: высшие учебные заведения это будут,

средние или курсы повышения квалификации и переподготовки? Но это тема отдельного, очень простого анализа и последующего разговора. Наверное, вопрос есть, если «Яндекс», посмотрев на то, что происходит, стал готовить безопасников из своих курьеров.

Но в данном случае автор поднял, на мой взгляд, другую важнейшую проблему — общую как для вузов, так и для колледжей. Это проблема отсутствия в учебных заведениях:

♦ современной учебно-материальной базы, позволяющей обучать студентов всему спектру средств защиты;

нужно делать) готовят в вузах, а вот откуда берутся специалисты третьей категории? Пока в основном это энтузиасты-самоучки, недоучившиеся в вузах, или просто самоучки из интернета. Для работодателей приём на работу таких «бойцов» — настоящая потеря, в которой иногда везёт. Сейчас крупные игроки рынка ИБ создают для решения собственных кадровых задач свои центры дополнительного образования или профессиональной переподготовки, но в целом такой подход создавшееся положение в стране не исправит.

НЕ ВУЗОМ ЕДИНЫМ...

На самом деле, решением могло бы стать создание системы среднего профессионального образования по направлению информационной безопасности. Тем более что именно эта категория специалистов наиболее востребована, в том числе и в регионах.

ОБЛАЧНОЕ РЕШЕНИЕ

Не секрет, что в разных регионах совершенно разные возможности по созданию и содержанию высокотехнологичных учебных центров. Поэтому выход видится в создании серьёзной технологической базы облачного типа, которая

на уровне облачных сервисов могла бы предоставить доступ любому учебному заведению, любому студенту к получению практических навыков по защите информации на самом современном уровне.

Целью создания таких центров могла бы стать выработка как новых подходов к воспитанию специалистов среднего звена в сфере ИБ, так и отраслевых требований к таким специалистам, что поможет эффективному достижению главной цели — формирования федерального кадрового резерва в области защиты информации.

Для этого необходимо решить ряд задач, среди которых:

- ♦ создание некоммерческой учебно-методической и просветительской организации (НУМПО ЗИ) по вопросам подготовки специалистов среднего технического звена с акцентом на изучение использования российских программно-аппаратных СЗИ всех направлений для различных отраслей;

- ♦ создание и поддержание в актуальном состоянии облачных сервисов, на которых колледжи и техникумы, работающие по программам ЗИ, могли бы получать некоммерческий доступ для своих студентов для практики на технических средствах защиты в условиях

моделирования сложных кибератак на инфраструктуры различного назначения;

- ♦ разработка и поддержание в актуальном состоянии моделей различных типов инфраструктур для различных отраслевых решений;

- ♦ создание и поддержание в актуальном состоянии базы данных по актуальным угрозам и видам атак и своевременное создание моделей актуальных видов атак для различных типов инфраструктур;

- ♦ формирование требований на изменения к различным направлениям специализаций в области ЗИ для подготовки рекомендаций для внесения изменений в стандарты образовательной деятельности (включая ФГОС, модели выпускников и т.д.) на основе опыта применения киберполигонов, анализа тенденций развития вредоносной активности и развития средств ЗИ, анализа передового опыта российских разработчиков;

- ♦ формирование и поддержание в актуальном состоянии программно-аппаратной базы облачных киберполигонов на базе отечественных решений;

- ♦ формирование и поддержание базы данных текущих и перспективных потребностей предприятий для своевременного внесения изменений в планы обучения по числу специалистов и их

- ♦ типовых методических материалов, учебных курсов и программ обучения на этой учебно-материальной базе.

Способа решить проблему, кроме как перевести практическое обучение на централизованные облачные платформы, нет. Тут автор прав. Однако это уже было. Не далее как в прошлом году крупные центры подготовки при крупных университетах по стране вроде как были заявлены. Наверное, они уже есть, наверное, на этом оборудовании и сервисах кого-то учат по новым современным программам обучения. Наверное, уже есть наученные новые квалифицированные специалисты. Осталось малое: понять, кого, чему, в каких объемах, кто учит и по каким программам? Может быть, и вопроса уже нет.

Но почему же «Яндекс» и другие компании продолжают идти своим путём? И почему вузы, насколько мне известно,

по-прежнему мучаются с учебно-материальной базой, а если покупают её, то за деньги спонсоров. А если их нет, этих спонсоров? Так и сидим в основной своей массе непонятно на каком ПО, старых серверах, в условиях санкционного воздействия и дефицита импортозамещения. Если так сидеть и дальше, то ничего, похоже, и не будет. Из ничего может родиться только ничего.

Оптимальный путь — создание в форме автономного учебного центра с государственным участием мощной стандартной облачной платформы обучения практическим технологиям безопасности в интересах всех учебных заведений страны. Для этого нужно сконцентрировать немалые выделяемые, но распыляемые сейчас финансовые средства в одну точку. При этом в учебных заведениях следует иметь рабочие места с удалённым доступом к этим

централизованным ресурсам для выполнения лабораторных и иных работ с учётом всего спектра средств защиты информации. Это позволит задать необходимую, стандартную и очень высокую планку практической подготовки в стране специалистов в области ИБ и действительно относительно быстро подготовить необходимое число специалистов, владеющих практическими навыками работы.

С учётом решаемой задачи обучения не думаю, что в этой системе остро будут стоять задачи обеспечения ИБ. Они выглядят стандартно. А вот к учебно-методической работе в этих центрах можно привлечь специалистов от наших отечественных вендоров, тем более что они сконцентрированы в двух-трёх крупных городах и уже сейчас имеют собственные и весьма неплохие программы обучения и хороший опыт в сфере подготовки кадров.

квалификации, в том числе потребности военных комиссариатов в подготовке указанных специалистов;

♦ оказание помощи в трудоустройстве специалистов — выпускников средних технических учебных заведений;

♦ организация полноценного самостоятельного центра повышения квалификации специалистов по направлению ЗИ на базе УМПО ЗИ;

♦ получение лицензий регуляторов, включая лицензии на образовательные виды деятельности.

БИБЛИОТЕКИ С ОТКРЫТЫМ КОДОМ

Параллельно с созданием образовательного центра необходимо будет решить ещё одну сопутствующую задачу.

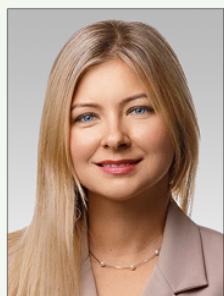
Образовательный центр должен базироваться на отечественном программном обеспечении (ПО), а одной из особенностей современного развития разработки ПО самого разного уровня — от сетевого/системного до приложений / облачных приложений — является широкое использование библиотек с открытым кодом.

Использование таких библиотек несёт в себе две большие проблемы — отсутствие гарантий поддержки в случаях форс-мажорных обстоятельств и высокая потенциальная степень угрозы включения в библиотеки вредоносного ПО и наличие недекларируемых возможностей (НДВ). Частично проблема могла бы быть решена сертификацией (оценкой соответствия требовани-

ям) библиотек ФСТЭК. Однако такой подход не позволяет быстро и гибко реагировать на изменения требований к конечному продукту, и, кроме того, для библиотек с открытым кодом часто бывает невозможно найти заявителя работ.

НЕКОММЕРЧЕСКИЙ ЦЕНТР РАЗРАБОТКИ ПО

Указанные проблемы создают значительные трудности в реализации программы импортозамещения на федеральном уровне. Одним из подходов в этом направлении может стать создание некоммерческого центра компетенций разработки программного обеспечения (НЦК РПО), создание и поддержание федеральной базы



Екатерина СТАРОСТИНА
архитектор кафедры
информационной
безопасности и системного
администрирования
колледжа IThub

BIS-КОММЕНТАРИЙ

НЕ НАДО БОЯТЬСЯ КОЛЛЕДЖА!

Последние месяцы в стране и мире наблюдается смещение тенденции в трудоустройстве в сфере ИБ и ИТ с кандидатов с высшим образованием на кандидатов среднего специального звена. В частности, компания Intel, пытаясь справиться с нехваткой кадров, нанимает на работу выпускников школ, едва поступивших в колледж. Пример компании «Яндекс» тоже наводит на мысли — этой весной она якобы объявила о том, что «Яндекс» будет делать ИТ-специалистов из своих курьеров. Это тот случай, когда «сказка ложь, да в ней намёк...» ИТ-компании прибегают к такого рода найму сотрудников в том числе и потому, что запас специалистов, уже имеющих багаж знаний и достаточный опыт работы, ищущих новую работу, практически исчерпан. На этом фоне компании начинают возвращать собственных

специалистов, нанимая их ещё на этапе обучения.

В связи с оттоком западных специалистов из России ведущие компании стали всё чаще делать выбор в пользу самостоятельного обучения своих сотрудников. Как показывает практика, именно такая тактика позволяет избежать нехватки специалистов и поддерживать высокие темпы роста российского рынка, особенно в части разработки своего программного обеспечения, а также и других технологически значимых отраслей, в то время как система высшего образования не успевает реагировать на изменения информационной повестки так быстро, как этого требуют современные реалии.

ПРИМЕР НАШЕГО КОЛЛЕДЖА

Прямым доказательством этого факта является постоянное сотрудничество ведущих профильных организаций России

с колледжем IThub — одним из первых продвинутых колледжей нашей страны не только с высоким уровнем теоретических и практических знаний, но и со своей корпоративной культурой, этическими ценностями и инновационными подходами к образованию. Не понаслышке зная боль бизнеса, будучи действующими сотрудниками российских компаний, коллектив нашей кафедры создал уникальное бизнес-ориентированное обучение. Формируя его программу, мы активно приглашаем к сотрудничеству российские компании и выстраиваем под них воронку подготовки востребованных специалистов информационной безопасности.

Исходим мы из конечной точки: каких именно специалистов не хватает бизнесу, что специалист должен уметь, какими навыками и знаниями обладать, чтобы безболезненно войти в

проверенного набора библиотек открытого кода.

Основными задачами НЦК РПО будут задачи, связанные с созданием и поддержанием жизненного цикла федеральной базы проверенного набора библиотек открытого кода (БОК):

- ♦ анализ потребностей производителей ПО в различных типах БОК;
- ♦ каталогизация и классификация различных типов БОК;
- ♦ проведение оценки актуальности использования БОК;
- ♦ формирование заказов на разработку и возможная разработка БОК, не имеющих аналогов;
- ♦ формирование решений на включение в базу новых БОК на основе заключений тестирования;

♦ тестирование на отсутствие НДВ и уязвимостей БОК, подлежащих включению в базу;

♦ обязательное тестирование Базы (части базы) БОК при выявлении новых критичных уязвимостей, актуальных для Базы (части базы);

♦ периодическое тестирование на НДВ и новые уязвимости всей базы;

♦ формирование рекомендаций производителям по использованию БОК для различных типов предметных областей;

♦ проведение на базе НУМПО ЗИ тестирования готового ПО на различных математических моделях в условиях воздействия различных типов критических угроз;

♦ формирование рекомендаций по использованию отечественной эле-

ментной базы для разработки программно-аппаратных комплексов, в том числе для защиты информации;

♦ разработка предложений по исключению БОК из базы.

ПОДВОДЯ ИТОГИ

Подводя итоги можно и нужно сделать выводы.

1. Специалисты разные нужны, специалисты разные важны.

2. Подготовка технических специалистов по ИБ/ЗИ — сложная многогранная задача, имеющая много вариантов решения на самых разных уровнях, и без активного участия непосредственных заказчиков подготовки таких специалистов решить её будет трудно.

конкретную компанию и оставаться в ней востребованным. Таким образом, мы выстраиваем действующую модель компетенций: «знания — навыки — компетенции», чтобы на выходе из колледжа отдавать компании бизнес-ориентированного специалиста.

Хочу подчеркнуть, что образовательная программа колледжа IThub строится по нескольким ключевым бизнес-ролям: «специалист по защите информации», «этичный хакинг», «сетевое и системное администрирование». Ведущими руководителями этих направлений выступают эксперты-практики подведомственной среды: руководитель дочерней компании «РЖД» «Цифровые сервисы» Михаил Абрамов, генеральный директор компании «Киберполигон» Лука Сафонов и другие.

В этом и есть конкурентное преимущество выпускника колледжа: учась после 9-го класса, уже на третьем курсе колледжа он может совмещать работу с учёбой, а на четвёртом, выпускном, курсе реализовать дипломный проект в профильной организации у ведущего эксперта отрасли, тем самым создав себе конкурентное портфолио для последующей своей реализации на рынке труда как специалиста.

ОПОРА НА ПРАКТИКОВ

Будучи практикующими экспертами, наши преподаватели как никто другой знают потребность компаний в конечном

сотруднике и могут наиболее точно сформировать программу обучения будущего специалиста. Более того, по линии информационной безопасности колледж связывает взаимная дружба с экспертами из таких российских компаний, как «Код безопасности», R-Vision, Positive Technologies, «Лаборатория Касперского», Bi.Zone, «P-Texno», «Инфотекс», «Информзащита», Stack Group, «Ростелеком-Солар», RuSIEM, «Астра Линукс», «ИнфоВотч», «Комрунет», «Орлан» и другими. При этом соглашение о сотрудничестве с той или иной компанией не ограничивается лишь точечной подготовкой специалистов, а также нередко перетекает в работу над конкретными проектами.

ЧЕГО БОЯТСЯ ШКОЛЬНИКИ

Конечно, сейчас в сфере СПО тема ИБ активно муссируется, продвигается.

Но после школы всегда сложно определиться с выбором, особенно после 9-го класса. Школьнику страшно идти в это направление, он думает: «Не потяну». Задача сегодняшнего сообщества, что вовлечено в образовательную деятельность, — это поменять отношение к образованию в сфере ИБ, сделать его доступным, понятным, с «человеческим лицом».

ФРАНЧАЙЗИНГ В ОБРАЗОВАНИИ

Поддержу идею о том, что создание высокотехнологичных учебных центров

позволит колледжам, особенно в регионах, получить доступ к необходимым образовательным инструментам. Колледж IThub также стремится к развитию в данном направлении. Открытие нами франчайзинговых филиалов в четырёх городах (Екатеринбург, Махачкала, Ростов-на-Дону и Владивосток) позволяет сделать образование в сфере ИБ в регионах более доступным, а отрасли — получить подготовленных специалистов.

ИМПОРТОЗАМЕЩЕНИЕ

Не останется без внимания и вопрос импортозамещения и использования отечественного программного обеспечения. Колледж IThub следует бизнес-ориентированной модели обучения, и при обучении студентов мы используем новые и актуальные отечественные разработки ПО в области ИБ, сетевого и системного администрирования.

Таким образом, прогрессивный подход к среднему профессиональному образованию, подготовка кадрового потенциала для российских компаний становится незаменимым вкладом не только в расширение профессиональных возможностей молодых специалистов, но и в укрепление информационного суверенитета нашей страны, поддержку идей импортозамещения и импортонезависимости. Ведь представить себе информационную безопасность без сильных специалистов в этой области практически невозможно.

ОСТРЫЙ ДЕФИЦИТ ИБ-СПЕЦИАЛИСТОВ СОХРАНЯЕТСЯ В РОССИИ

АНАЛИТИКИ HH.RU СПЕЦИАЛЬНО
ДЛЯ BIS JOURNAL



Ксения ТРОХИМЕЦ
заместитель
директора
департамента
специальных
проектов hh.ru

Аналитики hh.ru специально для BIS Journal продолжают следить за ситуацией со спросом и предложением специалистов по информационной безопасности в России в 2021 и 2022 годах.

За период с января по сентябрь 2022 года на hh.ru компании-работодатели опубликовали 21 290 вакансий для ИБ-специалистов, что на 20% ниже показателя аналогичного периода прошлого года. Отрицательная динамика вызвана серьёзной «просадкой» в количестве вакансий в апреле, июне и июле 2022 — их было в среднем на 1,2 тыс. меньше, чем в соответствующие месяцы прошлого года. Несмотря на отрицательную динамику спроса на ИБ-специалистов, дефицит кадров в этом секторе усугубляется: на одну открытую ИБ-вакансию по-прежнему приходится менее одного резюме (0,4 в течение 2021 и 0,7 в течение 2022). Для сравнения, в ИТ-сфере в течение 2021 года конкуренция составляла 1,8, в 2022 — выросла до 3,9. По подсчётам аналитиков hh.ru, для достижения минимально приемлемой и комфортной ситуации с наймом в данном сегменте (т.е. на одну открытую

вакансию приходилось бы четыре резюме, тогда у работодателя есть адекватный выбор среди кандидатов по уровню требуемых навыков и опыту) рынку труда требовалось дополнительно порядка 120 тыс. ИБ-специалистов в 2021 году и свыше 60 тыс. за девять месяцев 2022 года. Сегодня же разрыв спроса и предложения остаётся кратным и речь по-прежнему идёт о недостатке до десяти тысяч специалистов ежемесячно.

Ситуация вынуждает работодателей снижать требования к будущим сотрудникам в ИБ-подразделениях. Если в 2021 году свыше половины (51%) вакансий были открыты строго для специалистов с опытом от 1 до 3 лет, то в 2022 их стало 48%. Доли вакансий для опытных специалистов (свыше 6 лет) и молодёжи без опыта остаются прежними — 3 и 13% соответственно, что отражает готовность компаний обучать сотрудников.

Вместе с этим компании за год стали более чётко описывать требования к необходимым навыкам. Доля упоминаний навыков и знаний основ ИБ в вакансиях выросла с 18 до 31%, владение техническими средствами

информационной защиты — с 5 до 8%, средства криптографической защиты информации теперь встречаются в 7% ИБ-вакансий.

Медиана предлагаемой зарплаты ИБ-специалистов выросла на 6%, до 63 100 руб. против 59 500 руб. в 2021 году. Ожидания по зарплате, напротив, снизились на 4%, хотя остаются существенно выше рыночного уровня — с 78 300 руб. до 75 100 руб.

Географически рынок труда в ИБ агрегируют Москва и Петербург — на них по-прежнему приходится чуть больше половины всего объёма вакансий, причём столица нарастила свою долю за год почти на 3 п.п. Далее с большим отрывом идут компании из Новосибирской и Московской областей (по 3%). В остальных регионах равномерное распределение ИБ-вакансий.

В разрезе бизнеса чётко выделяются три отрасли по уровню спроса на ИБ-специалистов — это непосредственно ИТ-компании (доля в 2022—29%, +2 п.п.), финансовый сектор (12%, +1 п.п.) и телеком (8%, —3 п.п.). Госсектор нарастил долю в ИБ-вакансиях до 3% к осени 2022 года.

О HEADHUNTER

HeadHunter (hh.ru) — крупнейшая платформа онлайн-рекрутинга в России, клиентами которой являются свыше 515 тыс. компаний. Цель HeadHunter — помогать компаниям находить сотрудников, а людям — работу и делать так, чтобы процесс поиска сотрудников и работы был быстрым и оставал у обеих сторон только положительные впечатления. Обширная база компании содержит свыше 55 млн резюме, а среднее дневное количество вакансий в течение 2021 г. составило свыше 933 тысяч ежедневно. По данным SimilarWeb, hh.ru занимает третье место в мире по популярности среди порталов по поиску работы и сотрудников. HeadHunter — аккредитованная Министерством цифрового развития ИТ-компания, включена в Реестр аккредитованных ИТ-компаний России.



ПРИЁМНАЯ КАМПАНИЯ – 2022

ЖЕЛАЮЩИХ ПОСТУПИТЬ В ВУЗ СТАЛО МЕНЬШЕ. НАМНОГО

По итогам вступительной кампании 2022/2023 года Министерство науки и высшего образования РФ внесло изменения в «Порядок приёма на обучение по образовательным программам высшего образования — программам бакалавриата, программам специалитета, программам магистратуры», утверждённый приказом Министерства от 21 августа 2020 г. № 1076.

ЧТО ЭТО БЫЛО?

«Порядок приёма на обучение по образовательным программам высшего образования — программам бакалавриата, программам специалитета, программам магистратуры», утверждённый приказом Министерства науки и высшего образования РФ от 21 августа 2020 г. № 1076, по которому были проведены приёмные кампании 2021/2022 и 2022/2023 годов, неоднократно подвергался жёсткой критике со стороны как родительского сообщества, так и руководителей учебных заведений.

Порядок отменял вторую волну приёма, и абитуриент, идущий по общему конкурсу, до последнего не мог реально оценить свои шансы на поступление. И если в 2021 г. приёмная кампания прошла относительно спокойно, возмущались в основном родители, до последнего часа ловившие момент перекалывания оригиналов документов и согласий на зачисление, то в 2022 г. многие вузы были вынуждены проводить дополнительный приём, в том числе на бюджетные места. Значительно снизился и проходной балл на ранее популярные у поступающих специальности.

СМИ сообщали как о рекордном конкурсе на одни направления, так и о значительном снижении интереса (и проходных баллов) к ряду направлений подготовки даже в МГУ им. М. В. Ломоносова, МГТУ им. Н. В. Баумана, ВШЭ, ряде сильных технических и медицинских университетов. Многие региональные учебные заведения недобрали желающих учиться не только на, казалось бы,

непопулярные специальности в области машиностроения, физики и химии, природопользования или сельского хозяйства, но остались незаполненными и места на факультетах ИТ, журналистики, экономики и т.д.

Отмечалось, что и число сдававших профильные экзамены по математике в рамках ЕГЭ было меньше суммарных контрольных цифр приёма в университеты. Снизился и средний балл по русскому, физике и информатике, что также повлияло на ход и итоги приёмной кампании. Ряд технических вузов столицы и вовсе был вынужден давать рекламные посты в социальных сетях, рассказывая о своих направлениях и специальностях (в том числе по направлению «Информационная безопасность»), чего не было в прежние годы.

ЧТО ИЗМЕНИТСЯ В 2023 ГОДУ

Новая редакция Порядка приёма вступает в силу с 1 марта 2023 г., предполагается, что она продержится до 1 сентября 2027 г. Согласно нововведениям, абитуриент сможет подать заявления в

При сокращении бюджетных мест в технических университетах организации могут столкнуться с кадровым голодом, который наблюдается по ИТ- и ИБ-направлениям, где уже сегодня не хватает квалифицированных кадров

пять университетов, выбрав в каждом из них по пять направлений подготовки (ранее было десять). Университеты сохранили право установить меньшее количество специальностей (чем пользуются ведущие вузы страны, ограничившие выбор специальностей тремя направлениями).

Приказ вводит в оборот понятие «специальная квота», которое определено Указом Президента РФ от 09.05.22 № 268 «О дополнительных мерах поддержки семей военнослужащих и сотрудников некоторых федеральных государственных органов» и зачисление по которому уже проводилось в этом году. Таким образом, будет три конкурса на бюджетные места по целевой, особой и специальной квотам, на каждую из которых в отдельности положено выделить 10% бюджетных мест. В случае если бюджетных мест в рамках контрольных цифр приёма окажется меньше, чем требуется для всех льготных категорий, вуз вправе самостоятельно выделить одну совмещённую квоту и установить порядок зачисления по ней.

При подаче документов абитуриент должен указать приоритеты зачисления по различным условиям поступления, если он участвует в нескольких конкурсах и подаёт заявления в учебное заведение и его филиалы, на разные формы обучения, образовательные программы и готов участвовать в конкурсе как на бюджетные места, так и на коммерческой основе. Если у абитуриента есть право на поступление по квоте, но он готов участвовать и в общем конкурсе, это также ранжируется.

Авторы нововведений полагают, что с учётом расставленных приоритетов на каждом этапе зачисления учебная организация определит приоритеты поступающих по направлениям бакалавриата и специалитета, а абитуриент сможет лучше оценить свои шансы на будущее.

Важными для зачисления по направлениям бакалавриата и специалитета факторами остаются оригиналы документов об образовании, предоставленные вузу лично или через портал Госуслуг, если документы подавались в электронном виде. Приказом отменяется отдельное заявление о согласии на зачисление, его заменяет оригинал аттестата или диплома.

Изменить приоритеты зачисления, переложить оригинал аттестата или отказаться от зачисления вовсе можно на любом этапе приёмной кампании вплоть до дня завершения приёма документов. Эксперты полагают, что описанные выше нововведения не помогут абитуриентам и их родителям оценить шансы на зачисление по приоритетам при подаче документов в пять вузов.

Приём документов должен начинаться не позднее 20 июня и завершаться не ранее 20 июля и не позднее 25 июля. В то же время для учебных заведений, которые проводят конкурсы творческой, профессиональной или иной направленности, сроки окончания приёма документов могут сдвигаться на 7 или 10 июля. При этом вузы вправе проводить предварительные слушания в рамках творческих испытаний.

Все вступительные испытания, проводимые вузом самостоятельно, должны завершиться к 25 июля. Определиться с тем, в какой вуз подаётся оригинал аттестата, абитуриент должен до 12:00 по московскому времени в последний день приёма документов.

Конкурсные списки на бюджетные места бакалавриата и специалитета должны быть сформированы 27 июля, 28–30 июля проходит приём приоритетного зачисления, а основной этап длится с 4 по 9 августа. Дополнительный приём на бюджетные места бакалавриата и специалитета, которые остаются

незаполненными по итогам приёмной кампании, завершается не позднее 29 августа.

Зачисление на платные места бакалавриата, специалитета и магистратуры, как и правила зачисления по дополнительному набору, университет устанавливает самостоятельно.

ЧЕГО СТОИТ ЖДАТЬ

На фоне спада интереса к инженерным специальностям возник спор о сокращении бюджетных мест в технических вузах. Проблема обсуждалась на радио «Комсомольская правда», где сторонников сокращения представлял главный научный сотрудник Института образования ВШЭ профессор И. В. Абанкина, полагаящая, что многих технических специалистов вполне могут готовить колледжи.

Против такой позиции выступал ответственный секретарь приёмной комиссии МГТУ им. Баумана И. Д. Сидельников, который отмечал сложность освоения предметов в технических вузах на протяжении всего курса обучения и высокий отток студентов. Поэтому воронка приёма в технические вузы должна оставаться как можно более широкой, чтобы охватить больше абитуриентов, число которых сократится в процессе и по окончании учёбы: не все идут работать по специальности в дипломе. Но оставшиеся в профессии станут элитой, которая будет способна решать современные задачи.

При сокращении бюджетных мест в технических университетах организации могут столкнуться с кадровым голодом, который наблюдается по ИТ- и ИБ-направлениям, где уже сегодня не хватает квалифицированных кадров. С учётом оттока специалистов весной-осенью 2022 г. дефицит будет только расти.

Дискуссия продолжается в телеграм-каналах, её участники продолжают выяснять, что важнее: квалифицированные выпускники университетов, дожившие до диплома, или расходы бюджета на их подготовку с учётом отсева.



Марина БРОДСКАЯ
обозреватель BIS Journal

«ДУМАТЬ И ВКЛАДЫВАТЬСЯ В ОБРАЗОВАНИЕ!»

ТОЛЬКО ТАК МОЖНО РЕШИТЬ ПРОБЛЕМУ
КИБЕРБЕЗОПАСНОСТИ В СТРАНЕ

США, ШТАТ ФЛОРИДА. ЧЕТЫРЕ ПРОЕКТА

Центр кибербезопасности Флориды выделил Международному университету Флориды более \$2 млн на четыре проекта, направленных на обучение и подготовку студентов к карьере в области кибербезопасности.

Гранты, финансируемые программой Cybersecurity and Information Technology Pathways (Cyber/IT Pathways), помогут расширить программы Университета, направленные на решение проблемы нехватки квалифицированных кадров в области ИБ и ИТ. Средства пойдут на проведение исследований, повышение квалификации студентов и служащих государственных и некоммерческих организаций, а также на профориентацию школьников по направлениям кибербезопасности.

По прогнозам Бюро статистики труда США, число рабочих мест в сфере кибербезопасности в стране вырастет на 33% с 2020 по 2030 гг. Этот показатель растёт значительно быстрее, чем в среднем по всем другим профессиям. Карта вакансий CyberSeek показывает, что сегодня в США более 700 тыс. свободных рабочих мест в области ИБ. Флорида — четвёртый в США штат с наибольшим числом вакансий в этой сфере.

Программа Cyber/IT Pathways — совместная инициатива Департамента образования штата и Центра кибербезопасности Флориды — направлена на привлечение и подготовку как можно большего числа студентов в области кибербезопасности и ИТ. Общая сумма грантов в рамках этой инициативы составляет \$15,6 млн. Создатели программы ставят перед собой и другую задачу: увеличение числа национальных кадров в областях ИТ и ИБ.

— Cyber/IT Pathways — это крупная инвестиция в повышение готовности жителей Флориды к заполнению вакансий в сфере кибербезопасности и информационных технологий, — отмечает Джеймс Уэлш, директор Центра образовательных технологий и главный исследователь программы Florida Cyber/IT Pathways. — Мы рады, что наш региональный партнёр — Международный университет Флориды — поддерживает эту инициативу и вовлекает выпускников школ и колледжей в эти сферы.

Для финансирования в Международном университете Флориды были отобраны следующие программы:

♦ проект HaHa (Hands-on Hardware Security Education, Практическое обучение аппаратной безопасности) получил

\$1,2 млн. Программа направлена на расширение и диверсификацию образования в области аппаратной безопасности для удовлетворения растущих потребностей в кибербезопасности по всему штату и стране.

♦ Программа повышения квалификации в области кибербезопасности для учителей школ, основанная на Minecraft, получила \$250 тыс. Цель — внедрение игрового подхода к обучению в области ИБ на основе Minecraft — популярной игры среди подростков.

♦ Программа «Путь кибербезопасности для общественных и некоммерческих организаций» получила \$680 тыс. Эта программа включает специальное онлайн-обучение и очные семинары по ИБ и ИТ для специалистов государственных и некоммерческих организаций и направлена на то, чтобы НКО привлекали к образованию в области кибербезопасности учащихся из неблагополучных семей.

♦ Стипендиальная программа по разведке киберугроз (CTI) Университета выиграла более \$280 тыс. Программа стипендий CTI предоставляет студентам и аспирантам годовую программу подготовки кадров в области ИБ, которая включает междисциплинарную академическую подготовку,

наставничество, профессиональное развитие и гарантированные стажировки после окончания учёбы. Программа также предоставит студентам обучение по безопасности и сертификацию и покроет расходы на экзамены.

Стоит отметить, что ранее учебное заведение уже получало \$2 млн на разработку инструментов кибербезопасности с искусственным интеллектом и провело конференцию Национальной инициативы по образованию в области кибербезопасности — 2022 (NICE), посвящённую изучению способов подготовки квалифицированных кадров в области кибербезопасности.

ШТАТ АЛАБАМА. ПРО ИНЖЕНЕРОВ

Круглый стол, посвящённый реализации Национальной стратегии кибернетической инженерии (CIE), прошёл в Обернском университете (Алабама) по инициативе Института Чарльза Д. МакКрари. Национальная стратегия CIE объединяет разработчиков энергетических систем и стандартов, производителей, организации и научные круги, национальные лаборатории, владельцев и операторов инфраструктуры. Стратегия призывает использовать проектные решения и инженерные средства как для контроля за кибератаками, так и для уменьшения их последствий.

Для этого необходимо интегрировать киберустойчивость в проектирование, внедрение, эксплуатацию и обслуживание критически важной энергетической инфраструктуры, считают собравшиеся. Участники дискуссии рассмотрели пробелы в ИБ в современных подходах к инженерным операциям, изучили проблемы, с которыми сталкиваются сектора КИИ при защите от сложных киберугроз, и обсудили, как внедрение CIE может помочь управлять киберрисками по мере развития сети.

«Учитывая дефицит квалифицированных кадров в области ИБ, который оценивается в США в 700 тыс. человек, необходимо подготовить преподавателей и студентов к изучению новых направлений, — считает Чарльз МакКрари, бывший президент и главный исполнительный директор энергетической компании Алабамы. — Для

этого надо включить в программы подготовки инженеров новые курсы по информатике, добавить темы по кибербезопасности в некоторые курсы программирования или курсы по системам управления. Важно также не просто получение лицензии на право работы в той или иной области критически важной инфраструктуры, но и практическое применение навыков. Это важная задача, которая стоит перед преподавателями колледжей и университетов».

Декан университета Стив Тейлор сказал, что предложения ввести в некоторые программы обучения изменения и дополнения логичны. Но изменить несколько академических программ будет не просто с учётом требований к подготовке традиционных инженерных кадров и нагруженной учебной программы, в которой не так много места.

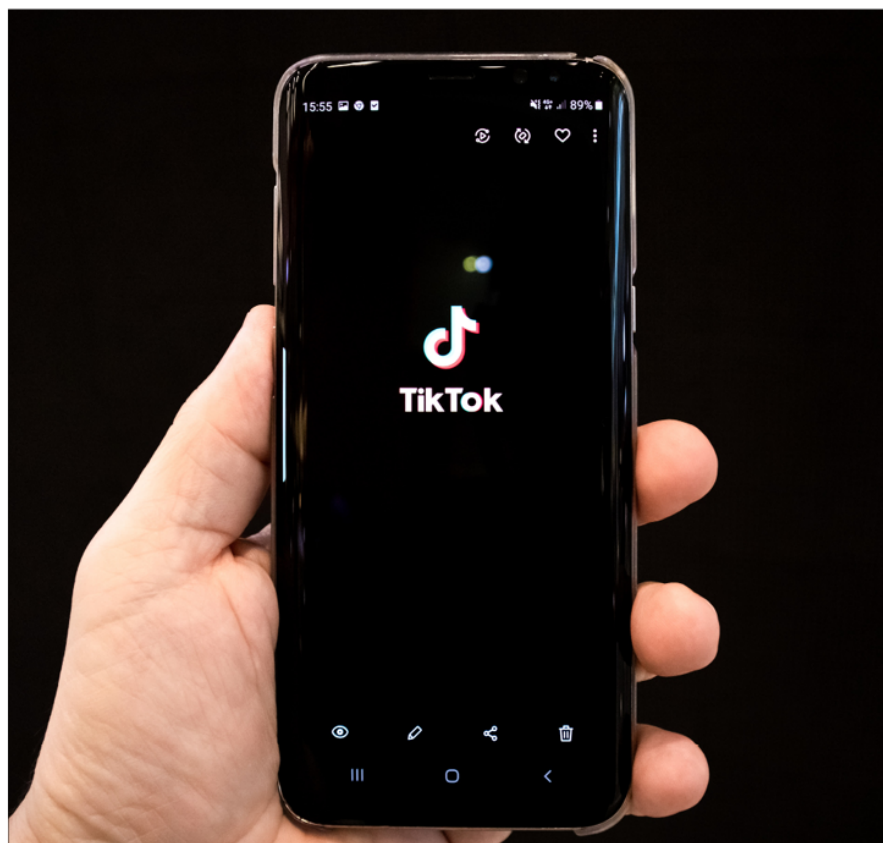
«Лучшая защита от киберугроз — это дальновидное, упреждающее нападение. Это затрагивает многие аспекты общества: от правительства до частного сектора, от электросетей до классных комнат, — считает директор Института

МакКрари Франк Чиллуффо. — Реальность такова, что, если вы хотите предсказать будущее, вы должны его сформировать».

«Один из приоритетов — изначально закладывать кибербезопасность в основу системы, — считает Пуеш Кумар, директор Управления кибербезопасности, энергетической безопасности и реагирования на чрезвычайные ситуации Министерства энергетики (CESER). — Кибербезопасность должна стать таким же ключевым компонентом в энергетическом секторе, как надёжность, безопасность и эффективность. Сейчас самое время это сделать».

ТИКТОК

Видеосервис TikTok запустил новую кампанию по повышению осведомлённости пользователей в вопросах кибербезопасности. TikTok пытается рассказать молодым пользователям об опасностях онлайн-взаимодействия, а также ведёт профориентацию, чтобы привлечь в сферу ИБ как можно больше сообществ. В рамках нового проекта сервис сотрудничает с Глобальным



киберальянсом (GSA) для разработки нового интерактивного инструментария по кибербезопасности для частных лиц.

В инструментарий включены ссылки на ряд приложений и образовательных ресурсов по ключевым проблемам кибербезопасности. Они могут побудить пользователей проявлять большую активность в мониторинге потенциальных угроз. Приложения могут быть полезными обычным юзерам — GSA выделяет некоторые важные инструменты безопасности, которые могут помочь любому при работе в Сети. TikTok также опубликовал новый обзор о том, как люди могут улучшить процесс обеспечения безопасности в Интернете.

Сервис также стремится повысить осведомлённость о рабочих местах в сфере кибербезопасности. «Мы считаем важным обеспечить представительство в индустрии кибербезопасности с помощью программ, направленных на диверсификацию, обучение и расширение возможностей. Поскольку в быстрорастущем секторе кибербезопасности не заполнено более 3,5 млн рабочих мест, TikTok поддерживает новую инициативу #SeeYourselfinCyber от Национального альянса по кибербезопасности (NSA)», — говорится в обращении компании. Цель программы — привлечь больше людей из недостаточно представленных сообществ к работе в сфере ИБ с целью их максимального представительства и объединения с различными группами пользователей.

В 2021 г. TikTok стал спонсором US Cyber Games и работал над укреплением связей с сектором кибербезопасности. Компания проводит программы профориентации в области кибербезопасности. Все эти усилия являются частью стратегии по повышению лояльности к США, чтобы облегчить проблемы, связанные со сбором данных пользователей.

TikTok пообещал предоставить более открытый доступ к своим алгоритмам и процессам модерации на фоне утверждений о том, что его системы подвергаются манипуляциям со стороны правительства КНР. TikTok неоднократно отрицал этот факт, но опасения сохраняются. Считается, что, продвигая

собственные инициативы в области ИБ, TikTok таким образом пытается улучшить свою репутацию.

ШТАТ ИНДИАНА. ТРИ В ОДНОМ

Университет Индианы предлагает своим магистрантам стать разносторонними специалистами — там уже пять лет работает программа получения степени магистра наук в области управления рисками в сфере кибербезопасности. Программа является результатом сотрудничества трёх школ: Школы бизнеса Келли, Школы права Маурера и Школы информатики, вычислительной техники и инженерии Ладди.

Выпускник 2020 г. Джозеф Шустер, получивший степень по кибербезопасности, сказал, что программа дала ему возможность отказаться от первого — музыкального — образования и превратить вторичный интерес к технологиям в карьеру в международной консалтинговой фирме, работающей в сфере ИБ.

«Те знания, которые я получил по программе, идеально подходят для управления рисками третьей стороны, чем я сейчас и занимаюсь», — сказал он. — Школы, больницы, муниципалитеты и предприятия ежедневно сталкиваются с атаками на ИТ-инфраструктуру. Программа подготовила меня к пониманию, как работает кибербезопасность в реальном мире. Это было учтено во всех трёх аспектах дипломной работы».

«Мы являемся первой в стране программой по кибербезопасности с тремя дисциплинами, которая знакомит студентов с техническими, юридическими и деловыми аспектами управления рисками кибербезопасности», — отмечает Апу Кападия, новый председатель программы.

Создатели уникальной интегрированной программы хотели восполнить нехватку квалифицированных специалистов в области ИБ в Индиане и США, уделяя особое внимание междисциплинарному киберобразованию и обучению прикладным сервисам. Объединив усилия, три школы создали единую магистерскую программу. Позже её дополнили курсами Клиники кибербезопасности IU, Hacking4Defense, а вершиной обучения стал уникальный курс, на

котором студенты работают с такими клиентами, как Microsoft и НАТО.

Междисциплинарный подход готовит студентов к защите интеллектуальной собственности и конфиденциальности, повышению безопасности систем и борьбе с киберугрозами в области национальной безопасности, даёт другие навыки. Студенты могут адаптировать свою учёную степень к широкой направленности или специализации в одной из четырёх областей: технологии, бизнес, юриспруденция или искусственный интеллект. Они также могут получить степень полностью онлайн или с помощью гибрида очных и онлайн-занятий.

Студенты, выбирающие гибридный вариант, как правило, являются недавними выпускниками бакалавриата, в то время как студенты, получающие степень онлайн, чаще имеют опыт работы в других сферах и хотят сменить направление деятельности или повысить свою квалификацию.

Студенты могут получить степень всего за год, а могут растянуть учёбу на пять лет. Большинство заканчивают её примерно за 2,5 года. К маю 2023 г. будет определена сотня лучших выпускников, которые продолжат успешную карьеру в консалтинговых компаниях, государственных учреждениях, некоммерческих организациях и высших учебных заведениях. Среди работодателей — Microsoft, Deutsche Bank, Ernst & Young и ФБР.

ШКОЛЬНЫЙ ОКРУГ ЛОС-АНДЖЕЛЕС. АТАКА В ДЕНЬ ТРУДА

Хакеры атаковали второй по величине школьный округ в США (600 тыс. учащихся от детского сада до 12-го класса) в выходные, посвящённые Дню труда. Округ охарактеризовал инцидент как «значительное нарушение инфраструктуры системы». Но официальные лица не ожидают серьёзных проблем с обучением и такими услугами, как логистика и питание, а бизнес-операции могут быть отложены или изменены.

С момента выявления инцидента окружные чиновники работали в тесном контакте с правоохранительными органами. Был активирован «протокол реагирования» для смягчения сбоя в

работе округа, включая доступ к электронной почте, компьютерным системам и приложениям. По оценке экспертов, целью хакеров была информация о платежах подрядчиков частного сектора, а не конфиденциальные данные, такие как заработная плата, медицинские и др.

Предполагается, что атака произошла из-за рубежа, есть три подозреваемых страны, однако суперинтендант полиции Лос-Анджелеса Альберто Карвалью их не назвал. Власти округа заявили, что в расследовании и реагировании участвовали Белый дом, Министерство образования США, ФБР и Агентство кибербезопасности и безопасности инфраструктуры Министерства внутренней безопасности.

Атака произошла на фоне роста числа атак программ-вымогателей, нацеленных на сектор образования. «Дело в том, что пандемия Covid вынудила большую часть сектора образования перейти в онлайн и сделала его привлекательной мишенью для хакеров по целому ряду причин, — считает Мэтью Уорнер, технический директор компании по кибербезопасности Blumira. — Школам часто не хватает финансирования для содержания штатного ИТ-персонала. Учащиеся используют собственные незащищенные устройства, что даёт хакерам больше возможностей для взлома школьных сетей. Кроме того, низкие бюджеты на образование затрудняют наём и удержание хороших специалистов в области ИБ».

На момент подготовки материала не было известно, заплатили ли чиновники школьного округа Лос-Анджелеса выкуп кибермошенникам, но округ призывал создать независимую экспертную группу для предотвращения будущих атак.

НИГЕРИЯ. БУДУЩЕЕ БЕЗГРАНИЧНЫХ ВОЗМОЖНОСТЕЙ

Министр государственного образования Нигерии Гудлак Нанах Опиа заявил, что его ведомство будет поддерживать программы частного сектора, направленные на обучение и повышение квалификации граждан страны. Это заявление было сделано в рамках знакомства с образовательной платформой GetBundi.



Запуск образовательной платформы GetBundi в Нигерии

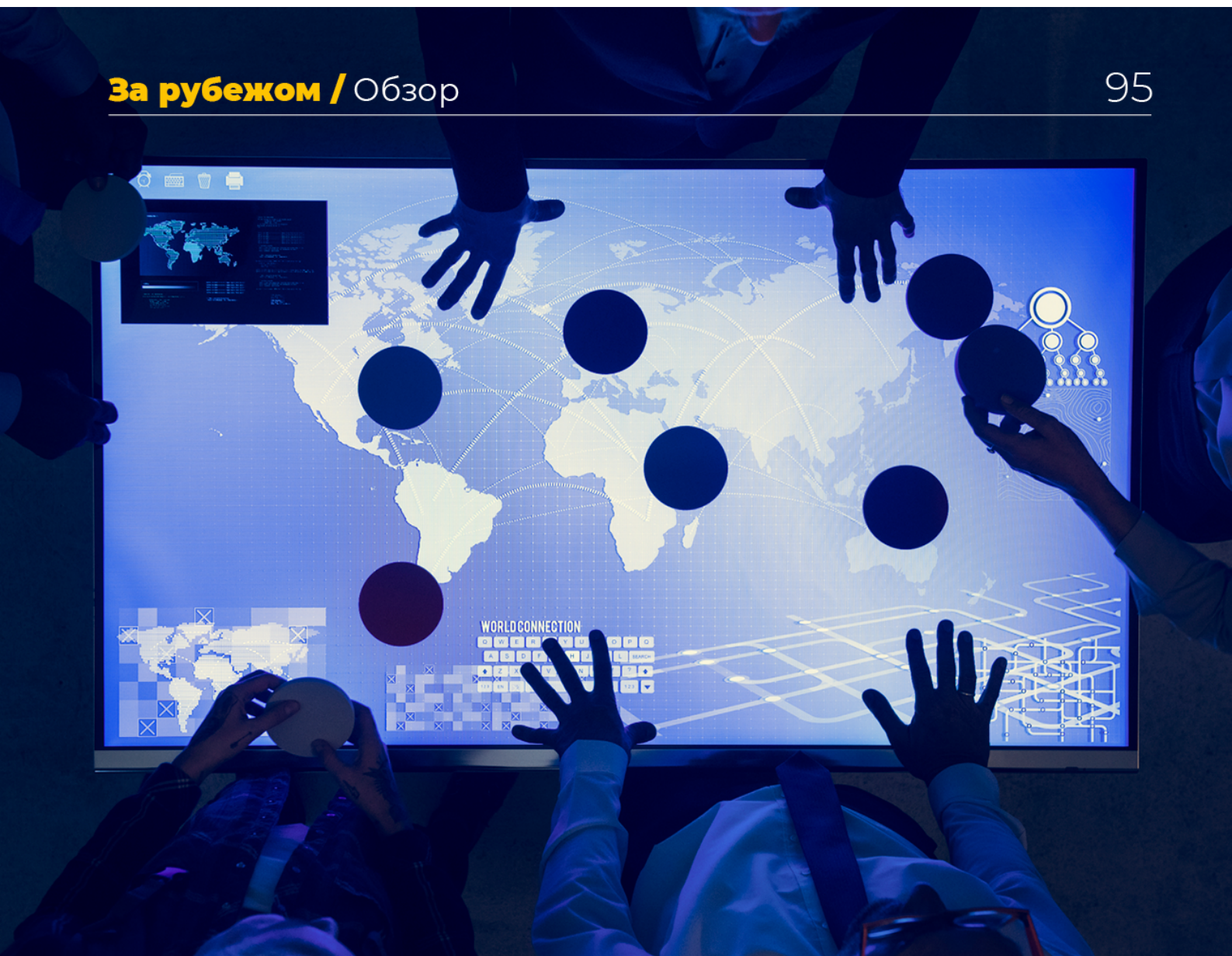
GetBundi — платформа EdTech, разработанная для учеников, имеющих базовое начальное образование, и направленная на понимание курсов по науке, математике и технологиям (STEM), а также английскому языку и цифровым технологиям, чтобы обеспечить слушателям успешную сдачу экзаменов. Она содержит более 1008 часов видеокурсов, проводимых одними из лучших учителей Африки. Переход на новый уровень обучения происходит после ежемесячных онлайн-семинаров с учителями в режиме вопросов и ответов. В первую очередь программа ориентирована на учеников средней школы, но заниматься могут и взрослые.

Оценивая платформу GetBundi, министр подчеркнул важность образования для развития нации. «Система образования Нигерии уделяет особое внимание подготовке детей к гражданской ответственности и развитию. Национальная политика в области образования признаёт его главным инструментом для обеспечения национальных изменений, формирования характера и устойчивого развития», — сказал министр. Он подтвердил, что министерство сделает всё возможное для поддержки GetBundi и любой другой инициативы частного сектора, направленной на просвещение нигерийцев и повышение квалификации рабочей силы. Это является частью целей министерства в рамках стратегического плана министерства.

Осита Опарайго, основатель медиагруппы Reddot Television Network и платформы GetBundi, отметил, что разработчики ориентируются на курсы STEM на уровне начального образования, а также на профессиональный институт цифровых навыков, целью которого является повышение квалификации 10 млн африканцев к 2032 г. Они хотят создать инклюзивное устойчивое развитие, основанное на технологиях.

Курсы STEM основаны на школьной программе Западной Африки для средних школ и могут использоваться в качестве пособия для учителей, для поддержки непрерывного обучения для учащихся в школе и в качестве учебного пособия для учащихся, не посещающих школу. Платформа может быть использована для подготовки к экзаменам, таким как WASSCE и NECO (африканские аналоги ЕГЭ и ОГЭ) и JAMB — вступительный экзамен на получение высшего образования.

Основатель GetBundi сказал, что курсы в области цифровых технологий сосредоточены на программировании, графике, кинематографии, редактировании видео, цифровом маркетинге и кибербезопасности. «За 10 лет, в период 2023–2032 годов, мы хотим повысить квалификацию 10 млн африканцев. Мы назвали этот план „Видение GetBundi 2032“, — пояснил Опарайго, обещая африканской молодёжи будущее безграничных возможностей, построенное на платформе GetBundi.



КИБЕРАТАКИ СТАЛИ МИРОВОЙ УГРОЗОЙ

И ТРЕБУЮТ ОБЩЕЙ СТРАТЕГИИ И СТАНДАРТОВ ЗАЩИТЫ

АВИАТОРЫ

Компании авиационного сектора отказываются от предписаний Агентства транспортной безопасности (TSA) Министерства внутренней безопасности США, которое требует оповещать ведомство обо всех инцидентах кибербезопасности в течение 24 часов.

По новым правилам, принятым в США в декабре 2021 г., каждый аэропорт и оператор авиакомпаний должны назначить координатора по кибербезопасности и сообщать об инцидентах в течение 24 часов. Ранее на чрезмерно жёсткие требования (в частности, уведомлять об инцидентах в

течение 12 часов) жаловались эксперты в трубопроводной отрасли. И TSA было вынуждено внести изменения в регламенты.

Эксперты по ИБ, работающие с авиакомпаниями, заявили, что за такой короткий срок невозможно классифицировать происшествие как



киберинцидент. Глава компании по управлению киберрисками CyberSaint Патрик О'Рейли приводит в качестве примера сканирование и просмотр хакерами систем, при которых злоумышленники ничего не крадут. Поскольку такое сканирование — явление частое, то сообщение о каждом инциденте ляжет ненужным бременем на испытывающие нехватку ресурсов правительственные учреждения. Во многих компаниях нет даже штатных сотрудников службы ИБ, поэтому неясно, как решить проблему отчётов в 24 часа.

О'Рейли пояснил, что другие положения правил, требующих наличия киберкоординатора, плана реагирования на инциденты и оценки пробелов в уязвимости, либо уже действуют, либо относительно бесспорны.

Важным в этих дебатах стало мнение Международной ассоциации воздушного транспорта (IATA) — крупнейшей негосударственной организации, представляющей авиакомпаний в

мире. Процесс разработки общепромышленной стратегии авиационной кибербезопасности находится в стадии обсуждения, создано несколько формальных и неформальных рабочих групп. Для эффективного решения вопроса требуется тесное сотрудничество между заинтересованными сторонами в отрасли и правительстве, соответствие документа международным руководствам и рекомендациям, единые термины и нормы. Директива TSA в данном случае не соответствует международным требованиям, несмотря на то что были проведены и разъяснительная работа, и консультации.

Согласно отчёту юридической фирмы Stephenson Harwood, только в 2020 г. было совершено 62 атаки программ-вымогателей на авиакомпании, аэропорты и компании, обеспечивающие жизнедеятельность отрасли (топливные трубопроводы, инфраструктуру заправщиков и др.). Стоимость требований о выкупе побила рекорды в

2021 году. Среди значимых инцидентов 2022 г. — атаки на Федеральное агентство воздушного транспорта России, системы авиакомпаний Sunwing Airlines (Канада) и SpiceJet (Индия). Европейская группа реагирования на компьютерные чрезвычайные ситуации в области управления воздушным движением (EATM-CERT) отмечает, что количество зарегистрированных кибератак на организации авиационной отрасли выросло на 530% с 2019 по 2020 г.

В целом, считают эксперты, международные правила дадут TSA больше информации о состоянии кибербезопасности и деятельности злоумышленников в отрасли. Данные позволят адаптировать поддержку систем в зависимости от типа атак, что поможет сектору стать более устойчивым к кибератакам.

ТРЕБОВАНИЯ СТАНУТ ЗАКОНОМ

Вопросы кибербезопасности перешли на правительственный уровень. После десятилетий, когда организации частного сектора в большей или меньшей степени справлялись с киберинцидентами самостоятельно, на проблему обратили внимание все: масштабы и последствия кибератак стали мировой угрозой.

В США готовится целый ряд нормативных актов и правоприменительных мер в области кибербезопасности. Федеральная торговая комиссия, Комиссия по ценным бумагам и биржам, Управление по контролю за продуктами и лекарствами, Министерство транспорта, Министерство энергетики и Агентство по кибербезопасности и инфраструктурной безопасности работают над новыми правилами. Кроме того, в прошлом году 36 штатов приняли новое законодательство в области кибербезопасности. В мировом масштабе уже существует множество правительственных инициатив: Китай и Россия требуют локализации данных, в Индии введена отчётность об инцидентах CERT-In, приняты Регламент по защите данных ЕС и отчётность об инцидентах.

В США новые правила потребуют от компаний сообщать о кибератаках, особенно в критически важных отраслях

инфраструктуры, таких как энергетика, здравоохранение, связь и финансовые услуги. Согласно этим правилам, инцидент с кибератакой на трубопроводную систему Colonial Pipeline и прекращение поставок топлива по стране на несколько дней не сможет повториться в глобальном масштабе.

На первый взгляд, требования к кибербезопасности кажутся очень разумными. Но есть много подводных камней. Что должно считаться «инцидентом» в области кибербезопасности: отказ системы при случайном вводе неправильного пароля, получение фишингового электронного письма или проникновение в систему хакеров? Что делать, если злоумышленник проник в систему, но был обнаружен и удалён до того, как был причинён вред? — задаётся вопросами Стюарт Медник из Harvard business review.

Эта двусмысленность требует от компаний и регулирующих органов соблюдения определённого баланса и понимания значимости инцидента. Согласно данным Национальной базы данных уязвимостей (NVD) только 288 из почти 200 тыс. известных уязвимостей активно используются в атаках программ-вымогателей. Знание этого позволяет компаниям уделять приоритетное внимание устранению таких уязвимостей. С другой стороны, компании могут обязать сообщать о тысячах инцидентов в день, даже если большинство из них были спамом. Это бремя как для компаний, так и для Агентства, которому нужно обработать потоки отчётов.

Международным компаниям придётся ориентироваться в различных стандартах отчётности в ЕС, Австралии, США и других странах, знать сроки подачи отчёта (6 ч. в Индии, 72 ч. в ЕС в соответствии с GDPR или 4 рабочих дня в США) с учётом национальных особенностей и множества ведомственных нормативных актов.

Компаниям, подпадающим под действие правил Комиссии по ценным бумагам и рынкам, к которым относятся большинство крупных компаний в США, необходимо быстро определить «материальность» и пересмотреть текущую политику и процедуры для соответствия правилам и упрощения

работы, особенно если решения должны приниматься часто и быстро.

Главное, необходимо поддерживать политику в отношении программ-вымогателей в актуальном состоянии. Необходимо пересмотреть политику компании в отношении оплаты программ-вымогателей, а также возможные изменения в политике киберстрахования.

Многие организации не знали, что в их системах есть уязвимость log4j, потому что это программное обеспечение часто поставлялось в комплекте с другим ПО. Новые правила потребуют от компаний ведения подробной и актуальной спецификации программного обеспечения (SBOM), чтобы быстро и точно знать все программы, встроенные в сложные компьютерные системы.

И конечно, сотрудники отдела ИБ компании должны ознакомиться с этими новыми или предлагаемыми правилами и оценить, какое влияние они окажут на организацию. Технические детали, оставленные на усмотрение команды по ИТ или ИБ, могут иметь далеко идущие последствия для всей компании. И вероятно, изменят многие политики и процедуры в организации.

ВЕЛИКОБРИТАНИЯ

Проект свода правил защиты телекоммуникационных сетей Великобритании от кибератак уже согласован со всеми заинтересованными сторонами и представлен в парламент в соответствии с требованием Закона о связи 2003 г. Он будет рассматриваться в течение сорока дней, после чего будет издан и опубликован.

Новые правила будут одними из самых строгих в мире и обеспечат гораздо более жёсткую защиту Великобритании от киберугроз, которые могут привести к сбою сети или краже конфиденциальных данных, полагают эксперты.

Закон о телекоммуникациях (безопасности), принятый в ноябре 2021 г., даёт правительству полномочия повышать стандарты безопасности мобильных и широкополосных сетей Великобритании. В настоящее время операторы связи несут ответственность за установление собственных стандартов безопасности в своих сетях. Однако анализ деятельности провайдеров

показал, что у них часто мало стимулов для внедрения передовых методов обеспечения безопасности.

Новые правила в статусе закона, разработанные совместно с Национальным центром кибербезопасности и агентством Ofcom, определяют конкретные действия для британских провайдеров общедоступных телекоммуникационных услуг. Они повысят киберустойчивость телекоммуникационных систем страны, внедрив передовые методы обеспечения ИБ в долгосрочные инвестиционные решения поставщиков и повседневную работу их сетей и услуг.

Поставщики будут обязаны:

- ♦ защищать данные, обрабатываемые их сетями и службами, и критически важные функции, которые позволяют работать и управлять ими;
- ♦ защищать ПО и оборудование, которые отслеживают и анализируют свои сети и услуги;
- ♦ понимать риски кибербезопасности и определять аномальную активность, регулярно отчитываться перед внутренними советами;
- ♦ учитывать риски поставщиков и подрядчиков, а также контролировать доступ третьих лиц в работу сетей для повышения безопасности.

Обсуждая закон, министр цифровой инфраструктуры Мэтт Уорман отметил, что правительство знает, «насколько разрушительными могут быть кибератаки на КИИ. Широкополосные и мобильные сети занимают центральное место в жизни граждан. Защита этих жизненно важных сетей, внедрение одного из самых жёстких в мире режимов безопасности телекоммуникаций поможет защитить коммуникации от текущих и будущих угроз».

По мнению технического директора NCSC, доктора Яна Леви, «...новые правила гарантируют, что безопасность и отказоустойчивость этих сетей и оборудования, которое их поддерживает, будут соответствовать требованиям будущего».

Британское агентство Ofcom будет осуществлять надзор, мониторинг и обеспечение соблюдения юридических обязанностей, а также будет иметь право проводить проверки помещений и систем телекоммуникационных фирм,

чтобы убедиться, что провайдеры выполняют свои обязательства. Если компании не будут этого делать, регулирующий орган сможет налагать штрафы в размере до 10% от оборота или, в случае продолжающегося нарушения, до 100 тыс. фунтов стерлингов в день.

С октября на провайдеров будут распространяться новые правила, и Ofcom сможет использовать свои новые полномочия по надзору за исполнением компаниями требований нового закона.

Ожидается, что поставщики услуг приведут сети в соответствие с требованиями правил к марту 2024 г. В своде правил также будут установлены дополнительные сроки для выполнения иных мер. Требования будут периодически обновляться, чтобы соответствовать уровню угроз и предотвращать любые кибератаки.

СТРАХОВЩИКИ ОТКАЗЫВАЮТСЯ ВОЗМЕЩАТЬ УЩЕРБ

Смена руководства компании Lloyd's привела к смене политики в области страхования киберрисков. Увеличение числа атак программ-вымогателей и всё более высокие требования к выкупам нанесли ущерб страховой отрасли.

Долгожданное решение компании Lloyd's о поэтапном отказе от покрытия кибератак, спонсируемых государствами, иллюстрирует ситуацию на страховом рынке, который уже много лет испытывает растущее финансовое давление. Отказ страховщиков также ставит перед американскими компаниями вопросы об их готовности к отражению кибератак и долгосрочных рисках в условиях всё более изощрённых угроз.

«Кибербезопасность остаётся приоритетной областью для Lloyd's», — говорится в заявлении пресс-секретаря компании. Lloyd's уже заявила, что продолжит придерживаться прагматичного и инновационного подхода к поддержке роста киберпространства.

Роль компании заключается в поддержке конкурентного и устойчивого рынка киберстрахования, но в бюллетене нет обязательных положений для агентов. Вместо универсального подхода новое руководство Lloyd's призывает

управляющих агентов проявлять должную осмотрительность в отношении атак, спонсируемых государствами.

Руководство для агентов появилось в то время, когда рынок киберстрахования находится под огромным давлением из-за роста числа атак программ-вымогателей. Давление усилилось после февраля 2022 г., с началом спецоперации России на Украине. Это вызвало значительные опасения клиентов страховых компаний по поводу нападений на их КИИ.

Данные S&P Global Ratings за июль свидетельствуют о значительной турбулентности на рынке киберстрахования. Ожидается, что премии по киберстрахованию будут расти на 25% в год и достигнут \$22,5 млрд к 2025 г. по сравнению с \$9 млрд в 2021 г.

Согласно отчёту, с 2019 по 2021 г. число заявлений о вымогательстве выросло на 232%, а в первом квартале 2022 года уровень невыплат по заявлениям о вымогательстве составил 54% по сравнению с 15% в первом квартале 2019 г.

Есть и другие неприятные вопросы, с которыми рынку придётся столкнуться в связи с исключениями в отношении кибервойн, например, бремя доказывания степени участия государства и соответствия атаки целям конфликта, считает Мануэль Адам, заместитель директора S&P Global Insurance Ratings.

Исследование Blackberry и Corvus показывает проблемы малых и средних организаций. Только 55% респондентов имели покрытие киберстрахования, а 78% добавили такое покрытие к ранее существовавшему полису, что указывает на то, что оно не является приоритетным направлением. Из числа застрахованных компаний 44% организаций имеют страховку на сумму до \$600 тыс., что значительно ниже порогового значения для среднего спроса на страхование от программ-вымогателей.

Смена руководства Lloyd's и изменение политики в области страхования киберрисков вытекают из сложившейся на рынке ситуации. Страховщики вынуждены снижать свои риски, чтобы быть прибыльными, поэтому они ввели строгие требования к киберзащищённости клиентов и задают им дополнительные вопросы. Новые

исключения являются продолжением положений об исключении кибервойн и киберопераций, которые вступили в силу в этом году.

Lloyd's не одинок в переосмыслении политики страхования. Весной 2022 г. немецкий перестраховщик Munich Re раскрыл планы по вводу военных исключений или положений с аналогичными намерениями, которые адекватно решают конкретные проблемы кибербезопасности.

МИГРАЦИЯ

«Австралии необходимо создать программу поддержки миграции в области ИБ, чтобы страна наращивала свой потенциал для защиты от хакеров, работающих под прикрытием других государств, и иных игроков, которые стремятся причинить вред стране, — заявила министр внутренних дел и кибербезопасности Австралии Клэр О'Нил на саммите по вопросам занятости, который прошёл в конце августа в Албании. — Программа миграции, включающая финансовую поддержку людей с навыками работы в сфере кибербезопасности, имеет решающее значение. Нам нужно подумать о том, как включить возможность создания новых рабочих мест в стратегических отраслях, обеспечивающих суверенитет страны. Нам нужно будущее, созданное в Австралии.

Если у нас не будет процветающей, разнообразной и квалифицированной рабочей силы в области кибербезопасности, мы продолжим нести финансовые затраты, которые налагают на экономику и граждан различные киберинциденты», — сказала О'Нил.

Пандемия коронавируса дала Австралии возможность реформировать иммиграционную систему. О'Нил отметила, что двухлетний запрет на въезд и выезд из страны показал зависимость Австралии от миграции. Принимая во внимание тот факт, что страна не является привлекательным местом для высококвалифицированных специалистов, предпочитающих мигрировать в Канаду, ФРГ или Израиль, министр отметила необходимость переосмысления процесса миграции. Переезд в Австралию стал сложной задачей для людей, приезжающих в страну жить или работать: 70 уникальных визовых



программ, каждая со своими критериями и подкатегориями; сотни трудовых договоров и несколько списков квалифицированных профессий — разобратся в этом по силам не каждому. К тому же в стране действует устаревшая система обработки данных, которая не соответствует назначению.

ГРОМКИЕ ВЗЛОМЫ

Судостроительная компания Sembcorp Marine (штаб-квартира в Сингапуре) приняла оперативные меры после обнаружения факта проникновения неизвестных в свои компьютерные сети. Инцидент и связанные с ним риски были эффективно устранены, сообщается в пресс-релизе компании.

Установлено, что была затронута личная информация, относящаяся к работающим и бывшим сотрудникам компании и её гостям, а также информация, относящаяся к деятельности фирмы. Все пострадавшие стороны были

уведомлены об инциденте, Sembcorp обязалась помочь им управлять всеми возможными рисками и принять соответствующие последующие меры.

Бизнес-операции Sembcorp Marine затронуты не были, сканирование, проведённое экспертами по ИБ, не выявило утечки конфиденциальных данных. Ожидается, что кибератака не окажет существенного влияния на материальные активы и прибыль на акцию Sembcorp Marine.

Компания Samsung подтвердила утечку данных, затрагивающую личную информацию клиентов. По заявлению компании, инцидент был обнаружен в конце июля. «Неавторизованная третья сторона получила информацию из некоторых систем Samsung в США». Компания заявила, что 4 августа установила, какие данные клиентов были скомпрометированы. Номера социального страхования и кредитных карт затронуты не были, но была взята

информация о клиентах — имя, контактная и демографическая информация, дата рождения и регистрационная информация о продукте.

«Мы уведомляем пользователей об инциденте», — говорится в заявлении.

Представитель Samsung отказался сообщить, сколько клиентов пострадало или почему компании потребовалось больше месяца, чтобы уведомить клиентов о нарушениях. Компания отметила, что координирует свои действия с правоохранительными органами, а также предприняла шаги для защиты своих систем и привлекла стороннюю фирму по кибербезопасности.

Это второй случай, когда Samsung подтверждает утечку данных в этом году. В марте 2022 г. компания признала, что хакерская группа Lapsus\$ завладела почти 200 Гб конфиденциальных данных, включая исходный код различных технологий и алгоритмов операций биометрической разблокировки.



Александр ВИНОГРАДОВ
с.н.с. ФГУП «ЦНИИХМ»



Сергей МЕНЬШИКОВ
основатель Belarusian InfoSecurity
Community

РОССИЯ — БЕЛАРУСЬ: ДИАЛОГ ДРУЗЕЙ

КАК СТО БР ВОЗРОДИЛСЯ В ТТП ИБ

Каждый российский специалист прекрасно знает про комплекс стандартов СТО БР ИББС. Многие по нему ещё живут, но формально с 2014 г. этот комплекс «приказал долго жить». А жаль. Тем не менее, хотя ЦБ и попытался расширить область ИБ за счёт разных нормативных актов и ГОСТа 57580, забыть СТО БР всё же не получается.

Да и не нужно забывать хорошее, особенно когда речь идёт о лучших практиках. Поэтому Национальный банк Республики Беларусь (далее — НБРБ) принял решение разработать и утвердить для белорусских банков комплекс Технических требований и правил информационной безопасности в банковской деятельности (далее ТТП).

В настоящее время утверждены семь документов:

- ♦ ТТП ИБ 1.1–2020 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Общие положения и терминология»;

- ♦ ТТП ИБ 2.1–2020 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Требования к системам менеджмента информационной безопасности»;

- ♦ ТТП ИБ 3.1–2020 «Информационные технологии и безопасность. Обеспечение информационной безопас-

ности банков Республики Беларусь. Требования по обеспечению информационной безопасности при использовании технологий виртуализации»;

- ♦ ТТП ИБ 4.1–2020 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Менеджмент рисков информационной безопасности»;

- ♦ ТТП ИБ 5.1–2020 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Оценка соответствия информационной безопасности банков Республики Беларусь требованиям ТТП ИБ 1.1–2020 и ТТП ИБ 2.1–2020»;

- ♦ ТТП ИБ 6.1–2020 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Рекомендации по документационному обеспечению деятельности в области обеспечения информационной безопасности в соответствии с требованиями ТТП ИБ 1.1–2020»;

- ♦ ТТП ИБ 7.1–2020 «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь. Рекомендации по менеджменту инцидентов информационной безопасности»;

- ♦ ТТП ИБ 8.1–2021 «Информационные технологии и безопас-

ной безопасности банков Республики Беларусь. Требования по защите программного обеспечения банковских мобильных приложений».

Из многообразия видно, что НБРБ подошёл основательно к решению вопроса обеспечения информационной безопасности в РБ.

Давайте рассмотрим, в чём различие ТТП ИБ и СТО БР ИББС.

- ♦ ТТП 1.1–2020. Документ сформирован на основе семи глав СТО БР ИББС 1.0–2014. Отличие только в отсутствии текста, связанного с персональными данными.

- ♦ ТТП 2.1–2020. Документ сформирован на основе восьми глав СТО БР ИББС 1.0–2014. В общем текст повторяется, за исключением приложений. Что бросается в глаза, «самооценка» теперь — «внутренний аудит». Добавлены пункт 21 «Требования к организации ИБ на стадии жизненного цикла автоматизированной банковской системы» и пункт 22 «Требования к обеспечению защиты информации организации БС» (7, 8, 9-й разделы ГОСТ Р 57580.1–2017).

(В данном документе присутствует несколько приложений:

- пример плана обеспечения непрерывности ИБ;
- типовые недостатки в реализации функций безопасности автоматизированных систем;
- порядок применения положений стандарта ГОСТ Р 57580.1 при

формировании дополнительных требований ИБ к системе защиты информации организации БС;

- рекомендации к проведению контроля исходного кода;
- рекомендации к проведению оценки защищённости;
- рекомендации к проведению контроля параметров настроек технических защитных мер (выявление ошибок конфигурации).

♦ ТТП 3.1–2020. Документ разработан на основании РС БР ИББС 2.8–2015. Текст сохранён, за исключением специфики РБ.

♦ ТТП 4.1–2020. Документ разработан на основании РС БР ИББС 2.2–2009 и СТО БР ИББС 1.4–2018.

♦ ТТП 5.1–2020. Первое, что бросается в глаза, — данные требования и правила созданы не на основе СТО БР ИББС-1.2–2014, а на основе предыдущей версии 1.2–2010. Заменены два групповых показателя ИБ, связанных с персональными данными, два показателя, связанных с организацией ИБ на стадиях жизненного цикла АБС и обеспечения защиты информации в организации БС (с учётом разделов 7, 8, 9 ГОСТ Р 57580 1–2017). Математика и круговая диаграмма повторяют СТО.

♦ ТТП 6.1–2020. Документ разработан на основании РС БР ИББС 2.0–2007. Так как документ был создан в 2007 году и к настоящему времени много уже было доработано в области ИБ, необходимо было пересмотреть Приложение Б. Добавить в него более практичные названия документов, привести к единому наименованию внутренние документы Банка.

♦ ТТП 7.1–2020. Документ разработан на основании РС БР ИББС 2.5–2014 и СТО БР ИББС 1.3–2016. Текст сохранён, за исключением специфики РБ.

♦ ТТП 8.1–2021. Данный документ основан не на комплексе стандартов СТО БР.

Нужно сказать, что сохранение текста в ТТП из российских документов и сама специфика заключается в том, что на момент «разработки» документов в Республике Беларусь не был урегулирован специальными нормативными актами вопрос защиты ПД и



соответствующие разделы просто были изъяты из рассмотрения.

Вышеуказанные документы разработаны в развитие серии государственных стандартов серии «Информационные технологии и безопасность. Обеспечение информационной безопасности банков Республики Беларусь», действующих с 2013 года: СТБ 34.101.41, СТБ 34.101.42, СТБ 34.101.61, СТБ 34.101.62, СТБ 34.101.68. Информацию о них можно почерпнуть, например, на tnpa.by.

Со слов заказчиков ТТП (НБ РБ), следует отметить, что «документы выпущены с целью повышения уровня обеспечения кибербезопасности, но на данном этапе носят рекомендательный характер». В перспективе после внесения изменений в Банковский кодекс РБ планируется на основе прилагаемых требований доработать и утвердить стандарты информационной безопасности, которые уже будут обязательны для исполнения в банковской сфере. Ничего не напоминает?

На практике сейчас (уже по прошествии более двух лет) ТТП мало используются в отрасли (даже в рамках надзорных мероприятий НБ РБ их не

использует), и, кроме того, существуют организационные сложности в осуществлении дальнейших планов.

Что сказать в завершение статьи: НБРБ очень сильно постарался и выпустил все эти документы. Но не стоит забывать, что у специалистов ИБ России имеется большой опыт внедрения комплекса стандартов СТО БР — более 12–14 лет. Многие учились и как внедренцы, и как аудиторы, и стоило бы, наверное, создать совместными усилиями методические рекомендации, в которых и будет отражён весь накопленный опыт, а также более детально разъяснены и ТТП 1.1, и ТТП 2.1.

Кроме того, стоит организовать и совместное обучение специалистов ИБ Беларуси и России. Там российские специалисты смогут научить белорусских коллег практическому внедрению методических рекомендаций. Такое взаимодействие, безусловно, позволит сократить время и избежать грубых ошибок при внедрении СТО БР.

Алексей САВИЧЕВ
исполнительный директор
Центра DPO, Сбербанк

Амина ЗАМУЛИНА
руководитель направления
Центра DPO, Сбербанк

СУРОВЫЙ ОПЫТ ПОДНЕБЕСНОЙ

СИСТЕМА РЕГУЛИРОВАНИЯ
ПЕРСОНАЛЬНЫХ ДАННЫХ
В КИТАЕ



До 2021 г. сфера персональных данных в Китае была достаточно расплывчата и сегментирована. С принятием нового Закона о защите персональной информации (Personal information protection law), далее — PIPL — сфера регулирования ПДн в Китае приняла более структурированный и прозрачный формат.

PIPL не единственный закон, затрагивающий обработку персональной информации. Имеется множество других федеральных, региональных, общих и секторальных законов, стандартов, регламентов и руководств, посвященных

ПДн. Тем не менее именно PIPL является «системообразующим» нормативным актом, задающим общий тренд регулирования ПДн в Китае. В первой части обзора мы познакомимся именно с ним.

ОБЩИЕ СВЕДЕНИЯ

Надзорный орган. Центральным органом по вопросам персональной информации в Китае является Управление по вопросам Киберпространства Китая (Cyber Administration of China), далее — САС. САС отвечает за комплексное планирование и координацию деятельности по вопросам защиты персональ-

ной информации, а также связанные с ними надзор и контроль.

Уполномоченные органы в сфере персональных данных:

Народный Банк Китая (People's Bank of China, PBC). Является секторальным уполномоченным органом. PBC может осуществлять мониторинг за соблюдением требований о ПДн, а также издавать стандарты и правила обработки в рамках своей юрисдикции.

Комиссия по регулированию банковской и страховой деятельности Китая (China Banking and Insurance Regulatory Commission, CBIRC). Является секторальным уполномочен-



ным органом. CBIRC может осуществлять мониторинг за соблюдением требований о ПДн, а также издавать стандарты и правила обработки ПДн в финансовых и страховых организациях.

Министерство промышленности и информационных технологий (Ministry of Industry and Information Technology, MIIT). Ответственно за регулирование и надзор в области ПДн в рамках своей юрисдикции (например, при разработке и использовании мобильных приложений).

Министерство общественной безопасности (Ministry of Public Security, MPS). Является ключевым

органом по борьбе с киберпреступностью. MPS также отвечает за уголовные расследования незаконного получения, продажи и раскрытия ПДн.

Государственное управление по регулированию рынка (State Administration for Market Regulation, SAMR). Осуществляет регулирование и надзор в области обработки персональной информации в рамках защиты прав и интересов потребителей.

Национальный Технический Комитет по Стандартизации информационной безопасности (Technical Committee 260, TC260). Занимается разработкой и унификацией наци-

ональных стандартов в области кибербезопасности, включая обработку и защиту персональных данных.

PIPL и GDPR

PIPL является гибридом европейского и китайского подходов к регулированию ПДн, построен по примеру GDPR и имеет много общего с европейским регламентом, например структуру, принципы и основания обработки ПДн, права субъектов и обязанности операторов и обработчиков, а также требования к трансграничной передаче данных.

Отличие китайского подхода. В рамках национальных стандартов в Китае детализируются виды данных, которые могут приравниваться к ПД, в том числе биометрическим и чувствительным. Национальные стандарты прямо отмечают, что такая информация, как список друзей в социальных сетях или список групп и чатов, также является персональными данными субъекта. Данные о финансовых счетах и геолокации признаются чувствительными ПДн.

Данные как государственно значимый актив. Персональные данные являются государственно значимым «активом», который особо защищается в целях обеспечения национальной безопасности и суверенитета КНР. Этим объясняются специфические требования к порядку трансграничной передачи ПДн, например получение в ряде случаев разрешения уполномоченного органа на передачу или прохождение специальной государственной сертификации.

ЗАКОН О ЗАЩИТЕ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ (PIPL)

PIPL вступил в силу 1 ноября 2021 г., он состоит из 74 статей. Структура и основные положения закона перекликаются с GDPR, поэтому специалистам, знакомым с европейским регламентом, легко ориентироваться в PIPL. Китай создал гибрид режима персональных данных, взяв за основу европейский подход к обработке ПДн и адаптировав его с учётом «китайской специфики».

Территориальное действие. PIPL устанавливает экстерриториальный характер действия. Его положения по

общему правилу применяются к обработке персональной информации на территории КНР, а также к обработке за пределами Китая с целью:

- ♦ предоставления товаров и услуг физическим лицам на территории КНР;
- ♦ аналитики поведения физических лиц на территории Китая;
- ♦ по иным основаниям, предусмотренным законами КНР (без детализации).

Ключевые принципы:

- ♦ законность, необходимость и добросовестность обработки (ст. 5);
- ♦ минимизация данных и ограничение целью (ст. 6);
- ♦ прозрачность обработки (ст. 7);
- ♦ точность информации (ст. 8);
- ♦ безопасность и конфиденциальность (ст. 9);
- ♦ запрет на незаконную обработку ПДн, включая прямой запрет на незаконную продажу и покупку ПДн или обработку ПДн, наносящую вред национальной безопасности и публичным интересам (ст. 10).

Основания обработки (ст. 13 PIPL):

- ♦ согласие субъекта;
- ♦ заключение и исполнение договора с субъектом;
- ♦ подбор кадров;
- ♦ требование закона;
- ♦ публичные интересы (например, публикация в СМИ);
- ♦ реагирование на чрезвычайные ситуации (в сфере общественного здравоохранения, включая защиту жизни и здоровья граждан);
- ♦ статистические исследования.

Требования к согласию:

- ♦ добровольный характер;
- ♦ явность и конкретность;
- ♦ информированность.

Отдельные согласия. В ряде случаев PIPL предусматривает обязанность по сбору «отдельных согласий»:

- ♦ обработка чувствительных данных;
- ♦ передача ПДн другому оператору данных (передача ПДн третьим лицам);
- ♦ трансграничная передача ПДн;
- ♦ обработка изображений и отличительных идентификационных признаков для целей, отличных от обеспечения общественной безопасности.

Всегда ли нужно отдельное согласие, как того требует PIPL? Статья

13 PIPL предусматривает перечень базовых оснований обработки ПДн. Ряд особых положений Закона также предусматривает обязательность получения согласия для обработки ПДн в конкретных обстоятельствах.

Вместе с тем ст. 13 устанавливает, что в случае, когда иные положения PIPL требуют получения согласия субъекта на обработку ПДн, получение такого согласия не является обязательным, если применяется одно из базовых оснований обработки по ст. 13 PIPL.

Так, положения о трансграничной передаче обязывают оператора получить отдельное согласие субъекта и, в отличие от GDPR, не предусматривают такое основание, как передача для целей реализации договора по ст. 49. Однако на практике трансграничная передача ПДн зачастую является одним из этапов общего процесса обработки ПДн, которая может осуществляться на основании заключения/реализации договора, стороной которого является субъект.

В отсутствие устоявшейся практики и разъяснений уполномоченных органов на данный момент сложно прийти к окончательному ответу на вопрос, обязательно ли получение отдельного согласия в случае, описанном выше.

Следует отметить, что анонимные данные исключены из действия PIPL. При этом обезличенные данные продолжают считаться ПДн. Правила обезличивания содержатся в Руководстве по деидентификации персональной информации от 2019 г.

Также PIPL запрещает отказывать в предоставлении товаров и услуг в случае непредставления ПДн субъектом, если такие данные не являются необходимыми для оказания соответствующих услуг.

Примечательно, что в апреле 2022 г. аналогичные поправки были приняты в России к Закону «О защите прав потребителей» № 2300–1.

Права субъектов. Права субъектов ПДн, предусмотренные PIPL, схожи с перечнем прав по GDPR и включают:

- ♦ право на информацию;
- ♦ право на ограничение или возражение против обработки ПДн;

- ♦ право на доступ и переносимость;
- ♦ право на изменение и удаление данных;

♦ право возражать против решений, принятых исключительно на основании автоматизированной обработки.

Управление данными и безопасность. PIPL предусматривает обязанность операторов данных принимать меры организационного и технического характера для обеспечения:

- ♦ соответствия требованиям законодательства (compliance);
- ♦ защиты конфиденциальности ПДн.

В ряде случаев назначение DPO является обязательным.

Закрепляется требование о назначении представителя на территории Китая для компаний, которые зарегистрированы и ведут свою деятельность за рубежом.

Оператор данных обязан на регулярной основе проводить комплаенс-аудиты.

Вводится характерный для GDPR механизм проведения оценок DPIA. Проведение DPIA является обязательным перед началом обработки ПДн в случаях:

- ♦ использования информации в процессе автоматизированного принятия решений;
- ♦ обработки чувствительных данных;
- ♦ поручения обработки обработчику, передачи данных самостоятельно оператору или раскрытие ПДн в публичном домене;
- ♦ трансграничной передачи данных;
- ♦ в иных случаях, существенным образом влияющих на права субъектов ПДн.

Уведомление о нарушениях. По аналогии с GDPR, PIPL устанавливает обязанность информировать надзорный орган и в ряде случаев субъектов ПДн о нарушениях безопасности ПДн. Данная обязанность возлагается только на операторов данных, но не на обработчиков.

Уведомление надзорного органа: во всех случаях.

Уведомление субъектов: оператор не обязан информировать субъектов в случаях, когда им были предприняты достаточные меры для предотвращения вреда субъектам. Тем не менее в случаях, когда надзорный орган приходит к

выводу о риске вреда субъектам, он может обязать оператора уведомить субъектов о таком нарушении.

Сроки: PIPL не устанавливает конкретный срок подачи соответствующего уведомления, ограничиваясь требованием о том, чтобы оно было подано «незамедлительно».

ОБМЕН ДАННЫМИ — УПРАВЛЕНИЕ ПОТОКАМИ ДАННЫХ

Обмен данными между операторами. Перед передачей ПДн от одного оператора к другому передающая сторона обязана:

- ♦ информировать субъекта ПДн о деталях передачи (включая контактную информацию получающей стороны);
- ♦ получить отдельное согласие субъекта ПДн на передачу.

Операторы, совместно определяющие цели и методы обработки, должны заключить соответствующее соглашение, регулирующее их права и обязанности в отношении обработки.

Поручение на обработку. При поручении обработки третьему лицу (обработчику) необходимо заключить договор, определяющий:

- ♦ цели;
- ♦ сроки и методы обработки;
- ♦ категории ПДн;
- ♦ меры безопасности;
- ♦ права и обязанности сторон;
- ♦ право оператора на мониторинг деятельности обработчика.

Как и в GDPR, не допускается привлечение субобработчиков без предварительного согласия оператора. Обработчик обязан действовать строго в рамках поручения на обработку ПДн.

ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПДН

Особенность: «политический» характер защиты китайских данных как актива, имеющего государственное значение.

Реторсии: PIPL допускает принятие ограничительных мер в отношении зарубежной страны (региона) в ответ на принятие ею дискриминирующих запретов или ограничений в отношении КНР. К зарубежным физическим или юридическим лицам, осуществляющим обработку ПДн в нарушение прав

и интересов граждан Китая, либо во вред национальным интересам Китая, могут применяться ограничивающие меры вплоть до полного запрета обработки ПДн.

Запросы зарубежных госорганов. Передача данных зарубежным государственным органам допускается только при получении предварительного одобрения компетентного органа КНР.

Перед передачей ПДн за пределы Китая оператор обязан:

- ♦ Получить отдельное информированное согласие субъекта, которое должно включать:

- наименование и контактную информацию получателя;
- цели и методы обработки;
- категории передаваемых ПДн;
- способ реализации прав в отношении зарубежного получателя.

- ♦ Провести оценку DPIA.
- ♦ Выполнить одно из дополнительных специальных условий:

- пройти оценку безопасности уполномоченного органа (State Cyberspace and Information department);
- получить сертификат уполномоченного органа (на данный момент требование не конкретизировано);
- заключить стандартные договорные условия по форме, утвержденной уполномоченным органом (State Cyberspace and Information department);
- исполнить иные требования, предусмотренные законом (например, в случае обработки генетических данных должны соблюдаться требования Административного регламента по вопросам человеческих генетических ресурсов).

Стоит отметить, что в настоящее время разрабатывается Руководство по оценке безопасности при трансграничной передаче данных. Проект документа находится на публичном обсуждении.

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ

Следя мировым тенденциям последних лет, PIPL устанавливает весьма ощутимые штрафы за нарушения

требований к обработке ПДн. Также PIPL предусматривает как ответственность оператора, так и персональную ответственность лица, виновного в нарушении.

Максимальный размер административного штрафа — 50 млн юаней (около 510 млн рублей, или \$7,5 млн или 5% от оборота за предыдущий год).

ИНЫЕ АКТЫ КИТАЯ В СФЕРЕ ОБРАБОТКИ И ЗАЩИТЫ ПДН

Как было отмечено, PIPL не единственный закон, затрагивающий вопросы обработки ПДн. Для получения более полного понимания регулирования сферы ПДн в Китае рекомендуется ознакомиться со следующими правовыми актами (перечень не является исчерпывающим).

Действующие:

- ♦ Гражданский кодекс КНР, 2021 (ст. 1032–1039);

- ♦ Закон о защите информации (DSL), 2021;

- ♦ Закон о кибербезопасности (CSL), 2017;

- ♦ Национальный стандарт по технологиям информационной безопасности — Руководство по проведению оценки воздействия на защиту персональной информации, 2020;

- ♦ Национальный стандарт по технологиям информационной безопасности — Руководство по защите персональной информации, 2020;

- ♦ Руководство Центрального Банка КНР по защите финансовой персональной информации, 2020;

- ♦ Национальный стандарт по технологиям информационной безопасности — Руководство по деидентификации персональной информации, 2019.

На рассмотрении:

- ♦ Руководство по проведению оценки воздействия на защиту персональной информации при трансграничной передаче ПДн;

- ♦ Руководство по уведомлению о конфиденциальности и согласию на обработку персональной информации;

- ♦ Руководство по защите персональной информации при обработке в публичных облаках.

(Окончание обзора
в следующем номере)



Борис СТОЛПАКОВ
историк криптографии, кандидат
физико-математических наук

ИЗ ТЬМЫ ВЕКОВ ЗВУЧАТ ЛИШЬ ПИСЬМЕНА

В 2022 ГОДУ — ДВА ЮБИЛЕЯ, СВЯЗАННЫХ
С РАСШИФРОВКОЙ ДРЕВНИХ ПИСЬМЕННОСТЕЙ

Ныне трудно представить себе, что ещё чуть более полувека назад слово «криптография» было совершенно непривычно широкой аудитории. Вместе с тем термины «зашифрование», «дешифровка» многим казались вполне понятными. Безусловно, немалая в том заслуга авторов всемирно известных литературных произведений, прежде всего А. Конан Дойля. Внесла свой вклад и научно-популярная литература, связанная с историей и языкознанием. Накопилось уже немало книг, увлекательно повествующих о процессе дешифровки древних текстов на утраченных языках.

ЮБИЛЕЙНЫЙ ГОД

Недавно список интересных изданий пополнил русский перевод книги Майкла Ко «Разгадка кода майя». Как учёные расшифровали письменность древней цивилизации» (англ. *Breaking the Maya Code*). Раньше в сообщениях об этом сочинении название переводили как «Взлом кода майя», что точнее соответствует оригиналу. Вероятно, автор книги в первом англоязычном издании 1992 г. хотел привлечь к ней внимание броским заголовком.

Появление русского издания именно теперь можно объяснить, несомненно, сразу несколькими памятными для любителей лингвистики и дешифровки датами уходящего 2022 г.

Как известно, благодаря французскому египтологу Ж. — Ф. Шампольону с 1822 г. стало возможным чтение многочисленных древнеегипетских текстов. Именно с той поры 200-летней давности началось увлекательное знакомство широкой аудитории с муками дешифровки древних письменностей.

Но всё же издание книги М. Ко больше связано с другим юбилеем. Она посвящена нашему соотечественнику Юрию Валентиновичу Кнорозову, родившемуся в 1922 г. Именно ему удалось внести главный вклад в дешифровку письменности майя в 1952 г.

Сама история утраты знаний об этой письменности весьма поучительна. Ведь в первые десятилетия после появления испанцев в 1517 г. в Центральной Америке письменность майя опиралась на множество её знатоков среди этого народа, проживающего и поныне на полуострове Юкатан, а также подкреплялась немалым числом читаемых текстов. Однако уже во второй половине XVI века и читателей, и сами тексты можно было отыскать лишь с большим трудом. Таков результат встречи с другой цивилизацией — европейской. Вероятно, сказались и завезённые из Европы новые болезни — грипп, корь и оспа, смертельно опасные для местных жителей.

ЗАБРАКОВАН МЕДКОМИССИЕЙ

Будущий удачливый дешифровщик Юрий Кнорозов родился в пригороде

Харькова в семье крупного транспортного руководителя. После окончания школы в 1939 г. он собирался выбрать одну из военных специальностей подобно старшим братьям, но был забракован медицинской комиссией. Запасным вариантом стал исторический факультет Харьковского университета, где всё сложилось благополучно. Вскоре Кнорозова увлекли лекции по психологии и древнеегипетский язык.

Великая Отечественная война вновь изменила все замыслы. В начале июля 1941 г., после второго курса, Юрия направили на строительство оборонительных сооружений под Чернигов. Там он в числе многих попал в «котёл», уцелел и в октябре вернулся по уже оккупированной территории домой. Как известно, весной 1943 г. Харьковщина была освобождена на короткое время советскими войсками. Тогда Юрию удалось добраться до Воронежа, а затем и до Москвы. Благодаря помощи отца в сентябре 1943 г. Кнорозова приняли на второй курс исторического факультета МГУ. В апреле 1944 г. он был призван на нестроевую службу телефонистом и в октябре 1945 г. вернулся в МГУ на третий курс. Приведённые подробности здесь вполне уместны, поскольку они значительно повлияли на события жизни молодого Ю. Кнорозова.

УЧИТЕЛЬ

На истфаке МГУ Юрий увлёкся этнографией, её и выбрал для своей специ-



Иллюстрация 1. Фрагмент надписи из музея Паленке, Мексика

ализации. Кафедру этнографии тогда возглавлял Сергей Павлович Толстов. Он стал научным руководителем Юрия. Фамилия Толстов хорошо знакома выпускникам технического факультета ВШ КГБ и ИКСИ. Им памятен Георгий Павлович Толстов (1911–1986) — известный математик, знаменитый своими лекциями и замечательными учебниками по математическому анализу. Учителем Кнорозова стал старший брат Георгия Павловича — Сергей Павлович.

С. П. Толстов (1907–1976) — крупный историк, этнограф, открыватель древнехорезмийской цивилизации — был значителен и как человеческая личность. В первые же дни Великой Отечественной войны молодой про-

фессор МГУ Толстов записался добровольцем. Вскоре по указанию властей всех профессоров вернули на места работы, но трое отказались подчиниться, один из них — Сергей Павлович. На фронте его способности быстро стали востребованы. Его назначили командиром отделения разведки батареи в противотанковом дивизионе, а затем — командиром взвода разведки арtpолка стрелковой дивизии. В октябре вместе с дивизией он попал в окружение под Ельней. Возглавил выход отряда, хотя сам был ранен и контужен. На этом фронт для С. П. Толстова закончился, а после госпиталей в конце 1942-го его назначили директором Института этнографии АН СССР. Одновременно

в 1943–1945 годах он был деканом истфака МГУ.

ПЕРВОЕ ЗНАКОМСТВО С ПИСЬМЕНАМИ МАЙЯ

Практикой по этнографии на истфаке тогда руководил С. А. Токарев, возглавлявший в Институте этнографии направление американистики. Он и увлёк Кнорозова письменностью майя, предложив познакомиться со статьёй немецкого исследователя П. Шельхаса «Дешифровка письма майя — неразрешимая проблема?». Это случилось в 1946 г.

Чтобы представить себе письменность майя, предлагаю взглянуть на один из её текстов в камне (илл. 1).



Иллюстрация 2. Фрагмент Дрезденского кодекса майя

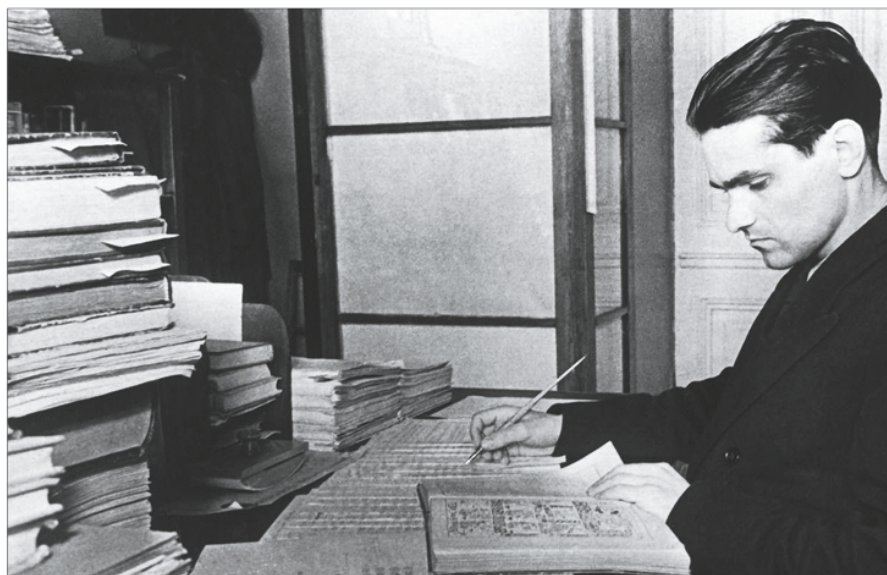


Иллюстрация 3. Ю. В. Кнорозов на рабочем месте

И КРИПТОАНАЛИТИКИ НЕ СМОГЛИ

Понятно, что исследователи из США и европейских государств давно, сразу после успехов Шампольона, пытались читать тексты майя. После Второй мировой войны привлекали к их дешифровке даже бывших, уже ставших известными, криптоаналитиков Уильяма Фридмана и его жену Элизабет. С У. Фридманом в США связывают успех взлома японской «пурпурной» шифровальной машины. Супружеская пара после недолгих попыток признала бессилие своих формально-логических методов, а большого желания погружаться в глубины исторической методологии у неё не было.

Самим историкам временами сопутствовал значительный успех, но лишь

в дешифровке некоторых специальных текстов. Так, ещё в 1880 г. в Дрездене сумели дешифровать календарь майя по материалам кодекса, хранившегося там в королевской библиотеке (илл. 2).

Кодексами обычно называют древние аналоги книг. Кодексы майя — это покрытые текстом длинные полосы местной бумаги из измельчённого луба фикуса, сложенные в виде гармошки. Дрезденский кодекс в разложенном состоянии имеет длину около шести метров.

Постепенно в среде исследователей восторжествовало мнение о чисто символической функции знаков майя, так до Шампольона думали и о назначении египетских иероглифов. В первой половине XX века сложилась влиятельная школа майянистики

во главе с энергичным англичанином Э. Томпсоном, который, полностью отрицая звуковую основу письма майя, препятствовал публикациям исследований в этом направлении. В то же время создавались всё более полные каталоги знаков майя.

РЕШИТЕЛЬНЫЙ ВЫБОР

Летняя практика Кнорозова в 1947 г. прошла на базе Хорезмской экспедиции в Узбекистане. По материалам практики и под руководством С. П. Толстова в 1948 г. Юрий защитил дипломную работу. Но вскоре при обсуждении с Толстовым планов на будущее он решительно заявил, что связывает их с майя и Мексикой, а не со Средней Азией.

Здесь следует упомянуть важный момент. К этому времени Юрий уже глубоко погрузился в майянистику. Он приступил к переводу «Сообщения о делах в Юкатане» епископа Диего де Ланда, важного источника по истории народа майя, содержащего сведения о языке и письменности. В библиотеке им. Ленина имелся микрофильм с французским изданием этой испанской рукописи XVI века. Как оказалось в дальнейшем, это произведение сыграло в деле дешифровки текстов майя ключевую роль — подобно случившемуся с Розеттским камнем, раскопанным французскими археологами и пригрозившимся Шампольону для чтения египетских иероглифов. Заметим, что рукопись де Ланда, впервые обнаруженная и изданная в 1864 г., неоднократно становилась основой для безуспешных попыток дешифровки письменности майя. А вот Ю. Кнорозов, как он сам вспоминал, уже в начале знакомства с текстом де Ланда почувствовал, что прикоснулся к ключу. Это ощущение стало стимулом к дальнейшему многолетнему кропотливому труду до самого его успешного завершения.

ПРИЯТНЫЕ ОЖИДАНИЯ БЫЛИ ПРЕРВАНЫ

Тогда, в 1948 г., приятные ожидания поступления в аспирантуру и приближения к крупному открытию неожиданно были прерваны. Оказалось, что пребывание Юрия на оккупированной территории в 1941–1943 годах не позволяло ему претендовать

на место в аспирантуре сразу после окончания университета, несмотря на энергичную поддержку Толстова и Токарева. Согласно практике того времени, Кнорозов должен был отработать 2–3 года учителем в сельской школе и только после этого поступить в аспирантуру. Такой вариант, вероятно, не устроил Юрия и его наставников. По их общему решению с 1 января 1949 Кнорозов был зачислен младшим научным сотрудником в Музей этнографии народов СССР в Ленинграде.

Обязанности в музее включали разбор коллекций и архива, «выбивание пыли из туркменских ковров» и проведение экскурсий для школьников на тему «Сталинская конституция». Конечно, главной задачей Юрия стала дешифровка письменности майя. В ту пору в предоставленной ему для жилья комнате стены были заполнены рисовками иероглифов майя, а рабочее место в музее — забито книгами (илл. 3).

Интересно, что соседство Юрию на рабочем месте почти весь 1949 г. составлял Л. Н. Гумилёв, знаменитый ныне историк и географ, а тогда молодой кандидат наук.

УДАЧА В САМОМ НАЧАЛЕ

Основой дешифровки Кнорозова стало признание им не рисуночного, а звукового характера письма майя. Юрий был уверен, что ключом к фонетическому чтению должен стать «алфавит де Ланда», несмотря на неудачи попыток его применения предыдущими исследователями.

Так, прежних дешифровщиков ставил в тупик пример де Ланда, в котором тот сообщал, что для обозначения слова «петля» («лэ») писцы майя использовали знаки «э-лэ-э-лэ». А Кнорозов быстро сообразил причину появления этого сочетания знаков. Ведь, диктуя слог «лэ», де Ланда вначале назвал составляющие его буквы, а затем и весь слог: «элэ» (испанское название буквы «л»), «э» (название буквы «э», совпадающее с её звучанием) и слог «лэ». Писец послушно записал всё, что ему продиктовали, так родилось непонятное «э-лэ-э-лэ». Точно так же выглядела запись и в других примерах де Ланда, и там тоже смешивались названия испанских



Иллюстрация 4. Лист рукописи с «алфавитом де Ланда»

букв с их фонетическими значениями (илл. 4).

Эта безусловная удача уже в самом начале исследования постепенно вселила уверенность и в его успешном завершении.

И СНОВА УДАЧНО СЛОЖИЛОСЬ

Интенсивные работы Юрия по дешифровке не только подтвердили весомость знаний, приобретённых в годы учёбы, но и потребовали значительно и быстрого их пополнения. Так удачно сложилось, что ровно в то же время английский исследователь Майкл Вентрис, ровесник Юрия, занимался дешифровкой крито-микенской письменности, пытаясь связать её фонетику с древнегреческим языком. Он активно популяризировал свою методику, но среди западных исследователей внимания не встретил. Юрий же, оценив сходство задач, своей и Вентриса, нашёл в его методе много полезного. По

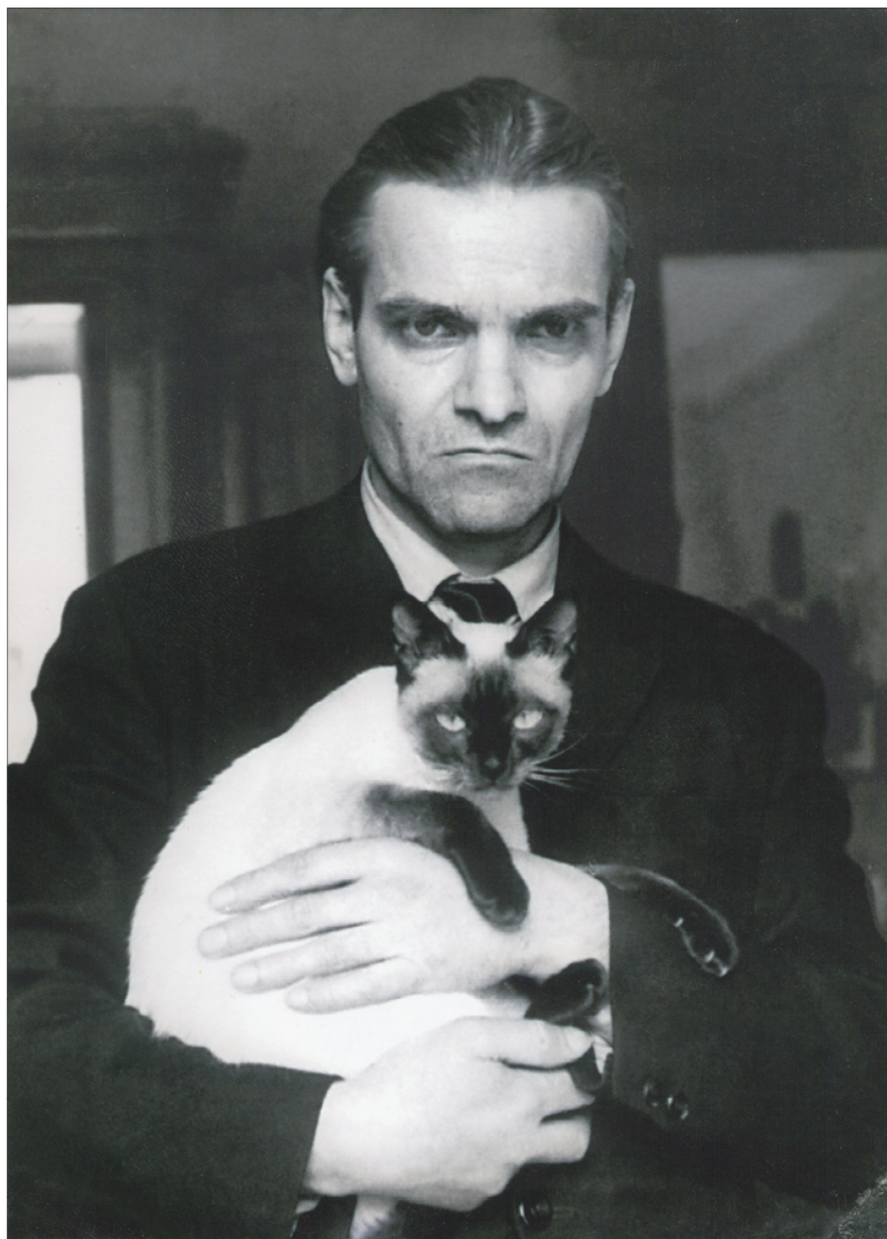
существу, это был комбинаторно-статистический метод, новый для этнографии и археологии и с безусловно криптографическими корнями. Вот он-то и стал теоретической базой дешифровки письменности майя.

Начались скрупулёзные статистические подсчёты частот важных характеристик письма по всем доступным кодексам майя с одновременной классификацией результатов такого анализа.

В результате своих трудов Кнорозов доказал, что в алфавите де Ланда представлены слоговые знаки. Кропотливыми исследованиями удалось продемонстрировать, как епископ добился точной передачи фонетики языка, различия твёрдых и мягких согласных, других нюансов звучания речи.

«ЭТА РАБОТА СОСТАВИТ СЛАВУ СОВЕТСКОЙ НАУКИ...»

Летом 1950 г. Токарев и Толстов предприняли вторую попытку устроить



Ю. В. Кнорозов с сиамской кошкой Асей (Аспидой)

Кнорозова в аспирантуру, на этот раз в Ленинградское отделение Института этнографии АН СССР (Кунсткамеру). По современным сведениям, наставники Юрия изначально предполагали, что его диссертация будет сразу на соискание докторской степени, а не кандидатской, поэтому готовились серьёзно. В 1950 г. Кнорозов поступил в Вечерний университет марксизма-ленинизма, сдал на отлично все вступительные экзамены в аспирантуру, на работе получил премию и благодарность с занесением в личное дело. Прощение

о зачислении Кнорозова в аспирантуру было подано в Президиум АН СССР в декабре 1950 г. В сопроводительном письме научный руководитель С. А. Токарев впервые заявил о наметившемся успехе в чтении письменности майя и предположил, что «эта работа, когда она будет доведена до конца, составит славу советской науки...»

И вновь было отказано по прежней причине — из-за пребывания на оккупированной территории. Но, несмотря на болезненные уколы самолюбия, работа продвигалась ударными темпами.

Уже в ноябре 1951 г. Кнорозов рапортовал в письме Токареву о завершении дешифровки.

МИНУЯ АСПИРАНТУРУ, СРАЗУ В ДОКТОРА НАУК

Первая статья о дешифровке письменности майя вышла уже в 1952 г. в академическом журнале «Советская этнография», его главным редактором был С. П. Толстов. Спустя год публикации появились на испанском языке в Мексике. Тогда же Кнорозов перешёл во вновь открытый сектор Америки, Австралии и Океании в Кунсткамере. Выполненный им перевод «Сообщения о делах в Юкатане» с обширным предисловием был принят к печати Издательством Академии наук. По существу, это была уже готовая диссертация. Наставники посоветовали Кнорозову представить её как соискателю учёной степени, минуя аспирантуру.

Защиту провели 29 марта 1955 г. в Москве, в диссертационном совете Института этнографии, где председательствовал С. П. Толстов. Накануне он оповестил журналистов, пообещав им громкое, общественно значимое событие.

После официальных оппонентов и внушительного доклада научного руководителя председатель совета С. П. Толстов объявил, что для работы Ю. В. Кнорозова «кандидатской степени мало». Его поддержали и официальные оппоненты, и члены совета. Докторов среди них было немало. По заранее подготовленной С. П. Толстовым процедуре провели двойное голосование и приняли положительное решение сначала о кандидатской, а затем и о докторской степени для соискателя.

ВКЛАД БЫЛ ОЦЕНЁН, НО...

Неординарное событие освещалось в советской прессе и за рубежом. Хотя Кнорозов не попал на прошедший тогда в Риме международный конгресс историков, его доклад был опубликован на русском и английском языках. Как общественное признание можно расценить и предновогоднюю публикацию в журнале «Советский Союз» популярной статьи Кнорозова «Загадка майя». А в 1956 г. состоялось и его очное общение с самыми значительными

специалистами по майянистике на Международном конгрессе американистов в Копенгагене. Вклад Кнорозова был оценён, но его подлинное признание среди майянистов растянулось на годы. Достигнутые результаты были бесспорны, но базовые положения, приведшие к ним, нередко вызывали возражения и неприятие, вплоть до подозрений в оккультизме. К сожалению, к науке здесь примешалась политика. Окончательное признание заслуг Кнорозова в майянистике пришло только к концу 1970-х годов.

ОТ «РУЧНОЙ» ДЕШИФРОВКИ — К «МАШИННОЙ»

А в конце 1950-х годов Юрий Валентинович с энтузиазмом принялся за расширение поля применения своей методики. Замышлялась даже разработка основ универсальной теории дешифровки древних письменностей. Такой шаг представлялся вполне естественным, ведь одновременно с Кнорозовым, благодаря использованию родственной методики, громкого успеха в дешифровке крито-микенского письма добился и М. Вентрис.

Предстояла трудоёмкая систематизация эффективно применённых методик, предполагавшая последующую их реализацию на средствах вычислительной техники. В 1959 г. Кнорозова привлекли в Научный совет по кибернетике при Президиуме АН СССР. Разработкой программ для ЭВМ занялись математики. Началось создание библиотеки программ, позволяющих статистически обработать системы письма, обладающие значительным объёмом текстов.

Летом 1959 г. материалы Кнорозова передали в Институт математики Сибирского отделения Академии наук. Руководители института уже в 1960 г. заявили о дешифровке письменности майя, якобы благодаря обработке с помощью ЭВМ массива рукописей. Эти результаты сенсационно докладывались на конференциях по машинному переводу и автоматической обработке текстов. Апогеем стало вручение Н. С. Хрущёву четырёхтомника «Применение электронных вычислительных машин в исследовании письменности древних майя». Хотя



Иллюстрация 5. Награждение Ю. В. Кнорозова президентом Гватемалы

основу этого труда составила база данных Кнорозова, его самого старательно задвинули на задний план, чем немедленно воспользовались и западные оппоненты.

Юрий Валентинович вскоре едко отозвался на принижение своего вклада статьёй в авторитетном академическом журнале «Вопросы языкознания», где отметил: «Проведённая авторами работа показала практически, что современная вычислительная техника может быть использована для целей дешифровки древних систем письма... Следует заметить, что если бы результаты „машинной“ дешифровки не совпали с результатами предшествовавшей ей „ручной“, то пришлось бы пересматривать „машинную“ (а не уже доказанную „ручную“), как её и придётся пересматривать в той части, где приведены заведомо неправильные фонетические чтения (хотя они также дублируют опубликованные раньше). „Машинная“ дешифровка только отчасти дублировала „ручную“ и не прибавила нового к нашим знаниям о письме майя».

Статья была оперативно опубликована и на испанском языке в Мексике.

РЯДОМ С ШАМПОЛЬОНОМ

В 1963 г. вышла монография Кнорозова «Письменность индейцев майя» с обширным каталогом иероглифов, автор

поместил туда и критический отзыв о работе новосибирских математиков. Вероятно, именно «колючие» внутренние академические отношения не позволили Юрию Валентиновичу достичь званий академика или члена-корреспондента. Вместе с тем он получал и премии, и государственные награды, а в 1977 г. был удостоен звания лауреата Государственной премии СССР. В официальной «Справке о творческом вкладе соискателя» его поставили рядом с Шампольоном. Свой лауреатский знак Кнорозов носил постоянно.

Крупных успехов в его научной карьере больше не случилось, хотя предпринимались достаточно эффективные попытки дешифровать письменность долины Инда, знаки острова Пасхи и другие древние тексты. При этом уже неизменно при анализе источников использовались и программы для ЭВМ.

В 1990-е годы Юрий Валентинович впервые посетил места обитания древних и современных майя — Гватемалу и Мексику (илл. 5).

Вероятно, в жизни Ю. В. Кнорозова, чьё столетие отмечается в 2022 г., были и другие значительные для него моменты, но главные события свершились уже в начале 1950-х годов.

«ОДНО ОБРАЗОВАНИЕ УМСТВЕННОЕ НЕ ДОВЕРШАЕТ ЕЩЁ ВОСПИТАНИЕ»

Н. И. ЛОБАЧЕВСКИЙ О ПРЕДМЕТАХ ВАЖНЕЙШИХ

Будущий 2023 г. объявлен годом педагога и наставника. Ранее российское правительство предлагало сделать его годом математики. В этой связи уместно вспомнить, что 1 декабря 2022 г. исполнится 230 лет со дня рождения известного организатора образования в России, математика и педагога Николая Ивановича Лобачевского.

«ВРЕМЯ ТОРЖЕСТВЕННОЕ ДЛЯ НАУК ТОЧНЫХ»

Николай Иванович родился в Нижнем Новгороде, но почти всю свою жизнь провёл в Казани. Там он учился сначала в гимназии, а затем в университете (1807–1811 гг.). После окончания университета был оставлен в нём для подготовки к педагогической деятельности, в 1816 году стал профессором. При жизни Лобачевский приобрёл известность именно как педагог и крупный организатор образования в России. А громкое мировое признание собственных научных достижений пришло гораздо позже его кончины.

Это была пора триумфа естественных наук и математики. В 1824 году со страниц популярного журнала «Вестник Европы» заявлялось следующее: «Кажется, настает время торжественное для наук точных и в нашем отечестве... Потребность математических знаний ощущается на всех путях службы; отличное уважение, знаки почестей, путь блистательный встречают каждого юношу, посвятившего труды свои сим занятиям».

В развитии российского образования Лобачевский принял весьма деятельное участие. Он был деканом физико-математического факультета (1820–1825 гг.) и ректором Казанского университета (1827–1846 гг.), а с 1845 г. до своей кончины в 1856 г. занимал ответственные посты попечителя и помощника

(заместителя) попечителя Казанского учебного округа, в который входили всё Поволжье от Астрахани до Вятки, Урал и Сибирь. Заметим, что со временем на всех перечисленных должностях Н. И. Лобачевского заменял или замещал Пётр Иванович Котельников — дед великого создателя радиосвязи Владимира Александровича Котельникова, уроженца Казани. Административная деятельность Лобачевского положила начало процветанию и славе Казанского университета.

Мы имеем возможность узнать здесь, в некотором смысле от самого Николая Ивановича, что он считал важным и для наставников, и для воспитанников.

РЕЧЬ О ВАЖНЕЙШИХ ПРЕДМЕТАХ ВОСПИТАНИЯ

Прочитанная в торжественном собрании Университета ректором оного, профессором Лобачевским 1828 г., июля 5-го

[1]¹ Вот уже год прошёл, любезные мои товарищи, как по избанию вашему несу я на себе должность, которой почести, важность и трудности служат доказательством лестной вашей ко мне доверенности. Не смею жаловаться на то, что вы захотели отозвать меня от любимых мною занятий, которым долгое время предавался я по склонности. Вы наложили на меня новые труды и чуждые до того мне заботы; но я не смею роптать, потому что вы предоставили мне новые средства быть полезным. Я принял ваш вызов, потому что уважал вашим мнением; потому что не хотел противиться общему желанию; потому что сам первый не мог оправдать того, кто на моём месте

вздумал бы отказаться. Наконец, выбор ваш утверждён был государем императором, и обязанности нового звания сделались для меня священными.

Пусть справедливо могу жаловаться на слабость сил моих и способность; но могут ли недостатки извинять меня, когда ревность к службе должна вознаграждать их? И мне ли не чувствовать усердия при тех счастливых обстоятельствах, в которых мы теперь находимся, которых начало заключается в общем источнике благоденствия России, в которых Университет исключительно за себя обязан благодарности щедрому монарху, исполнителям его воли, неусыпным попечениям ближайшего нашего начальника.

Итак, всё, чего бы желать надобно, наконец дано. Спрашивается, мы всё ли исполняли, что от нас требовалось? Вот как трудно мне успокоить мою совесть, когда я обращаюсь мыслями на первый год моего управления делами Университета. Вот как трудно мне в первый срок давать отчёт за себя, за весь Университет; надеяться на одобрение моих товарищей; родителей, которых дети воспитываются в сём заведении; всех посетителей, которые пришли быть судьями в общем деле и могли бы справедливо быть строгими судьями.

Пусть этот протёкший год дозволено мне будет называть годом испытания, желал бы следующий иметь право назвать годом исполнения и последний в трёхлетию — годом торжества моего.

Я сравниваю теперь себя с кормчим, который, не доверяя опытности, держался берегов; наконец, решается плыть в открытое море, и не робкое путешествие своё рассказывать, но советов просить должен. В воспитании юношества, в сём важном деле, где я по званию своему участвую более других членов Университета, в исполнении

¹ Нумерация, использованная в первом и последующих изданиях Речи Н. И. Лобачевского.

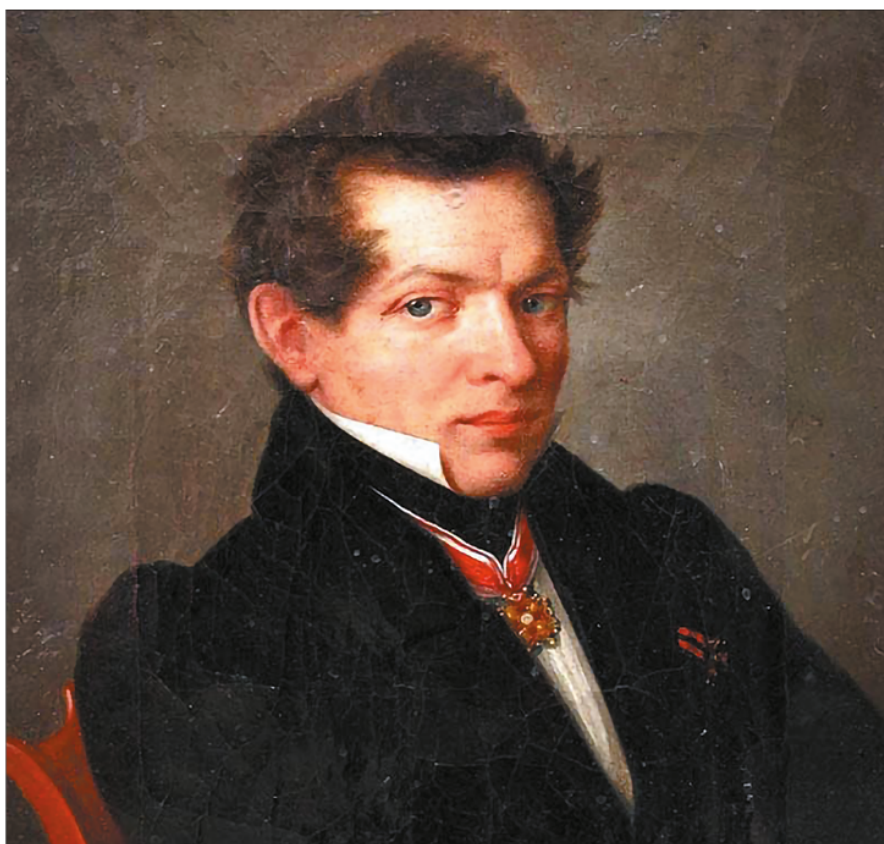
сей важной обязанности прошу ваших советов. Осмеливаюсь подвергнуть вашему суждению мои мысли, полагая, что они заключают в себе первые основания нравственности и могут указывать на те правила, которым следовать обязаны наставники. Ими намерен и я руководствоваться, как путешественник, чтобы не сбиться с пути, смотрит на приметы, расставленные по дороге.

[II] В каком состоянии, воображаю, должен бы находиться человек, отчуждённый от общества людей, отданный на волю одной дикой природе. Обращаю потом мысли к человеку, который среди устроенного, образованного гражданства последних веков просвещения высокими познаниями своими составляет честь и славу своего отечества. Какая разность, какое безмерное расстояние разделяет того и другого. Эту разность произвело — воспитание. Оно начинается от колыбели, приобретает сперва одним подражанием, постепенно развёртывается ум, память, воображение, вкус к изящному, пробуждается любовь к себе, к ближнему, любовь славы, чувство чести, желание наслаждаться жизнью. Все способности ума, все дарования, все страсти, всё это обделывает воспитание, соглашает в одно стройное целое, и человек, как бы снова родившись, являет творение в совершенстве.

Наружный вид его, возвышенное чело, взор, который всюду устремляется, всё созерцает вверху, вокруг себя; черты лица, в которых изображается чувственность, покорённая уму, — всё показывает, что он родился быть господином, повелителем, царём природы. Но мудрость, с которой он должен править с наследственного своего престола, не дана ему от рождения: она приобретается учением.

В чём же должна заключаться эта мудрость? Чему должно нам учиться, чтобы достигнуть своего назначения? Какие способности должны быть раскрыты и усовершенствованы, какие должны потерпеть перемены; что надобно придать, что отсечь, как излишнее, вредное?

Моё мнение: ничего не уничтожать и всё усовершенствовать. Неужели дары природы напрасны? Как осмелюсь осуждать их? Кого обвиним в них? Однако признаем виновника всему, что ни существует; исповедуем Его



Портрет Н. И. Лобачевского, 1839 год (художник Л. Д. Крюков)

и благоводем пред Его бесконечную премудростию.

Всего обыкновеннее слышать жалобы на страсти, но как справедливо сказал Мабли: чем страсти сильнее, тем они полезнее в обществе; направление их может быть только вредно.

Что же надобно сказать о дарованиях умственных, врождённых побуждениях, свойственных человеку желаниях? Всё должно остаться при нём: иначе исказим его природу, будем её насиловать и повредим его благополучию.

Обратимся, во-первых, к главной способности, уму, которым хотят отличить человека от прочих животных, противопоставляя в последних инстинкт. Я не того мнения, чтобы человек лишён был инстинкта, который является во многих действиях ума, который в соединении с умом составляет Гений. Замечу только мимоходом, что инстинкт не приобретается; Гением быть нельзя, кто не родился. В этом-то искусство воспитателей: открыть Гений, обогатить его познаниями и дать свободу следовать его внушениям. Ум, если хотят составить его

из воображения и памяти, едва ли отличается нас от животных. Но разум, без сомнения, принадлежит исключительно человеку; разум — это значит известные начала суждения, в которых как бы отпечатались первые действующие причины вселенной и которые соглашают, таким образом, все наши заключения с явлениями в природе, где противоречия существовать не могут.

[III] Как бы то ни было, но в том надобно признаться, что не столько уму нашему, сколько дару слова, одолжены мы всем нашим превосходством перед прочими животными. <...> Им запрещено передавать друг другу понятия. Одному человеку предоставлено это право; он один на земле пользуется сим даром; ему одному велено учиться, изощрять свой ум, искать истин соединёнными силами. Слова, как бы лучи ума его, передают и распространяют свет учения. Язык народа — свидетельство его образованности, верное доказательство степени его просвещения.

Чему, спрашиваю я, одолжены своими блистательными успехами в последнее



Здание Казанского университета

время математические и физические науки, слава нынешних веков, торжество ума человеческого? Без сомнения, искусственному языку своему, ибо как назвать сии знаки различных исчислений, как не особенным, весьма сжатым языком, который, не утомляя напрасно нашего внимания, одной чертой выражает обширные понятия. Такие успехи математических наук, затмивши всякое другое учение, справедливо удивляют нас, заставляют признаться, что уму человеческому предоставлено исключительно познавать сего рода истины, что он, может быть, напрасно гоняется за другими; надобно согласиться и с тем, что математики открыли прямые средства к приобретению познаний. <...> Их указал нам знаменитый Бэкон. Оставьте, говорил он, трудиться напрасно, стараясь извлечь из одного разума всю мудрость; спрашивайте природу, она хранит все истины и на вопросы ваши будет отвечать вам непременно и удовлетворительно. Наконец, Гений Декарта привёл эту счастливую перемену и, благодаря его дарованиям, мы живём уже в такие времена, когда едва тень древней схоластики бродит по Университетам. <...> Здесь учат тому, что на самом деле существует, а не тому, что изобретено одним праздным умом. Здесь преподаются точные и естественные науки с пособием языков и познаний исторических. Здесь преподаватели разделяют между собою предметы, которыми всю жизнь свою занимаются, ещё с молодых лет почувствовав в себе охоту и некоторые дарования. Как

жалко, что истинному просвещению предпочитают суетные выгоды домашнего воспитания. Кто хочет образовывать своих детей для государства, тот должен прибегнуть к средствам, которые одно только государство в состоянии доставить; тот должен учить своих детей в общественных заведениях.

[IV] Одно образование умственное не довершает ещё воспитание. Человек, обогащая свой ум познаниями, ещё должен учиться уметь наслаждаться жизнью. Я хочу говорить об образованности вкуса.

Жить — значит чувствовать, наслаждаться жизнью, чувствовать непрестанно новое, которое бы напоминало, что мы живём. <...> Единообразное движение мертво. Покой приятен после трудов и скоро обращается в скуку. Наслаждение заключается в волнении чувств, под тем условием, чтобы оно держалось в известных пределах. Впрочем, всё равно, на весёлое или печальное обращается наше внимание. И возвраты к унынию приятны; и трогательные картины бедствий человеческих нас привлекают. <...> Весёлое и печальное, как две противные силы, волнуют жизнь нашу внутри той волны, где заключаются все удовольствия, свойственные человеческой природе. Или подобно реке она течёт в излучистых берегах: то разливается в лугах радости, то обмывает крутые утёсы горестных размышлений. Ничто так не стесняет сего потока, как невежество: мёртвою, прямою дорогою провождает оно жизнь от колыбели к могиле. Ещё в низкой доле

изнурительные труды необходимости, мешаясь с отдохновением, услаждают жизнь земледельца и ремесленника; но вы, которых существование несправедливый случай обратил в тяжёлый налог другим; вы, которых ум отупел и чувство заглохло; вы не наслаждаетесь жизнью. Для вас мертва природа, чужды красоты поэзии, лишена прелести и великолепия архитектура, незамысловата история веков. Я утешусь мыслью, что из нашего Университета не выйдут подобные произведения растительной природы; даже не войдут сюда, если к несчастью уже родились с таким назначением. Не выйдут, повторяю, потому что здесь продолжается любовь славы, чувство чести и внутреннего достоинства.

[V] Кажется, природа, одарив столь щедро человека при его рождении, ещё не удовлетворялась. Вдохнула в каждого желание превосходить других, быть известным, быть предметом удивления, прославиться и, таким образом, возложила на самого человека попечение о своём усовершенствовании. Ум в непрестанной деятельности силится стяжать почести, возвыситься — и всё человеческое племя идёт от совершенства к совершенству — и где остановится?

[VI] Другие обязанности отзывают и охлаждают стремление к славе. Срочное время поручено человеку хранить огонь жизни; хранить с тем, чтобы он предал его другим. Он живёт, чтобы оставить по себе потомство. Любовь к жизни — сильное побуждение во всех тварях, ты исполняешь высокую цель природы. Я переступил через вершину моей жизни, при первом шаге чувствую уже тяжесть, которая увлекает меня по отлогости второй половины моего пути. Всегда был я внимателен к явлениям организма; теперь не могу наблюдать, не могу говорить о них равнодушно. Покоится жизнь в зерне растения под охранительной пленю против враждебных стихий; но деятельность их, наконец, улучшает время и до того беззаботная вдруг пробуждается от сна. Тогда, с превосходством ещё сил, строит она орудное жилище против непрестанного нападения. Скоро, почувствовав неравный бой, помышляет о победе и скрывается в новом зерне. Вот краткое описание явления жизни в растении, животном и человеке.

Чем удержать это стремление к побегу изменяющей жизни? Как рано пробуждается оно, и как верно рассчитано бывает время. Посмотрите на этот прививок: он уже цветёт в первую весну. Органическая сила в нём предчувствует, что отчуждённый черен от родного дерева не долговечен, и что ей надобно спешить с плодами. Посмотрите на огородные овощи, когда холодные ночи грозят им скорым морозом: вдруг останавливают они рост свой, и зёрна в них спеют. Яблоко, тронутое червём, зреет ранее других и валится на землю. Так порок сокращает жизнь; так юноша созревает преждевременно, удовлетворяя ранним своим желаниям, и ложится в могилу, когда бы ему надобно цвести. Мы все живём вдвое, вчетверо менее, нежели сколько назначено природой. <...> Натуралисты, сравнивая время возрастания человека и животных, приходят к заключению: мы должны бы, говорят они, жить около 200 лет. Но увы, напрасно жизненная сила собирает питательные соки; их сожигает огонь страстей, снедают заботы и губит невежество. Пылкость нашего соображения, наше знание, всегда готовые воспоминания будят страсти и призывают желания не должные. Наставник юношества пусть обратит сюда внимание и постарается предупредить безрассудность молодости, ещё не знающей цены своему здоровью.

О, как бы расточительны мы были с нашей жизнью, если бы мысль о смерти ещё не стояла на страже. Где более света, там гуще тень: так всё премудро соглашено в мире. Животное следует слепо своему побуждению. Человек знает наслаждения, ищет их с выбором, уточняет их; но он не большим пользуется превосходством — он знает, чего бы лучше не знать, знает, что он должен умереть. <...> Смерть, как бездна, которая всё поглощает, которую ничем наполнить нельзя; как зло, которое ни в какой договор включить не можно, потому что оно ни с чем не идёт в сравнение.

Но почему же смерть должна быть злом? Мы живём одно настоящее мгновение; прошедшее всё равно, как бы ни существовало; с будущим — последует то же. Когда смерть придёт, тогда всё равно — сколько мы ни прожили. Мы повинемся гласу природы, не в силах будучи ему противиться; но собственно

для нас какая выгода, жить более или менее?

Будем же дорожить жизнью, покуда она не теряет своего достоинства. Пусть примеры в Истории, истинное понятие о чести, любовь к отечеству, пробуждённая в юных летах, дадут заранее то благородное направление страстям и ту силу, которые позволят нам торжествовать над ужасом смерти. <...>

[VII] Быть готову всякий час принести эту великую жертву требует от нас премудрость Творца, вложившего в человеческое сердце с любовью к себе и любовь к ближнему. Отсюда истекают все начала нравственности и предмет воспитания, к которому, как важнейшему, прихожу я к последнему и не хочу говорить о нём, как о науке. <...> Ещё можем обойтись без писанных законов, когда они начертаны в сердцах наших. Мы родимся с добродетелями, и совесть дана им в охранение. Примеры научают лучше, нежели толкования и книги.

[VIII] Вы, воспитанники сего заведения, вы пользовались сими примерами. Уверен, что вы отсюда донесёте любовь к добродетели и сохраните её вместе с благодарностью к вашим наставникам. Вы узнаете, и опыт света ещё более уверит вас, что одно чувство любви к ближнему, любви бескорыстной, беспристрастной, истинное желание добра вам налагало на нас попечение просветить вас ум познаниями, утвердить вас в правилах веры, приучить вас к трудолюбию, порядку, к исполнению ваших обязанностей, сохранить невинность ваших нравов, сберечь и укрепить ваше здоровье, наставить вас в добродетелях, вдохнуть в вас желание славы, чувство благородства, справедливости и чести, этой строгой, неприкосновенной честности, которая бы устояла против соблазнительных примеров злоупотребления, недостижимых наказанием.

Ещё вы не в состоянии дать истинной цены словам моим, и не вдруг опытность может вразумить вас. Теперь вступаете вы в свет; новизна и многообразие впечатлений не даёт места размышлениям. Но придёт время, когда на блеске настоящего вдруг явится прошедшее с обворожительною прелестью своего туска, подобно нежной затуманенной резьбе на ярком золоте, подобно отражённым предметам в

слабом зеркале вод; тогда лета воспитания, лета беззаботной юности со всеми невинными удовольствиями представнут в вашем воспоминании, как образ совершенного счастья, невозвратно потерянного. Тогда вашего товарища учения встретите вы как родного; тогда в разговоре о вашей юности с благодарностью будете произносить имена ваших наставников, признаётесь, сколько много они желали вам добра, и с торжеством друг другу дадите обещание следовать примерам, от нас слышанным.

[IX] Расставаясь с вами, что скажу вам самого поучительного? Вы счастливее меня, родившись позже. Из истории народов видели вы, что всякое государство переходит возрасты младенчества, возмужалости и старости. То же будет и с нашим любезным отечеством. Хранимое судьбою, медленно возвышается оно в своём величии. <...> Счастливейшие дни России ещё впереди. Мы видели зарю, предвестницу их, на востоке; за нею показалось солнце... Я всё сказал этим.

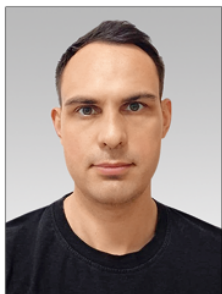
Эта речь была произнесена 35-летним Н. И. Лобачевским почти 200 лет назад.

АКТУАЛЬНАЯ И ПОНЫНЕ ПРОГРАММА ВОСПИТАНИЯ СТУДЕНТОВ

По современным мнениям педагогов, речь Н. И. Лобачевского, по существу, содержала в себе актуальную и поныне программу воспитательной работы университетского преподавателя со студентами. Конечно, каждый новый временной период добавлял и добавляет свои акценты и проблемы.

Здесь уместно обратить внимание на слова Николая Ивановича: «Одно образование умственное не довершает ещё воспитание». Ныне стали особенно актуальными и давние предупреждения академика Алексея Алексеевича Ухтомского, что просвещение и образование без нравственности более вредны для молодого человека, чем полезны, и могут привести его к духовному одичанию.

Вместе с тем на все времена остаётся задача всех причастных к педагогике: сохранить в студенчестве уверенность в своих силах и, подобно Н. И. Лобачевскому, надежду, что «счастливейшие дни России ещё впереди».



Александр ИГОНИН
эксперт BIS Journal

СКАЗКА О БОЛЬШОЙ КРАСНОЙ КНОПКЕ

Когда поднимаешься на ступеньку-другую вверх по корпоративной лестнице, начинаешь сталкиваться с различными вендорами и их предложениями. И с каждой ступенькой таковых становится всё больше, а предложения — всё красочнее и заманчивее. Оказывается, достаточно просто купить некую финтифлюшку за миллион чего-нибудь — и она, используя все последние достижения AI, ML, Big Data и блокчейна, одним махом делает так, что все проблемы решатся, цели — будут достигнуты, а KPI заколосятся и зазеленеют так, как ещё никогда не зеленели.

Сегодняшний автор этой колонки видел множество подобных презентаций, а некоторые из рекламируемых продуктов даже застал внедрёнными. И ни разу ещё не было такого, чтобы внедрение демонстрировало что-то хоть отдалённо близкое к обещанной рекламой картинке. Кровавому энтерпрайзу обычно требуется в лучшем случае год, чтобы чудо-продукт просто заработал, — а потом ещё год, а то и два,

чтобы завести в него нужные потоки данных, настроить логику работы и разобраться, что же теперь делать со всеми отчётами и оповещениями, которые он генерирует.

Когда слышишь речь очередного сейла, обещающего райские кущи, часто возникает труднопреодолимое желание в лучшем случае на него наорать, а то и вообще попросить его удалиться с помощью грубого физического воздействия. Из последних обещаний мне особенно запомнились:

- ♦ коробочка, которая может «целиком заменить аналитика SOC» на основе чудотворных ИИ-технологий;
- ♦ продукт, который полностью автоматически делает пентест всей сети компании и формирует по нему отчёт;
- ♦ платформа по поиску уязвимостей, которая не только все их находит, но ещё и автоматически патчит для любых ОС.

К сожалению, очень часто эти презентации демонстрируются высшему руководству потенциального заказчика в отсутствие на этой встрече его «технарей». А порой, в отчаянной попытке

заработать себе премию, недобросовестные сейлы идут на совсем уж сомнительный этический поступок. Так, недавно одному из руководителей высшего эшелона после полуночи пришло в мессенджере сообщение от ИБ-вендора, что их специалисты обнаружили серьёзнейшую уязвимость в веб-сервере

компании, требующую немедленного реагирования. После ознакомления с техническими деталями выяснилось, что уязвимость заключалась в не полностью корректно сгенерированном SSL-сертификате одного из публично доступных сайтов. Вещь, безусловно, неприятная, но уж точно не критическая и даже близко не смертельная. Зачем компании, продающей услуги, портить себе репутацию подобным низкопробным спамом в полночь — для меня настоящая загадка.

На фоне подобных безумных, непонятно на кого рассчитанных презентаций особенно ценны разговоры с коллегами, в которых рассказывают о реальном опыте, реальных сроках и реальных результатах. Например, я на днях услышал рассказ о внедрении SOAR: спустя полгода-год после начала проекта удалось автоматизировать около 30% планируемых задач. Вот это — реальные цифры, а не рекламное «через неделю наступило счастье».

Какой же из всего этого следует вывод? Решающей все проблемы Большой Красной Кнопки не существует, что бы там ни вещали вендоры. А значит, везде всё так же требуется долгая, кропотливая и не очень-то благодарная работа по построению комплексной системы защиты и (что ещё сложнее) поддержанию и развитию этой системы. Ну и, конечно, любимая наша автоматизация — но это уже совсем другая история.



PT NAD найдет хакера в вашей сети



РАССЛЕДОВАНИЕ АТАК

АНОМАЛИИ

СЕТЕВЫЕ УГРОЗЫ

ptsecurity.com

То, что так ждет ваш SOC

PT NAD 11 находит [аномалии]
и скрытые угрозы в сети





Kaspersky OT CyberSecurity

Прочный сплав технологий и экспертизы
для защиты промышленной инфраструктуры

kaspersky BRING ON
THE FUTURE

© 2022 AO Kaspersky Lab.
Registered trademarks and service marks are the property of their respective owners.

