BIS JOURNAL

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА

№4 (55) 2024

Сергей ЛЕБЕДЬ
Сбер
Ледокол российского кибербеза
→ 50

Денис БАТРАНКОВ
ИКС Холдинг
Путь к NGFW
→ 4

Парад NGFW → 4

Технологии SOC → 56

Илья ШАРАПОВ
Компания ТСС
Отечественные средства сетевой защиты. Обзор
→ 38

Ильназ ГАТАУЛЛИН
МТС RED SOC
Рост числа заказчиков в два раза. Почему?
→ 62


СЕТЕВАЯ ЗАЩИТА
ОТ МТС RED
Не ограничивайте
потребности — расширяйте
возможности
01
ngfw.mts.red
Рекламодатель ООО «Серенити Сайбер Секьюрити»

Сергей ПАЗИЗИН
научный редактор
BIS Journal

Ориентируясь на потребности читателей, редакция журнала приняла решение: в каждом номере всесторонне рассматривать одну из наиболее актуальных практических задач информационной безопасности. В настоящее время это, безусловно, импортозамещение межсетевых экранов нового поколения (NGFW).

Наша цель — рассказать об основных проблемах, особенностях подходов и применяемых технологических решениях при разработке межсетевых экранов нового поколения. Мы познакомим заказчиков с возможностями отечественных NGFW и планами по их развитию, подходами к тестированию и выбору оптимального решения.

Обсуждение темы в очном формате мы продолжим на ключевой конференции по сетевой безопасности 9 декабря в Москве, организованной Медиа Группой «Авангард».

Осенью этого года также пройдут две конференции, связанные с противодействием кибератакам: SOC Tech, посвящённая выявлению, противодействию и минимизации последствий инцидентов ИБ, используемым техническим средствам и организации работы центров мониторинга информационной безопасности, и SOC Forum, который в этом году «расширит рамки своей традиционной тематики Security Operations Center и будет посвящен комплексной кибербезопасности — Security Opportunities and Challenges».

Учитывая указанные события и актуальность темы противодействия кибератакам, в данном номере мы рассмотрим нюансы взаимодействия заказчиков и коммерческих SOC, расскажем об основных этапах адаптации под требования заказчика и настройке SIEM, инструментах выявления киберугроз.

BIS JOURNAL
ИЗДАЁТСЯ С 2010 ГОДА

УЧРЕДИТЕЛЬ-ИЗДАТЕЛЬ
ООО «Медиа Группа „Авангард“»
Адрес: 127473, Россия, Москва, 3-й Самотечный переулок, д. 21
Тел.: +7 495 921 42 44
Интернет-версия: ib-bank.ru/bisjournal
E-mail: bis@ib-bank.ru

Зарегистрирован 13 августа 2010 года Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзором) как «BIS Journal — Информационная безопасность банков».

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

Подписан в печать 27.09.2024. Тираж 7000 экз.
Цена договорная. Отпечатан в типографии «Московский Печатный Двор», 123298, г. Москва, 3-я Хорошевская 18, корп. 1, офис 201А

 16+

ТЕМА НОМЕРА. ПАРАД NGFW

ЧЕЛОВЕК НОМЕРА

ТЕМА НОМЕРА — 2. ТЕХНОЛОГИИ SOC

РЕГУЛЯТОРЫ

ИНФРАСТРУКТУРА

ЗА РУБЕЖОМ

УГРОЗЫ И РЕШЕНИЯ

СУБЪЕКТЫ

ПУТЬ К NGFW

Денис БАТРАНКОВ
директор по продуктам ИБ ИКС Холдинг

Течёт река жизни… Если оглянуться назад, в 90-х годах, когда в России только утверждался интернет, сетевая безопасность развивалась исходя из появляющихся у компаний задач. Постепенно развивались функции маршрутизации, стали появляться лидеры рынка, придумывающие свои протоколы, которые потом брались всеми как стандарт. Потом умерли протоколы IPS/SPX и вышел на смену TCP/IP. Умерли физические подключения через коаксиальный кабель, и появились подключения через коммутаторы по витой паре…

ПОЯВЛЕНИЕ ПРОКСИ-СЕРВЕРОВ

Сначала скорости каналов были небольшие, и первым сетевым устройством стал кеш-сервер, который скачивал популярные страницы и отдавал клиентам по запросу.

Затем появились задачи по подтверждению, что сайт тот самый, поэтому появился протокол SSL, который отдавал сертификат сервера, подписанный доверенным центром, и можно было проверить, что это тот самый microsoft.com, а не подменённый.

Потом появились задачи контролировать посещаемые категории сайтов. И появились первые движки, умеющие автоматически понимать категорию сайта и делать базу категорий, которую затем можно было использовать на своём прокси-сервере. И задача кеширования сайтов дополнилась задачей URL-фильтрации.

В процессе также выяснилось, что на сайтах бывает вредоносный код и эксплойты, и пришлось на прокси-серверах расшифровывать HTTPS-трафик и проверять антивирусами файлы, скачиваемые сотрудниками.

ПОЯВЛЕНИЕ STATEFUL INSPECTION И ALG

Затем появились функции сегментации сетей, первые пакетные фильтры и межсетевые экраны, позволявшие навести порядок между сегментами с разными политиками безопасности. Межсетевые экраны начали проверять заголовки пакетов в протоколах TCP, UDP, ICMP и принимали решение пускать только по разрешённым спискам адресов, портов и сервисов. Чтобы было удобнее писать правила, придумали stateful inspection, в котором для направленного от клиента к серверу пакета автоматически разрешались ответные пакеты. Выяснилось, что удобные для передачи данных и видео протоколы, такие как FTP или SIP, плохо работают через NAT, и стали появляться первые анализаторы приложений под названием Application Layer Gateway (ALG). Они меняли команды на уровне приложений, чтобы протокол работал через межсетевой экран. Например, параметры команды PORT в FTP. Да-да, уже тогда появлялись модули анализа приложений.

ПОЯВЛЕНИЕ IPS

В какой-то момент появились задачи обнаружения атак в сетевом трафике и первые системы обнаружения и предотвращения атак Intrustion Detection Systems (IDS) и Intrusion Prevention Systems (IPS).

Появились проблемы производительности. Выяснилось, что чем больше сигнатур проверяют трафик, тем больше нужно времени процессора на каждое сетевое подключение, и, соответственно, не на все подключения процессора стало хватать. Что делать?

Компания Internet Security Systems делает ход конём — создаёт модуль анализа приложений Protocol Analysis Module (PAM). Сначала он определяет, что за приложение генерирует трафик, и только потом проверяет в нём нужные сигнатуры, это ускоряет анализ.

Компании TippingPoint пришла идея использовать аппаратные ускорители, и появились первые аппаратные IPS с ускорителями.

ПОЯВЛЕНИЕ ПРОГРАММНО-АППАРАТНЫХ МЕЖСЕТЕВЫХ ЭКРАНОВ

Кстати, в 2000 году сменилась важная мировая парадигма: появились программно-аппаратные комплексы (ПАК) для защиты сети, внутри которых крутилась собственная ОС, и заказчики перестали сами инсталлировать системы защиты и системы управления к ним. Рынок достаточно долго привыкал к покупке ПАК вместо софта. Часть заказчиков до сих пор почему-то очень любит скачать дистрибутив и ставить его самостоятельно. Для таких любителей были придуманы virtual appliance. По сути, это софт, который можно запустить под гипервизором.

ШИРОКИЙ СПЕКТР СЕТЕВЫХ УСТРОЙСТВ

В итоге в какой-то момент в компаниях требовалось уже несколько устройств для защиты сети:

- прокси-сервер с URL-фильтрацией и антивирусом;
- антиспам;
- VPN-шлюз для удалённого доступа администраторов;
- VPN-шлюз для объединения филиалов,
- межсетевой экран;
- IDS или IPS;
- сканеры безопасности;
- нужное число систем управления всем этим!

И операторы переключались между консолями, чтобы понимать, что происходит в сети.

Как решение проблемы выступили устройства класса SIEM, в кото-

рые можно было отправить ещё и события с рабочих станций и серверов.

ПОЯВЛЕНИЕ УСТРОЙСТВ UTM КЛАССА «ВСЁ В ОДНОМ»

Следующим этапом на рынке стало появление многофункциональных устройств, где все функции были реализованы одновременно, а управление было единым для всего.

Это было экстремально удобно: можно в одной консоли увидеть события и межсетевого экрана, и IPS, и URL-фильтра, и других систем. Такие устройства назвали Unified Threat Management (UTM), что подчёркивало их ценность — единую консоль управления.

И снова появилась проблема производительности. Выяснилось, что имеющиеся серверы не могли на высоких скоростях выполнять все функции одновременно. Лидеры рынка придумывали всё новый и новый функционал, а включить его одновременно было невозможно. Что делать?

ПОЯВЛЕНИЕ NGFW

В 2007 году рынок взорвали устройства компании Palo Alto Networks. Компания решила сразу несколько проблем заказчиков:

- предоставила аппаратное устройство, где все функции можно было включить одновременно;
- решила проблему с визуализацией приложений на одном порту: по 443 и 80-му порту их ходят сотни разных;
- решила проблему с перемещением пользователей по разным IP-адресам: научились понимать, какой именно пользователь работает сейчас по данному IP-адресу;
- показала, что функционал GeoIP — хорошая штука;
- придумала, как писать правила по новым критериям: приложение, пользователь, страна;
- решила проблему с неизвестными вирусами в HTTP и FTP, предоставив сетевую песочницу в облаке;
- придумала цеплять профили безопасности к каждому правилу;
- реализовала сразу нужные сетевые функции.

Постепенно и другие компании реализовали этот функционал. Сегодня его называют Next-Generation Firewall (NGFW).

Постепенно мы привыкли к тому, что в одном устройстве находится всё: маршрутизация, VPN-шлюз, captive-portal, правила приложений и портов, IPS, URL-фильтр, инспекция SSL, антивирус, песочница, Threat Intelligence, инспекция приложений и туннелей, DLP.

При этом другая сетевая защита всё равно ещё работает на выделенных устройствах:

- Network Access Control (NAC);
- защита от DDoS;
- Web Application Firewall;
- Network Behavior and Anomaly Detecton;
- активные и пассивные сканеры безопасности.

ПОЯВЛЕНИЕ SASE И ZTNA

За это время NGFW стали развиваться в сторону Secure Access Service Edge (SASE), где уже NGFW предоставляется как сервис из облака. Более активно внедряли Zero Trust Network Access (ZTNA), где подключение по VPN не просто давало удалённый доступ, а ещё и клиент VPN проверял, что сам компьютер соответствует политике безопасности компании: там стоит нужный набор хостовой защиты — EDR, backup, DLP, обновления и нужные настройки. Всё активнее стали использовать SSL VPN, не требующий установки клиента. Также рынок стал пробовать использование технологии SD-WAN для балансировки работы сервисов между каналами на основе их качества.

ОБРУШЕНИЕ РЫНКА NGFW В 2022 ГОДУ

В 2022 году все поставщики такого оборудования прекратили свои подписки и Fortinet умудрился даже обвалить сервисы Ростелекома из-за остановки работы своих устройств на подписке.

Заказчики обнаружили, что им нужны российские аналоги. За два года с 2022 до 2024-й рынок российских NGFW прошёл большой путь. И сегодня в статьях этого журнала вы с ними познакомитесь.

ПОЧЕМУ NGFW СДЕЛАТЬ СЛОЖНО

Мне повезло самому участвовать в создании NGFW, и вот что я понял: тут недостаточно нанять программистов. Нужны сетевые инженеры, защищавшие сети. Только их понимание и опыт помогают аналитикам и программистам реализовать ровно те функции, которые нужны заказчикам.

Если посмотреть на историю компании Check Point, то она первооткрыватель, у неё было много гипотез, проб и ошибок. А когда ты делаешь продукт с нуля и точно знаешь, куда идёшь, то путь к результату получается понятным и быстрым. И ты точно попадаешь в потребности заказчиков.

Вторая сила компании-разработчика — эксперты, создающие сигнатуры атак и приложений, собирающих индикаторы компрометации, URL-категории. Чем больше у них насмотренность в атаках, тем лучше продукт будет защищать сеть. А поскольку Россия сегодня самая атакуемая страна, то и опыт защиты у нас самый большой.

Так что я считаю, продукты, которые мы сегодня создаём в России, скоро будут востребованы во всём мире.

КОНФЕРЕНЦИЯ ПО СЕТЕВОЙ БЕЗОПАСНОСТИ 9 ДЕКАБРЯ 2024 ГОДА

В нашей стране нужна отдельная конференция по сетевой безопасности, где все поставщики одновременно делятся своими новинками. ИТ- и ИБ-службы сегодня должны быстро разобраться в имеющихся предложениях, и поэтому мы сделали платформу, где можно будет поделиться инновациями, услышать мнение рынка и показать свои продукты. Это не только NGFW, но и песочницы, антиспам, поведенческие системы NDR, WAF, VPN, Anti-DDOS, NAC, MFA, балансировщики, устройства для тестирования и так далее.

Приходите 9 декабря 2024 года в Сокольники!

ГАРДА

Гарда NDR

Network Detection and Response

#детектируй #реагируй

Защитите свой бизнес от направленных атак и программ-вымогателей

Единый центр управления

Визуализация скрытых киберугроз

Расследование инцидентов

Вам нужен Гарда NDR, чтобы:

- выявить обход периметровых систем защиты и компрометацию учетных записей сотрудников;
- защитить сетевую инфраструктуру от zero-day атак с помощью искусственного интеллекта;
- выявить скрытые точки доступа в сеть, подключения к бот сетям и теневую ИТ-инфраструктуру;
- обеспечить безопасность при работе с подрядчиками;
- осуществлять проактивный поиск угроз;
- автоматически реагировать на выявленные угрозы;
- контролировать весь трафик, используя SPAN, GRE, TAP, сетевой брокер, NetFlow, IPFIX, ICAP;
- защищать без агентов IoT, Industrial IoT, SCADA и специализированные системы.

Смотрите видео с примером работы

Свяжитесь с нами:
info@gardatech.ru

* NDR, Network Detection and Response — обнаружение и реагирование на сетевые инциденты. ** Zero-day атаки — атаки нулевого дня.

Сетевая
Безопасность

[NGFW,WAF,NDR,VPN,ZTNA,Anti-DDOS,NAC,MFA]
netsec.ib-bank.ru

*когда?
09.12.2024

Конференция по сетевой безопасности

*где?
г. Москва, отель «Холидей Инн Сокольники»

Организатор
АВАНГАРД

ТРИ ЭЛЕМЕНТА ДЛЯ СЕТЕВОЙ БЕЗОПАСНОСТИ

Олег ХНЫКОВ
руководитель продвижения продуктов сетевой безопасности Positive Technologies

За последние два года, согласно аналитике Positive Technologies, количество кибератак увеличилось на 110%, и каждая третья из них была целевой. В топ-3 хакерских целей входят госучреждения, промышленные предприятия и финансовые организации, но статистика показывает, что с разной интенсивностью атакуют компании из всех отраслей.

Неужели на рынке не хватает решений для ИБ, которые позволяют эффективно противостоять злоумышленникам или хотя бы выявлять их присутствие до причинения ущерба? В этой статье разберёмся, как атакуют российский бизнес и какие средства защиты помогают предотвращать кибератаки.

КАК АТАКУЮТ БИЗНЕС

Обычно сначала хакеры проводят разведку и ищут потенциальные точки проникновения в компанию. Разведка бывает двух типов: пассивная и активная. К пассивной относятся поиск информации в публичном пространстве и даркнете, сбор доменных имён и данных о сотрудниках. К активным — сканирование периметра.

Окей, цели обозначены — пора выбрать техники атаки и осуществить проникновение. На этом этапе злоумышленники:

- взламывают сервисы на периметре (эксплуатируют уязвимости);
- рассылают фишинговые письма;
- взламывают Wi-Fi;
- получают доступ к устройствам с помощью украденной или скомпрометированной учётной записи;
- компрометируют цепочку поставок;
- компрометируют доверенную инфраструктуру (например, VPN).

Получив первичный доступ, хакеры расширяют присутствие внутри инфраструктуры с помощью следующих техник:

- закрепление;
- внутренняя разведка;
- повышение привилегий;
- перемещение внутри периметра;
- взлом ключевых систем.

Последний и самый важный этап — нанесение ущерба. К нему относятся:

- уничтожение данных и систем;
- кража данных;
- взлом целевых систем (кража денег, нарушение производственных процессов и другое).

Тщательно спланированная атака занимает от нескольких недель до нескольких месяцев. А значит, у службы безопасности достаточно времени, чтобы выявить угрозу и принять необходимые меры. Главное — понимать, какие инструменты способны с ней справиться.

КАКИЕ ИНСТРУМЕНТЫ НУЖНЫ

Если посмотреть на схему атаки, можно выявить общий знаменатель — сеть. Разберёмся, какие системы сетевой безопасности существуют на рынке.

Анализатор NetFlow — система для статистического анализа сетевого трафика. Выявляет базовые атаки по индикаторам компрометации и может обнаруживать аномалии сетевых узлов на основе машинного обучения. Однако стоит помнить, что выявление аномалий на основе статистики может создавать большое количество ложноположительных срабатываний, а для настройки ML-механизма нужны знания обо всех узлах в инфраструктуре. Система нетребовательна к аппаратной платформе и, как правило, применяется внутри сети.

WAF — межсетевой экран уровня веб-приложений, который обеспечивает защиту опубликованных сервисов на периметре от атак из списка OWASP Top 10 и WASC. Некоторые продвинутые WAF-решения включают защиту от DDoS-атак уровня L7.

NGFW — программно-аппаратный комплекс для защиты от сетевых атак, который разграничивает доступ пользователей к приложениям. Обычно такие устройства ставят на внешнем и внутреннем периметре для разделения сетевых зон и уменьшения площади атаки. Комплекс содержит модули безопасности (обычно IPS, потоковый антивирус и URL-фильтр), которые призваны не дать злоумышленникам проникнуть за периметр на высоких скоростях. При этом NGFW не собирает и не хранит данные и содержимое сессий.

Решение класса NTA (NDR) — система для обнаружения сложных кибератак и аномалий внутри сети методом поведенческого анализа. Под капотом таких систем — модули, правила и машинное обучение. Их задача — досконально анализировать внутренний трафик, разбирать протоколы до уровня приложений и искать следы хакеров. Они требовательны к аппаратным платформам, так как обрабатывают большой поток данных, собирают и хранят огромное количество артефактов и контекста, профилируют каждое сетевое устройство и находят отклонения от типичного поведения.

Песочница (sandbox) — решение, которое выявляет сложное вредоносное ПО, изучая подозрительные файлы в изолированной среде. Как правило, подключается к системам ИБ и ИТ через API или ICAP и может анализировать полученные от них

объекты. Но ключевая задача песочницы — блокировать в почтовом трафике ВПО, которое пропускают потоковые антивирусы.

Мы разобрались с видами систем и определили область применения каждой. Сосредоточимся на системах сетевой безопасности. Для этого вернёмся к циклу атаки и увидим, что на каждом этапе нужны определённые инструменты:

- **проникновение** — NGFW + песочница;
- **закрепление и продвижение** — NGFW + система NTA (NDR) + песочница;
- **развитие атаки и нанесение ущерба** — NGFW + система NTA (NDR) + песочница.

Теперь понятно, что для предотвращения всей цепочки кибератаки понадобится связка трёх продуктов. На первый взгляд, это избыточно, но, если копнуть глубже и посмотреть на сценарии применения, всё встанет на свои места (рис. 1).

Мы видим, что невозможно обнаружить и остановить кибератаку с помощью одной системы. Каждое средство защиты решает свою задачу, но вместе они могут выстроить практическую кибербезопасность — не позволяют реализовать целевую атаку на бизнес.

Сценарий	NGFW	Система NTA (NDR)	Песочница
Выявление целевых атак	Частично	Да	Да
Блокировка сетевых атак	Да	Да	Да (в связке с NGFW)
Проактивный поиск угроз	Нет	Да	Да
Выявление отклонений от типичного поведения узлов	Нет	Да	Нет
Расследование кибератак	Нет	Да	Да
Ретроспективный анализ	Нет	Да	Да
Фильтрация веб-ресурсов	Да	Нет	Нет

Рисунок 1. Сценарии применения трёх продуктов

ПОРЯДОК ВНЕДРЕНИЯ СИСТЕМ СЕТЕВОЙ БЕЗОПАСНОСТИ

Идеально, когда все системы сетевой безопасности внедрены, настроены и работают. Но далеко не каждая служба безопасности владеет нужным набором инструментов. Сейчас наведём порядок (рис. 2).

В первую очередь следует внедрить NGFW. Это базовое устройство, которое отделяет внутреннюю сеть компании от интернета. Политики безопасности настраиваются один раз и обновляются периодически, а значит, не нужно работать со средством защиты регулярно. Дополнительно NGFW устанавливают на границы

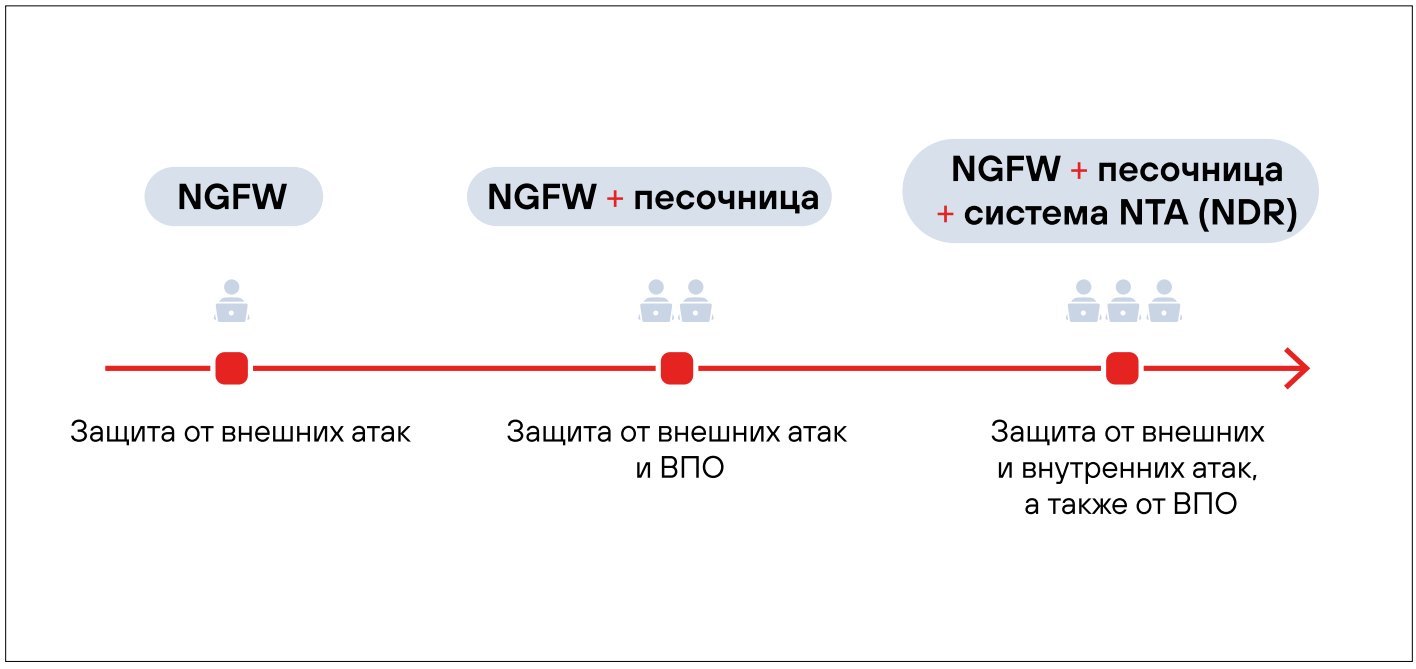
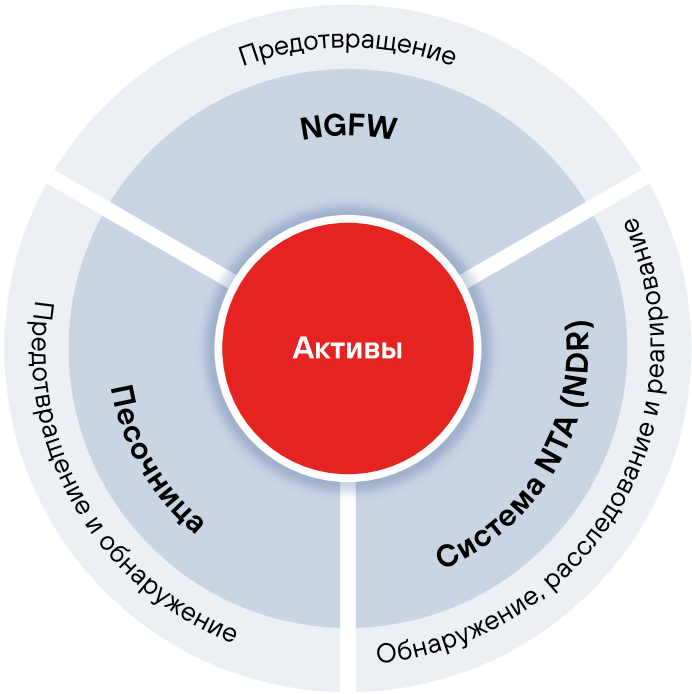


Рисунок 2. Этапы внедрения систем сетевой безопасности



РЕЗУЛЬТАТ СИНЕРГИИ ПРОДУКТОВ:

- полный контроль сети и отсутствие теневой инфраструктуры;
- защита периметра;
- макро- и микросегментация;
- защита от неизвестного ВПО и угроз нулевого дня;
- своевременное выявление ВПО;
- точное обнаружение хакеров внутри сети;
- выявление сетевых аномалий и отклонений от типичного поведения устройств;
- профилирование сетевых узлов;
- расследование сетевых атак и реагирование на них.

Рисунок 3. Синергия продуктов

сетевых сегментов со своим набором политик. Для управления системой понадобится один специалист.

Песочница внедряется второй. Она подключается к NGFW и параллельно устанавливается в разрыв сети на почтовый трафик. Для работы с двумя системами одновременно требуется несколько специалистов, которые будут защищать периметр и почту от сетевых атак и неизвестного ВПО.

Третий этап — внедрение системы NTA (NDR). Это решение подключается к коммутаторам доступа или ядра внутри сети либо к NGFW. Система получает от NGFW копию расшифрованного трафика для последующего анализа и выявления сетевых аномалий. Если во внутренних сегментах передаются файлы, решение извлекает их и отправляет на анализ в песочницу, а после получает вердикт. Система требует внимания службы безопасности, а значит, необходимо выделить специалистов, которые будут мониторить внутреннюю сеть.

Такая последовательность позволит навести порядок на периметре и внутри инфраструктуры, вовремя выявлять и блокировать целевые атаки, а также контролировать активность пользователей в корпоративной сети (рис. 3).

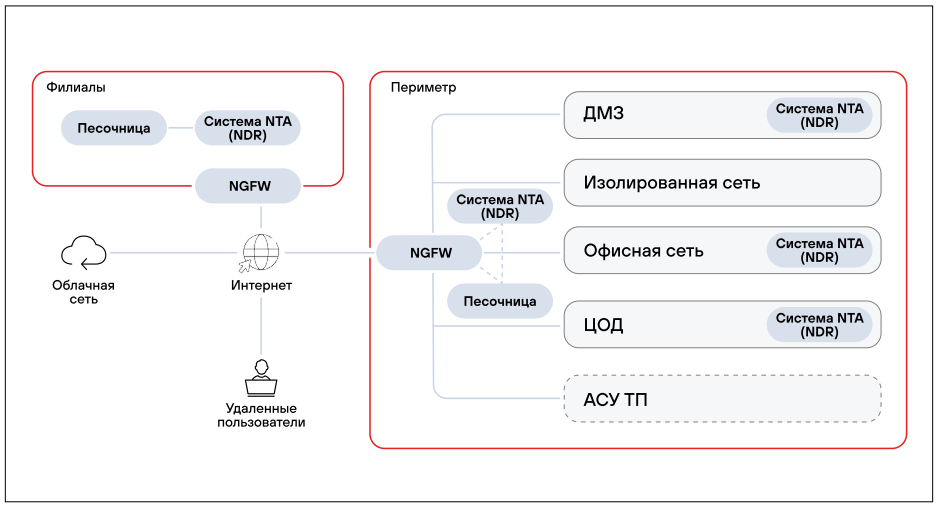


Рисунок 4. Рекомендуемые точки установки систем сетевой безопасности

ОСНОВЫ РАЗМЕЩЕНИЯ СРЕДСТВ СЕТЕВОЙ БЕЗОПАСНОСТИ

От правильного расположения систем в инфраструктуре зависит, насколько точно служба безопасности сможет противостоять атакующим. Рекомендуемые точки установки представлены на упрощённой схеме (рис. 4).

NGFW устанавливается на периметре сети и на границах сегментов (например, между ДМЗ и офисной сетью). К нему подключаются система NTA (NDR) и песочница. К ДМЗ, офисной сети и ЦОД рекомендуется подключать дополнительные сенсоры системы анализа внутреннего трафика. Для филиалов точки установки будут аналогичными.

ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ СИСТЕМ СЕТЕВОЙ БЕЗОПАСНОСТИ

Напоследок рассмотрим пример атаки и покажем, как защититься от неё с помощью продуктов Positive Technologies — PT NGFW, PT NAD и PT Sandbox (рис. 5).

С помощью вредоносного ПО хакер заражает рабочую станцию компании и получает к ней удалённый доступ. После этого осуществляет внутреннюю разведку, подбирает учётные данные (техника password spraying*) и TGT-билет для доступа к сервисам (Kerberoasting*).

Далее атакующий закрепляется на сервере СУБД и создаёт задачу в доменном контроллере, чтобы заразить максимальное количество устройств, включая устройства удалённых пользователей. Получив доступ к конфиденциальным данным, выгружает их в облачное хранилище, маскируя вредоносную активность под легитимные действия (рис. 6).

Теперь посмотрим, как будет выглядеть аналогичная атака с работающими системами безопасности.

PT NGFW в связке с PT Sandbox смогли бы предотвратить заражение рабочей станции вредоносным ПО. При передаче объекта по электронной почте PT Sandbox защищает пользователей в режиме inline. Если в инфраструктуре нет PT NGFW или PT Sandbox, обнаружить заражение рабочей станции и определить обратное соединение с узлом злоумышленника к злоумышленнику сможет PT NAD.

Кроме того, PT NAD однозначно выявит внутреннюю разведку, password spraying*, Kerberoasting*, перемещение внутри периметра и позволит быстро определить масштаб кибератаки. А PT NGFW не даст атакующим передвигаться между корпоративной сетью и ЦОД.

PT NAD определит создание задачи для массового заражения устройств, PT Sandbox — распространение вредоносного ПО, а PT NGFW — распространение задачи на удалённых пользователей.

На последнем этапе PT NAD обнаружит эксфильтрацию данных за периметр, а PT NGFW заблокирует угрозу в соответствии с политикой безопасности.

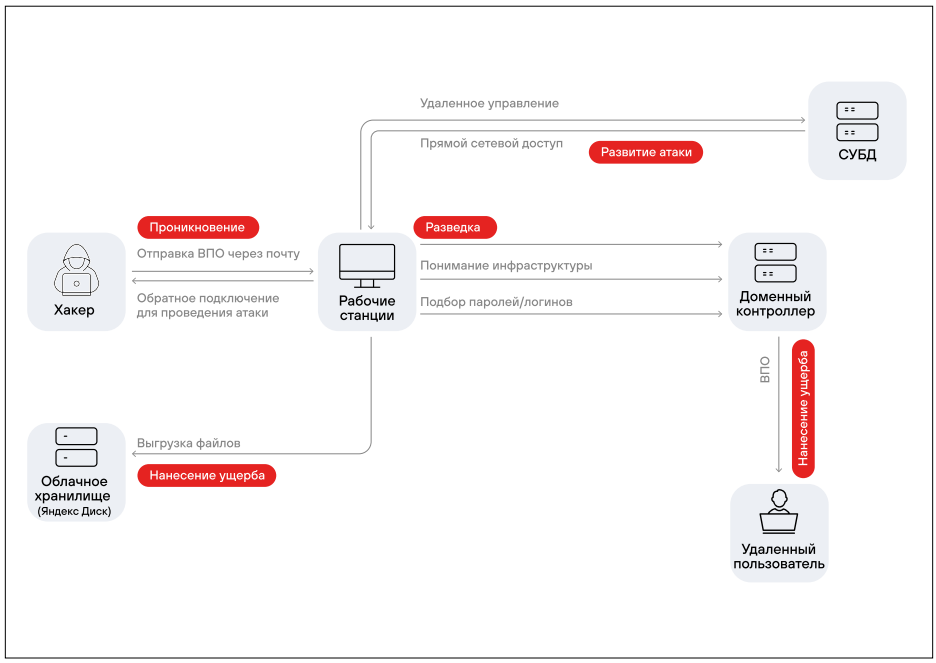


Рисунок 5. Цепочка атаки с причинением ущерба бизнесу

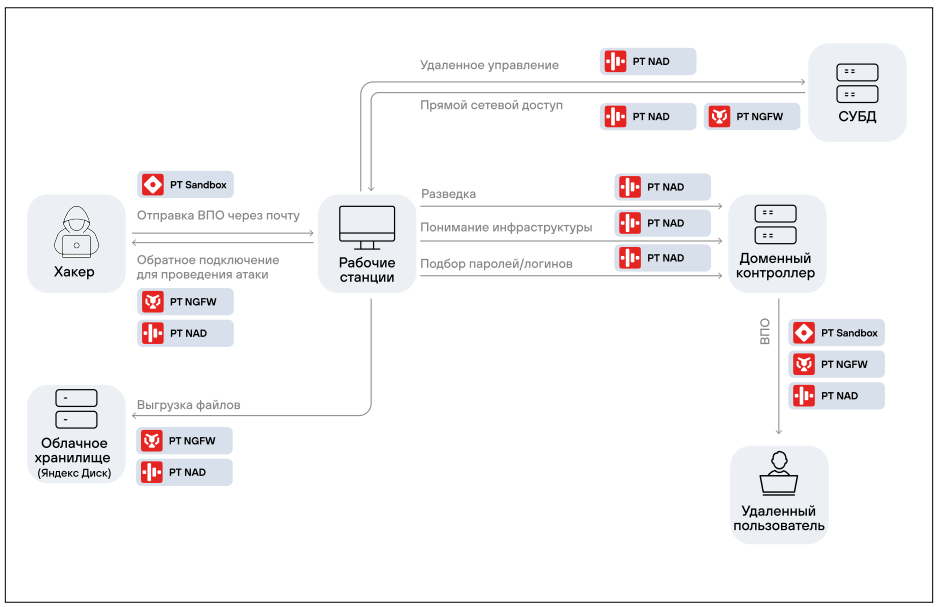


Рисунок 6. Применение инструментов сетевой защиты

ЗАЩИТА ОТ КИБЕРАТАК С ПОМОЩЬЮ ПРОДУКТОВ POSITIVE TECHNOLOGIES

Инструменты сетевой безопасности важны, особенно если у компании есть несколько филиалов и офисов. Продукты Positive Technologies тесно интегрируются друг с другом и покрывают практически все этапы кибератаки. PT NGFW и PT Sandbox позволяют предотвратить проникновение хакеров в сеть на периметре, PT NAD и PT Sandbox помогают вовремя увидеть развитие атаки и продвижение атакующих внутри сети. А объединение трёх продуктов защитит бизнес от целевых атак.

* Техника злоумышленников из матрицы MITRE ATT&CK

NGFW С ЧЕЛОВЕЧЕСКИМ ЛИЦОМ

Сергей ПЕТРЕНКО
директор продуктового портфеля MTC RED

Павел ГУСЬ
ведущий системный архитектор MTC RED

Российский рынок межсетевых экранов нового поколения (NGFW) — один из самых быстрорастущих сегментов отрасли кибербезопасности и при этом один из самых высококонкурентных. На данный момент он представлен более чем десятком решений от разных вендоров. Между тем отрасль отмечает растущий запрос на высокопроизводительные NGFW со стороны заказчиков. Так, согласно опубликованному в июле опросу MTC RED, 55% компаний — пользователей данного класса решений в качестве важных характеристик при выборе NGFW обозначили высокую скорость обработки трафика и масштабируемость.

Очевидно, что для создания таких сложных продуктов и управления ими необходимы специалисты со знаниями и опытом. В этой статье расскажем о том, какая команда осилит разработку подобных решений, а также о знаниях и опыте, необходимых для эффективного управления ими.

КТО НУЖЕН ДЛЯ СОЗДАНИЯ КОСМИЧЕСКОГО КОРАБЛЯ МОЩНОГО NGFW

Высокопроизводительный NGFW — это настоящий комбайн из различных ИБ и сетевых технологий. Такие решения невозможно создать только на программной основе, здесь нужна программно-аппаратная реализация. Значимых вендоров, которые ведут разработку NGFW как ПАК, сейчас в России не более десятка. Ещё меньше тех, кто создаёт своё решение полностью с нуля, не используя продукты, созданные ранее и немного для других целей. Такой native-подход имеет явное преимущество в виде отсутствия архитектурных и иных ограничений со стороны унаследованных технологий (legacy-кода). Но и требует привлечения большего числа специалистов для самостоятельной разработки.

Создание такого рода решений, как это ни банально звучит, начинается с формулировки образа идеального NGFW и чёткого определения аудитории, которой нужен новый продукт. Именно на старте надо определиться с концепцией будущего ПАК, при этом учтя текущие рыночные реалии — полностью российские или доступные open-source-технологии в основе, требования регуляторов к такого рода решениям, возможные технологические партнёрства, проблемы уже существующих продуктов на рынке, тренды развития мировых лидеров и многое другое. Здесь нужны глубокие знания технологий и рынка NGFW, носителем которых может быть как один человек — директор продукта, так и «коллектив авторов» в лице продуктовых менеджеров, а также специалистов по разработке, продажам и маркетингу.

Для создания и развития будущего NGFW не обойтись без двух ключевых ролей: продуктового менеджера — владельца продукта и технического руководителя команды разработки. Владелец продукта глубоко знает рынок: постоянно изучает рыночную аналитику, активность конкурентов, развитие технологий, понимает требования заказчиков, федеральных и отраслевых регуляторов, на основе чего формирует и в дальнейшем корректирует образ продукта с точки зрения конкурентоспособности. В свою очередь, технический руководитель воплощает запросы рынка и клиентов в продукте с помощью команды разработки. В целом для такого решения, как ПАК NGFW, достаточно одного владельца продукта и технического руководителя.

Под техническим руководителем выстраивается определённая иерархия ролей команды разработки. Часть из этих ролей выполняет свои задачи последовательно, передавая результаты работы по цепочке следующему звену. Другая часть работает

параллельно друг с другом, синхронизируясь на определённых этапах.

ОТ АРХИТЕКТУРЫ К РАЗРАБОТКЕ

Сформированный образ NGFW передаётся на проработку архитекторам, которые выстраивают структуру будущего решения. В отличие от владельца продукта или технического руководителя, архитекторов для такой сложной системы нужно несколько в соответствии с пулом используемых технологий. Ведь архитектор должен обладать глубочайшими знаниями того технического стека, на котором он специализируется. В случае с ПАК NGFW один архитектор займётся проектированием аппаратной платформы, другой — сетевой подсистемы ПО, третий — подсистемы безопасности.

Когда архитектура разработана, в процесс включаются системные аналитики: получая на вход архитектуру, они продумывают, как именно можно её реализовать. Цель системных аналитиков — превратить результаты труда архитекторов в набор задач, понятных разработчикам. Таких задач могут быть сотни. Кроме того, системные аналитики могут разделить структуру на модули и каждый из них описать в виде требований к разработке. Таким образом, большая задача создания решения декомпозируется на несколько параллельных веток разработки. В целом количество системных аналитиков коррелирует с числом архитекторов, но также зависит и от сложности продукта. Если продукт простой, то один системный аналитик может работать сразу над несколькими продуктами, но, поскольку ПАК NGFW очень сложное решение со множеством подсистем, здесь нужна целая команда, прорабатывающая разные части архитектуры.

Теперь в дело вступают разработчики. На 95% текущая разработка отечественных NGFW — это программирование, потому что российские вендоры сами не производят аппаратную часть своих решений. В некоторых случаях вендоры могут разрабатывать аппаратную архитектуру своих будущих NGFW, но производством микропроцессоров, аппаратных ускорителей и т.п. никто из них сам не занимается.

Сейчас общепринятая практика разработки подразумевает микросервисную архитектуру, когда решение не имеет одну большую монолитную структуру, а представляет собой набор микросервисов, которые параллельно разрабатывают разные команды, и эти сервисы объединены между собой лишь на уровне общей архитектуры и API. Так работает и команда разработки NGFW, в состав которой могут входить самые разные специалисты — от программистов на ассемблере до программистов на C++ и на более современных и популярных языках программирования, инженеры-программисты ПЛИС и другие. У каждой группы в составе команды разработки должен быть лидер (team-lead) — их число зависит от количества групп. А вот общее число разработчиков в случае с такими сложными системами, как NGFW, может колебаться от 20 до 100 с лишним человек.

В частных случаях, в зависимости от фокуса решения, в разработке NGFW могут присутствовать специфические роли. Например, SRE-инженер, если речь идёт о высоконагруженных платформах, или инженер-программист решений для АСУ ТП, если речь о промышленных системах.

БОЛЬШЕ ЗАДАЧ ДЛЯ РАЗРАБОТКИ

NGFW — это средство защиты информации, создание которого является лицензируемой деятельностью в России. Соответственно, для выполнения требований законодательства такой продукт подлежит обязательной сертификации во ФСТЭК России. Поэтому ещё на этапе разработки архитектуры ПАК NGFW к созданию решения подключаются специалисты по сертификации, которые анализируют, какие требования к функциональности средства защиты данного класса предъявляет регулятор, и определяют, как они будут реализовываться в коде и аппаратной платформе продукта. Таким образом, разработчики, помимо задач от системных аналитиков по реализации бизнес-функций решения, получают и задачи от команды сертификации по функциональности, необходимой для выполнения требований регуляторов.

Также ещё на этапе системного анализа сопровождать ПАК начинают технические писатели, которые создают пакет документации для решения. Технические писатели работают в связке с системными аналитиками и разработчиками: по мере того как аналитики формулируют требования к продукту, а разработчики их реализовывают, писатель отражает их в документации.

По мере готовности продукта технический писатель вручную запускает работу системы и, проходя все сценарии, описывает их в руководствах пользователя и администратора. По сути, в случае разработки средств защиты информации он уже не столько писатель, сколько универсальный технический специалист, который сам запускает продукт и проверяет его работу, иначе он не сможет её описать.

Помимо стандартного пакета документов (руководства пользователя, без которого продукт не может быть передан даже во внутреннее тестирование, регламента обновлений, паспорта продукта и прочих общепринятых документов), технические писатели разрабатывают и более сложную документацию для сертификации, в том числе по ГОСТ 19 и 34 серии и для сертификации во ФСТЭК (технические условия, техническое задание, паспорт на СЗИ и проч.) Одновременно с системными аналитиками, специалистами по сертификации и техническими писателями UX/UI-дизайнер создаёт интерфейс NGFW. Это может быть один специалист или несколько в зависимости от развитости системы. Он проектирует пользовательские сценарии и создаёт визуальный интерфейс для взаимодействия пользователя с решением. Затем интерфейс передаётся разработчикам для программирования его работы.

ОТ ТЕСТИРОВАНИЯ К СБОРКЕ

После того как группы разработки выпускают свои части кода, его забирают на тестирование и отладку тестировщики. Их задача — найти возможные ошибки в коде, а также несоответствия требованиям к продукту. После обнаружения ошибок код возвращается в разработку для исправления, и таких итераций может быть несколько. Некоторые критичные ошибки в коде могут иногда даже приводить к корректировке архитектуры решения. Численность тестировщиков напрямую зависит от количества работающих над продуктом программистов: в среднем на трёх разработчиков необходимо по одному тестировщику.

Параллельно с тестировщиками к проверке кода подключаются специалисты по безопасной разработке (AppSec и DevSecOps), чтобы выявить наличие уязвимостей в коде и также вернуть его разработчикам на устранение. Это обязательная часть создания любого ПО, которому необходимо пройти сертификацию. Далее ветки кода с устранёнными ошибками и уязвимостями собираются в единый код специалистами по DevOps. Они собирают на сборочном конвейере все части кода, компилируют и проверяют сборку на бесшовную работу.

И безусловно, невозможно выпустить продукт, не обеспечив его техподдержку, которая стандартно делится на первую, вторую и третью линии. Первая линия принимает заявки, вторая консультирует клиентов по настройкам решения и внедрению, а третья устраняет ошибки и уязвимости в продукте, а также сбои в работе оборудования по принятым замечаниям от заказчиков.

КТО НУЖЕН ДЛЯ УСПЕШНОГО УПРАВЛЕНИЯ ПАК NGFW

Вендор выпустил ПАК, компания-заказчик внедрила его в своей инфраструктуре. Теперь заказчику нужно выделить специалистов для работы с решением. Для управления ПАК NGFW минимально необходимо четыре сотрудника для анализа поступающей из системы информации в режиме 24×7: три человека — стандартная дежурная смена согласно требованиям законодательства и один — чтобы люди могли уходить в отпуск. При этом профессиональные навыки специалистов зависят от задач организации.

Если NGFW используется только для маршрутизации в сетях передачи данных, для управления им достаточно рядовых сетевых инженеров, которые есть в любой компании с развитой ИТ-инфраструктурой. Таким специалистам необходимо пройти короткий курс обучения основам управления ПАК от вендора, и этого достаточно для выполнения задач управления сетевой инфраструктурой: настройки взаимодействия между сетями и узлами сетей, каналов связи между ними и т.п.

В интерфейсе любого NGFW есть инструменты, которые отвечают за соединение определённых узлов сети и позволяют создавать разрешающие правила взаимодействия между ними. Через вкладки интерфейса можно создавать правила маршрутизации, осуществлять тонкую настройку мониторинга проходящего через оборудование трафика с целью выявления различных проблем, например конфликтов IP-адресов и проч. Это несложные задачи, с которыми отлично справятся сетевые инженеры: знаний в области информационной безопасности от таких специалистов не потребуется.

Если же ПАК NGFW используется в целях защиты от сетевых атак, в этом случае уже не обойтись без знаний в области информационной безопасности: понадобится как минимум умение читать логи, понимание, какие данные в них записываются и как на эту информацию реагировать; наличие знаний о технологиях IPS/IDS/SSL и множестве других.

Специалисты по кибербезопасности с помощью NGFW исследуют сам трафик — наличие в нём различного рода вредоносных запросов, признаков атак. Бывают ситуации, когда новое вредоносное ПО не детектируется NGFW: например, вендор решения не успел выпустить обновление, а от регулятора в компанию уже поступила рекомендация настроить средства защиты для блокировки угрозы. В таком случае ИБ-специалисту нужно самостоятельно создать в системе новое правило безопасности для её отражения. Или же, скажем, в компании используются NGFW от разных вендоров, и не на всех из них могут автоматически обновляться правила безопасности. В таких случаях ИБ-специалисту, работающему с NGFW, необходимо самостоятельно обновить правила на устройствах.

Эта работа подразумевает профессиональный уровень аналитика ИБ или специалиста по кибербезопасности. При таком сценарии предпочтительно деление сотрудников, работающих с NGFW, по профессиональным навыкам в сочетании два на два: пара высококвалифицированных специалистов по кибербезопасности — они в бэкграунде имеют базовые инженерные знания — и пара сотрудников среднего уровня со знаниями сетевых технологий.

ВЫВОДЫ

Теперь вы знаете о том, какая команда нужна для создания и управления современными высокопроизводительными NGFW. Однако порой мы сталкиваемся с заказчиками, у которых в целях экономии на управление NGFW выделен лишь один-два специалиста. В результате, отказываясь от мониторинга атак в режиме 24x7, такие компании повышают свои риски кибербезопасности. Кроме того, получается, что закупленный крутой ПАК не работает в полную силу, а, по сути, является роутером. Для таких клиентов выходом из положения может стать модель NGFWaaS, при которой администрирование и мониторинг установленного у клиента ПАК NGFW осуществляет сервис-провайдер. Это позволяет, растянув платежи, уложиться в бюджет и при этом получить круглосуточный мониторинг сетевых атак от сервис-провайдера без необходимости найма дефицитных специалистов в штат.

Kaspersky Anti Targeted Attack

Специализированная защита от целевых кибератак

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

kaspersky АКТИВИРУЙ БУДУЩЕЕ

kaspersky.ru/enterprise

ДиалогНаука

СИСТЕМНАЯ ИНТЕГРАЦИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

dialognauka.ru

НЕОЧЕВИДНЫЕ ВОПРОСЫ РАЗРАБОТКИ NGFW

КАК МЫ ФОРМИРУЕМ КОМАНДУ И ОБУЧАЕМ ПАРТНЁРОВ

Альберт МАННАНОВ
руководитель продукта Solar NGFW

Solar NGFW вышел на рынок в 2023 году, а в первой половине 2024 ГК «Солар» представила решение в программно-аппаратном исполнении. Разработка продукта такого уровня — это сложный и многокомпонентный процесс, который требует вовлечения множества специалистов самых различных областей компетенций. А значит, помимо технологических и организационных аспектов, необходимо учитывать и человеческий фактор — наём, обучение и удержание персонала.

Если перед вендором, который взялся разработать собственный NGFW, стоит задача разработать скоростное решение, стандартный сетевой стек Linux уже не подойдёт: он не разрабатывался для высокоскоростной обработки сетевых пакетов, а значит, требуется забрать часть или полную функциональность у ядра Linux.

«Солар» пошёл именно этим путём, так как наш ПАК ориентирован на потребности организаций enterprise-уровня, поэтому демонстрирует высокую производительность, от 5 Гбит/с в режиме NGFW до 75 Гбит/с в режиме межсетевого экранирования. Кроме стандартного набора IPS, используются уникальные сигнатуры от Solar 4RAYS для защиты от самых новых угроз, что даёт дополнительную нагрузку. И этот путь создания высокопроизводительной платформы в качестве основы Solar NGFW требует высокой экспертности нашей команды разработки. Рассмотрим ключевые навыки.

Архитектурная сложность NGFW повышает требования к многообразию и уровню компетенций инженера. Сформированная архитектура позволяет наращивать функциональность самого продукта, и на этом этапе подключаются аналитики, которые фиксируют требования к его возможностям. Аналитики должны сочетать в себе квалификацию ИБ- и ИТ-специалиста, иметь опыт и знания о принципах работы NGFW и в то же время понимать, как сформулировать требования для разработчиков: переводить с языка бизнеса на язык разработки.

Для NGFW, как и для любой высоконагруженной системы, задача тестирования стоит отдельным пунктом — это функциональные и нагрузочные тесты. QA-инженеры должны понимать ключевые метрики проверки качества NGFW, глубоко разбираться в сетевых технологиях и кибербезопасности. Навык разработки автотестов помогает повысить скорость и качество проверки, но с точки зрения формирования команды добавляется новая компетенция.

Реалии рынка и отрасли кибербезопасности ещё выше поднимают планку для вендора. К примеру, требования регуляторов периодически меняются, а значит, специалист должен постоянно адаптироваться к новым технологиям и методологиям. Как мы знаем на опыте внесения Solar NGFW в список Единый реестр отечественного ПО, сертификации компонентов и получения сертификата соответствия ФСТЭК России, безопаснику необходимо понимать не только функции решения, но и сам процесс обработки пакетов.

Часть требований к вендору NGFW выставляет непосредственно заказчик. Это техническая поддержка, которая работает по SLA, квалифицированные пресейлинженеры и инженеры внедрения. У них должен быть широкий кругозор во всех аспектах NGFW, ведь в ходе взаимодействия с заказчиками возникают вопросы как по части ИТ, так и по ИБ. Далеко не каждый специалист обладает таким багажом знаний, поэтому в правильном подходе должны быть предусмотрены разные уровни, от базового до пресейлов-экспертов, которых привлекают к сложным архитектурным запросам.

Итак, для успешной разработки NGFW нужна слаженная команда профессионалов с хорошими навыками по своей специальности и глубоким пониманием направления сетевых технологий и сферы информационной безопасности. Если говорить прямо, готовых специалистов с такой квалификацией просто нет. Поэтому в «Соларе» мы делаем ставку на подготовку собственных талантов и фокус на мотивацию и удержание сотрудников.

С начала года команда NGFW выросла втрое, и это не предел, потому что сейчас мы продолжаем разработку новых функций в соответствии с целями импортозамещения, с развитием сетевой архитектуры наших клиентов, с трендами отрасли. В 2025 году планируются очень

насыщенные релизы, включающие, например, полноценный remote access VPN и увеличение производительности до 100 гигабит в секунду в режиме межсетевого экрана с контролем приложений. Для выпуска новых функций в срок требуются дополнительные ресурсы, поэтому процесс развития компетенций в команде поставлен на рельсы. Расскажу о нашем опыте и подходах, которые позволяют эффективно и в срок решать задачи разработки и сопровождения продукта.

АДАПТАЦИЯ И КУРАТОРСТВО

В первые три месяца сотрудник должен понять, как и с какими задачами ему предстоит работать, к кому он может обратиться по тому или иному вопросу. Мы составили карту пути новичка, на которой обозначены ключевые точки — знакомство с людьми, процессами и задачами, обучение на практике, с помощью дистанционных курсов и погружения в базу знаний, калибровочные встречи в середине и конце испытательного срока. Сотрудники с самого начала видят карту этого пути, а в процессе получают напоминания о разных его этапах и пульсопросы.

Руководитель модифицирует план адаптации под конкретную роль или даже сотрудника, а затем контролирует его прохождение. В помощь руководителю есть чек-листы, гайды и даже курсы, например, по проведению встреч и предоставлению обратной связи. Это ёмкие, но подробные материалы с примерами вопросов и конкретными советами, которые помогают выстроить доверительные отношения и объективно оценить прогресс.

У куратора не менее важная роль: он оказывает эмоциональную поддержку, мотивирует и делится опытом на равных. Иногда новичок стесняется задать важные для него вопросы — про неписаные правила и порядки, реальную нагрузку, нерабочие активности и неформальное общение с коллегами. Куратор должен стать тем, к кому не страшно обратиться за помощью и советом, а также сам проактивно интересоваться, есть ли у подопечного вся нужная информация, оборудование и доступы, убеждаться, что он включён в процессы.

Со следующего года трек обучения как клиентов, так и партнёров станет неотъемлемой частью программы онбординга в наш продукт

В свою очередь, кураторам тоже нужна поддержка — не только материалами и чек-листами, но и в управлении временем, мотивации и балансе основной и дополнительной деятельности. Такой подход к адаптации требует многогранной и постоянной работы, но он того стоит: новые сотрудники быстро понимают, подходит ли им компания, плавно погружаются в работу и раньше начинают показывать результат.

ОБУЧЕНИЕ

Знакомство с компанией и задачами плавно перетекает в погружение в конкретный продукт, с которым предстоит работать. Например, новый аналитик NGFW начинает с того, что изучает концепцию создания и развития этого класса продуктов, а затем — конкретно Solar NGFW и Solar webProxy, на базе которого строился межсетевой экран нового поколения: их архитектуру и функциональные возможности, принципиальные различия двух классов. Параллельно сотрудник изучает основы сетевой безопасности по базовому онлайн-курсу. Следующий шаг — изучение дорожной карты продукта. Затем новичок изучает возможности Solar NGFW на стенде, для чего выполняет упражнение — самостоятельно разворачивает его на стенде на OpenStack.

Кстати, обучение мы проводим не только для своих сотрудников, но и для партнёров, а также для конечных пользователей — администраторов NGFW. Цикл обучения включает как основы сетевой безопасности, так и конкретные особенности Solar NGFW. Обучение заказчиков и партнёров проводится на базе авторизованного учебного центра, с прохождением тестирования и выдачей сертификатов. Сейчас мы запускаем первые группы, выстраиваем процессы, ставим их на поток. Со следующего года трек обучения как клиентов, так и партнёров станет неотъемлемой частью программы онбординга в наш продукт.

ШИРОКИЙ ВЗГЛЯД НА МОТИВАЦИЮ

Финансовые условия — неотъемлемая часть мотивации, но это далеко не единственный фактор принятия решения. Я верю и не раз убеждался на опыте, что для хорошего специалиста важно, какие именно задачи он решает, насколько они интересны лично для него и актуальны вообще, получает ли он профессиональное развитие на своём месте работы, есть ли ясный трек для роста.

NGFW хотя и не новый продукт, но яркий и известный, он сегодня в фокусе. Если говорить о Solar NGFW, то продукт развивается в графике с собственными прогнозами производства, его дорожная карта открыта клиентам, и мы находимся с ними в тесном контакте — исследуем их потребности и боли, собираем обратную связь, пожелания по функциональным возможностям, адаптируем решение под их сложившуюся архитектуру. Наша команда делает интересную и благодарную работу, и специалисты видят результат своего труда: на их глазах развивается продукт, который защищает крупнейшие компании ключевых отраслей, ложится в основу кибербезопасности инфраструктуры страны. Предлагая такую возможность, можно привлечь в команду людей, действительно увлечённых своим делом, и эта команда сможет разработать качественный продукт.

INFOWATCH ARMA СТЕНА (NGFW)

РЕАЛЬНЫЙ ОПЫТ ВНЕДРЕНИЯ НА СОБСТВЕННОЙ ИНФРАСТРУКТУРЕ, РЕЗУЛЬТАТЫ И ВЫВОДЫ

Стас РУМЯНЦЕВ
Product manager InfoWatch ARMA NGFW

Владимир САДОВНИКОВ
CTO InfoWatch ARMA

Если бы всего пару лет назад мы задали вопрос IT или ИБ-специалисту, какой NGFW лучше выбрать, все в один голос рекомендовали бы продукты иностранных вендоров. Эти решения созревали десятилетиями, были вне конкуренции по своим характеристикам и, как следствие, доминировали на российском рынке. Сейчас, когда переход на отечественные NGFW должен произойти в сжатые сроки, компаниям предстоит не только выбрать оптимальное решение под свои задачи, но и внедрить его на собственной инфраструктуре, причем так, чтобы не «положить» весь корпоративный трафик. На основе опыта внедрения собственного продукта InfoWatch ARMA Стена (NGFW) на инфраструктуре ГК InfoWatch рассказываем, как развиваются события, когда компания уже выбрала межсетевой экран и приступает к его пилотированию. Мы дадим рекомендации для заказчиков NGFW, какие важные моменты нужно учесть на старте, как сформировать список требований, какие шаги нужно предпринять для доработки и как на выходе получить рабочий продукт. Сегодня InfoWatch ARMA Стена (NGFW) защищает всю инфраструктуру ГК InfoWatch, а мы благодаря этому пилоту «прочувствовали» все этапы внедрения NGFW в двойном объеме как заказчик и как разработчик. Наш опыт будет полезен заказчикам любого NGFW, поскольку их ждут аналогичные вызовы, ведь большинство российских решений еще только проходит обкатку реальной практикой.

Созданием NGFW мы, как и большинство компаний на российском рынке, вплотную занимаемся последние несколько лет, при этом еще в 2019 году мы разработали и выпустили коммерческий релиз МСЭ для защиты промышленных сетей InfoWatch Industrial ARMA Firewall, который отлично зарекомендовал себя на рынке. То есть в разработке межсетевых экранов мы далеко не новички. На базе этого промышленного экрана была построена первая версия NGFW.

Владимир САДОВНИКОВ:

В 2022 году после ухода зарубежных производителей многие российские компании остались без защиты от кибератак, количество которых резко выросло, поэтому нам было важно предложить рынку рабочий вариант защиты сетевого периметра. Однако по мере разработки функциональности мы пришли к необходимости создания новой платформы для корпоративного NGFW — с новым уровнем производительности и широким набором опций, а значит и другой архитектурой.

При планировании разработки обновленной версии мы выделили для себя три крупных сегмента заказчиков, на которых стали ориентироваться прежде всего. Первые — те, кто уже имеют представление об NGFW, давно используют ведущие мировые решения и привыкли к высокому качеству сервиса, широкому набору функциональности. Теперь они ищут достойную замену этим продуктам — как в связи с регуляторными требованиями, так и из-за сложности с закупкой, обновлением лицензий, обслуживанием зарубежных межсетевых экранов.

Вторые — те, кто раньше закрывал задачи по защите сетевого трафика с помощью набора различных узкоспециализированных продуктов. Они выстраивали в своей ИТ-инфраструктуре некую цепочку ПО, чаще всего на базе Open Source, поддерживали ее во многом на энтузиазме администраторов. Теперь подобное решение не подходит им либо по причине регуляторных требований, либо из-за повышения рисков киберугроз, роста количества целевых атак, в том числе, на небольшие компании.

Третьи — те, кто уже приобрели российское решение NGFW, но по тем или иным причинам хотят дополнить его недостающей функциональностью, либо полностью поменять.

Очевидно, что обновленную версию нужно было собирать с учетом запросов и требований этих целевых аудиторий, ставить на пилоты и полученную экспертизу использовать для доработки продукта. Еще до начала внедрения внутри мы начали общаться с клиентами и партнерами на предмет того, какие функции межсетевых экранов им необходимы в первую очередь — здесь и сейчас. Мы проводили опросы с целью сформировать критически важный набор фичей, опрашивали специалистов, которые эксплуатируют решение и со стороны ИТ, и со стороны ИБ и постепенно верифицировали список требований. При этом мы помнили про ограничения по сертификации — ведь решение должно выполнять критически важные задачи существующих инфраструктур и для этого пройти сертификацию ФСТЭК.

В какой-то момент мы решили «съесть кактус» целиком и внедрить наш NGFW на инфраструктуру ГК InfoWatch в качестве основного решения. Этот переход также позволял нам отладить процесс технической поддержки продукта, провести эксплуатацию последней версии в рабочих условиях и предоставить в команду разработки максимально развернутый отчет о выявленных дефектах. Сейчас это звучит сильно упрощенно, но на практике все происходило гораздо сложнее. Внутреннее пилотирование оказало большое влияние на весь процесс разработки. Разработчики следовали старому принципу «Eat your own dog food», так как фактически они сами первыми сталкивались с результатами своего труда. Весь процесс внедрения можно разделить на несколько ключевых блоков:

- Составление ТЗ и требований
- Доработка
- Внедрение
- Техническая поддержка
- Выводы

СОСТАВЛЕНИЕ ТЗ: ТОРГ, КОМПРОМИСС И УРЕЗАНИЕ ТРЕБОВАНИЙ

В формировании ТЗ принимали участие департаменты ИТ и ИБ ГК InfoWatch, каждый из которых предоставил свой список требований. По факту эти списки представляли собой развернутый перечень возможностей иностранного NGFW.

Мы пошли от простого к сложному, не пытались встроить все известные на рынке фичи именно в текущую версию, планировали, что из функционала нужно прямо сейчас, какие возможности можно реализовать позже, а что и вовсе избыточно. Мы также ориентировались на акту-

альный гигиенический минимум, без которого не выживет ни одна сеть, на текущие потребности клиентов и функционал, который им нужен уже сегодня.

Таким образом у нас сформировалось несколько больших групп, в каждой их которых содержался ранжированный перечень требований:

- межсетевой экран
- система обнаружения вторжений
- сетевые функции
- мониторинг и события
- управление
- отказоустойчивость
- защита доступа
- VPN.

Процесс работы с требованиями двигался быстрыми темпами — месяц на обсуждение и «отсеивание» и еще три месяца на реализацию. В результате переговоров в строчках требований мы срезали более двадцати процентов, в смыслах и объемах работ получилось гораздо больше. Фактически от списка «хотелок» остался перечень конкретных функций.

Полный перечень возможностей InfoWatch ARMA Стена (NGFW):

Владимир САДОВНИКОВ:

Некоторые заказчики говорят нам, сделайте как у Check Point, а там еще более навороченный комбайн, еще более сложный маршрутизатор, еще больше протоколов, но не все это действительно необходимо. Давайте исходить из своих реальных потребностей, не нужно во всем ориентироваться на западные решения с их спецификой и более чем 50-летним опытом разработки. Не нужно искать цифры и показатели Cisco в отечественных продуктах, лучше оценить то, что реально нужно вашему бизнесу прямо сейчас.

ДОРАБОТКА: ПРОИЗВОДИТЕЛЬНОСТЬ И ФУНКЦИОНАЛЬНОСТЬ, КОТОРЫХ ДОСТАТОЧНО

Есть уровень требований, под который в любом случае придется подгонять продукт. В нашем случае доработка понадобилась, потому что мы используем специфические сервисы, такие как поддержка ActiveSync, Radius и другие. Помимо плановых работ во внутреннем пилоте выявилось много интересных моментов, о которых мы даже не подозревали.

Много усилий пришлось потратить на мелкие доработки, чтобы все «поехало», как надо. Каждый пункт из списка требований сначала тестировался внутри команды разработки, потом в команде ГК InfoWatch. Значительная часть времени ушла на внутреннюю коммуникацию и консультирование, так как поначалу было сложно воспринимать свою компанию как внешнего заказчика: все сидят в одном офисе и для решения срочного вопроса проще дойти до коллеги в соседний кабинет, вместо того, чтобы заводить тикет в CRM.

В контексте доработок продукта важно рассказать о скорости и производительности нашего решения, как мы двигались в этом направлении, к каким результатам и выводам пришли.

Сегодня мы производим NGFW в трех аппаратных конфигурациях: K10000, K1000 и K100. Все аппаратные платформы сертифицированы Минпромторгом и отличаются форм-факторами, количеством портов и пропускной способностью. Они отвечают запросам большинства коммерческих компаний на российском рынке — как сегмента средний бизнес, так и крупных. Как правило, в их распределенной инфраструктуре распространены сетевые интерфейсы 1 Гбит/сек и 10 Гбит/сек. К слову, в наших собственных сетях только в отдельных точках было 10 Гбит/сек, остальное все было гигабитное. Что касается интерфейсов 25 Гбит/сек или 40 Гбит/сек — это уже уровень дата-центров.

Недавно InfoWatch ARMA Стена (NGFW) успешно прошел независимое тестирование в формате vendor-agnostic в лаборатории «Инфосистемы Джет». По результатам тестов наше решение показало производительность 6,2 Гбит/с, что полностью отвечает требованиям корпоративного сегмента. На момент завершения тестов нашего NGFW, это был лидирующий результат среди российских решений, представленных в проекте.

Результаты тестов на странице спецпроекта «Инфосистемы Джет» по тестированию межсетевых экранов нового поколения:

Это был важный опыт тестирования продуктов с помощью ряда новых инструментов, мы получили обратную связь по сценариям работы и пользовательскому опыту, который используем для расширения функциональности и улучшения продукта по выявленным в процессе точкам роста.

Владимир САДОВНИКОВ:

Для нас ценность проекта заключалась в возможности протестировать работу нашего NGFW в лаборатории независимого интегратора с прозрачными условиями тестов и профилем трафика, а также оценить резуль-

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ INFOWATCH ARMA СТЕНА (NGFW)

- Стабильная скорость до 8 Гбит/с при 35000 правил IPS и 100 правилах МЭ (по результатам внутренних тестов InfoWatch).
- Скорость до 6,2 Гбит/с при 55000 правилах IPS и 200 правилах МЭ (по результатам независимого тестирования компании «Инфосистемы Джет»).
- В линейке — три аппаратные конфигурации NGFW: с производительностью 100 Мбит/сек, 1 Гбит/сек и 10 Гбит/сек.

таты относительно других игроков рынка, как это могут сделать заказчики на основе данных «Инфосистемы Джет»

ПОЧЕМУ NGFW ПОКАЗЫВАЕТ РАЗНЫЕ СКОРОСТИ?

Основная сложность тестирования заключается в том, что существуют очень разные сценарии использования. Результат, полученный во время тестирования в лаборатории «Инфосистемы Джет», показывает скорость, полученную во время атаки и при срабатывании практически всех правил, чего и требует методика. В реальной жизни мы можем написать гораздо больше правил и при этом получить еще более высокую скорость. Однако для написания правил межсетевого экрана нужна определенная топология сети, без которой получится только множество надуманных правил, которые никогда не отработают или же будут слишком однотипными, что также слишком отдалит синтетические тесты от реальных сценариев использования. Во время тестирования в “Инфосистемы Джет” мы получили скорость 6,2 Гбит/с, хотя на практике при таком же наборе правил у наших заказчиков и на наших собственных мощностях мы легко получаем скорость свыше 8 Гбит/с. Часто слышу вопрос, почему нельзя получить ровно 10 Гбит/с? Это априори недостижимая цифра, так как по мере включения большего числа правил и усложнения логики разбора трафика затрачивается ненулевое время на его обработку, что как раз съедает часть пропускной способности.

ВНЕДРЕНИЕ: ОЖИДАНИЯ И РЕАЛЬНОСТЬ

Пилоты обычно длятся несколько месяцев, при этом в процессе обкатки могут появиться различные проблемы и вопросы, частично их можно решить без дополнительной разработки за счет гибких настроек и изменения конфигураций. Сроки доработки тоже могут быть разными — от пары часов, когда нужно просто пересобрать цепочку настроек, до запросов на новую функциональность, работа над которой может длиться полгода.

Проблема, с которой мы столкнулись — наша большая сеть, в которой все «крутилось» на разном оборудовании, оказалась не готова к NGFW. Реальность и наши ожидания сильно разошлись. Тогда мы сделали первый тестовый контур ARMA, который на данный момент работает как полноценная тестовая альфа-лаборатория, куда выгружаются самые свежие версии, а во внешний контур уходят протестированные и более стабильные релизы.

Решение было запущено на гостевой сети Wi-Fi, мы получили большое количество обратной связи от коллег, и когда добились качественной работы NGFW на этом участке, то перенесли его на более крупный сегмент сети.

Владимир САДОВНИКОВ:

Весь корпоративный трафик проходит через наш продукт, включая видеозвонки, доступ к внутренним ресурсам, почту, VPN и т.д. Таким образом, разработчики не только создают продукт, но и активно используют его, проверяя производительность и функциональность в реальных условиях. При этом у них есть возможность убедиться в работоспособности пользовательских сценариев, корректности применяемых параметров безопасности, общей производительности и зафиксировать ошибки, которые могут возникнуть в процессе отладки.

Самым большим вызовом для нас на этом этапе было решиться на финальный переход. Все боялись «повернуть рубильник» и перейти в продакшн, хотя мы были готовы даже к максимально неприятному сценарию, что сеть ляжет на некий промежуток времени. Мы топтались на месте и теряли время, однако опасения не оправдались, и основные проблемы решились на тестовом контуре.

У всех компаний разные сети, их невозможно сделать одинаковыми и

Изобретен аппарат автоматического бритья:
— Бросаешь рубль, суешь туда голову, и он тебя автоматически бреет.
— Но ведь у всех разные лица?!
— До первого бритья — да...

предусмотреть все сценарии: разные сегменты и контуры, у кого-то подсети виртуальные, у кого-то под капотом legacy 20-летней давности. Для решения вопросов с доработкой продукта после внедрения отлично сработала связка инженеров поддержки, которые общались с заказчиком и командой разработки и связка команды разработки с инженерами с передачей обратной связи в заказчика. Когда все звезды сошлись и наладились процессы, у нас заработал конвейер поставки обратной связи, анализа и поиска решений с последующей доработкой фичей.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА, ПРОТЕСТИРОВАННАЯ НА СЕБЕ

Отсутствие качественной техподдержки может остановить любое пилотирование. Мы смогли выстроить процесс сервиса нашего продукта, его доработки и устранения дефектов за пару часов в том числе благодаря тому, что работали в буквальном смысле за одной "стеной": ИТ и ИБ служба выступали в роли заказчика, а отдел разработки отвечал за устранение неполадок, поставку фичей и поиск оптимальных конфигураций большого количества взаимосвязанных функций и сервисов.

Сейчас несколько раз в неделю мы обсуждаем новые запросы, все получают обратную связь по своим статусам и видят планы разработки, обмениваемся информацией о сроках установки фичей, оцениваем потребность в том или ином функционале. Мы тесно взаимодействуем со всеми участниками процесса из других департаментов и можем планировать свою нагрузку, заказ дополнительного оборудования, переезды инфраструктуры и другие активности. Мы не блокируем друг друга, а работаем в единой команде, и это позволяет нам продвигаться дальше.

С самого начала мы сделали упор на качественный сервис, скорость и оптимальность доработки, для этого пришлось внести изменения в CRM-систему, добавить в нее возможности, которые обеспечивают эффективную коммуникацию с заказчиком. Мы выстраиваем необходимую функциональность в продуктивном диалоге с клиентами и помогаем найти оптимальное решение даже в сложных случаях.

Владимир САДОВНИКОВ:

Мы работаем на уровне приоритетов, чтобы цель, которую мы преследуем, была закрыта. На этапе внедрения главной целью было — запуститься. На этапе, когда мы уже запустились и набили шишки, цель была устранить ошибки, чтобы коллеги могли продолжить тестирование.

ЧТО ДАЛЬШЕ?

Мы планомерно добавляем в NGFW пользовательские сценарии из перечня, который получился по итогам общения с внутренними и внешними заказчиками, и корректируем их по мере появления новых потребностей. По результатам пилотов наших клиентов валидируем полученные сценарии и технические требования и вносим в состав нашего решения.

До конца 2024 года мы расширим интеграционные возможности нашего продукта в части его взаимодействия с внешними SIEM-системами, консолью управления InfoWatch ARMA Management Console и линейкой и линейкой продуктов для защиты данных InfoWatch. Интеграция крайне важна, поскольку внедрение NGFW происходит на сформированной инфраструктуре и наш продукт должен качественно дополнять все ее элементы — например, обогащать SIEM-систему данными, управляться централизованно через привычный клиенту интерфейс, давать возможность реализации новых сценариев DLP.

Также мы продолжаем процесс сертификации программной части нашего продукта. До конца 2024 года мы рассчитываем получить от ФСТЭК подтверждение по типам профилей защиты Б и Д, а в следующем году — по типам А и ММЭ.

ВЫВОДЫ ПО РЕЗУЛЬТАТАМ ВНУТРЕННЕГО ПИЛОТА

1. Компании, которая решила поставить у себя NGFW, нужно обязательно готовить к этому свою ИБ-службу: пересматривать правила, которыми они закрывали безопасность сети, и адаптировать их под новое решение. ИБ-специалистам должно быть удобно работать с новым инструментом.

2. Не стоит ориентироваться на абстрактные цифры по производительности из тендерных заданий. Лучше оценить реальные показатели, которые поддерживают ваши сети и сетевые карты, а также скорости ваших устройств.

3. Даже при наличии типовых сценариев универсального NGFW нет и не может быть. Сегменты сети в каждой организации разные, и нагрузка в отдельных сегментах распределяется по-разному. В одном из наших пилотных проектов у заказчика из промышленного сектора не оказалось единой точки входа трафика, и мы после долгих совместных поисков нашли наиболее критичные места: две точки с кластерами, где реально проходил трафик 10 Гбит/сек, и две без кластеров — чуть менее важный сегмент с трафиком до 100 Мбит/сек. Это хороший пример того, как у одного клиента для закрытия его потребностей были применены сразу несколько продуктов нашей линейки.

И, наверное, самый общезначимый вывод:

Продукты и рынок отечественных NGFW находятся практически в начальной стадии, и сейчас у бизнеса есть отличная возможность принять участие в развитии этого сегмента под российские реалии. Это win-win процесс, когда и разработчики, и заказчики совместно обогащают продукт и развивают отрасль в целом.

ТЕХНОЛОГИЧЕСКИЕ ПАРТНЁРСТВА

ИЛИ КАК ПОЛУЧИТЬ МАКСИМУМ ОТ NGFW

Дмитрий ЛЕБЕДЕВ
ведущий эксперт отдела продвижения продуктов «Кода Безопасности»

Спустя два года после ухода зарубежных ИБ-вендоров из России отечественные производители смогли заместить иностранные решения во многих областях. Но в ряде сегментов, например Межсетевых экранов нового поколения (NGFW), ещё есть над чем работать.

Сегодня NGFW особенно актуальны, поскольку защищают ИТ-инфраструктуры крупных организаций, относящихся к государствообразующим. Спрос на NGFW поставил российских ИБ-вендоров перед сложным выбором:

1. Развивать продукты для задач вне NGFW. Недостаток: *отвлечение ресурсов для развития NGFW, востребованного в текущих реалиях.*

2. Концентрация только на NGFW. Недостаток: *слабая зрелость решения для задач крупных заказчиков.*

Также выяснилось, что каждый вендор хорош в отдельных сегментах кибербезопасности: у одного NGFW работает стабильно, но не очень функционален, у другого — в решении есть множество защитных механизмов, но нет централизованного управления. А ведь именно комплексность и сбалансированность — одно из главных преимуществ NGFW как продукта.

В итоге оптимальным решением оказалось создание технологических партнёрств с различными ИБ-компаниями. Так, вендоры могут объединить лучшие наработки в рамках одного продукта, а крупные заказчики получают NGFW с необходимым функционалом.

КИБЕРАЛЬЯНС

Следуя этой логике, «Код Безопасности» создал КиберАльянс — комплекс технологических партнёрств с вендорами-лидерами разных ИБ-

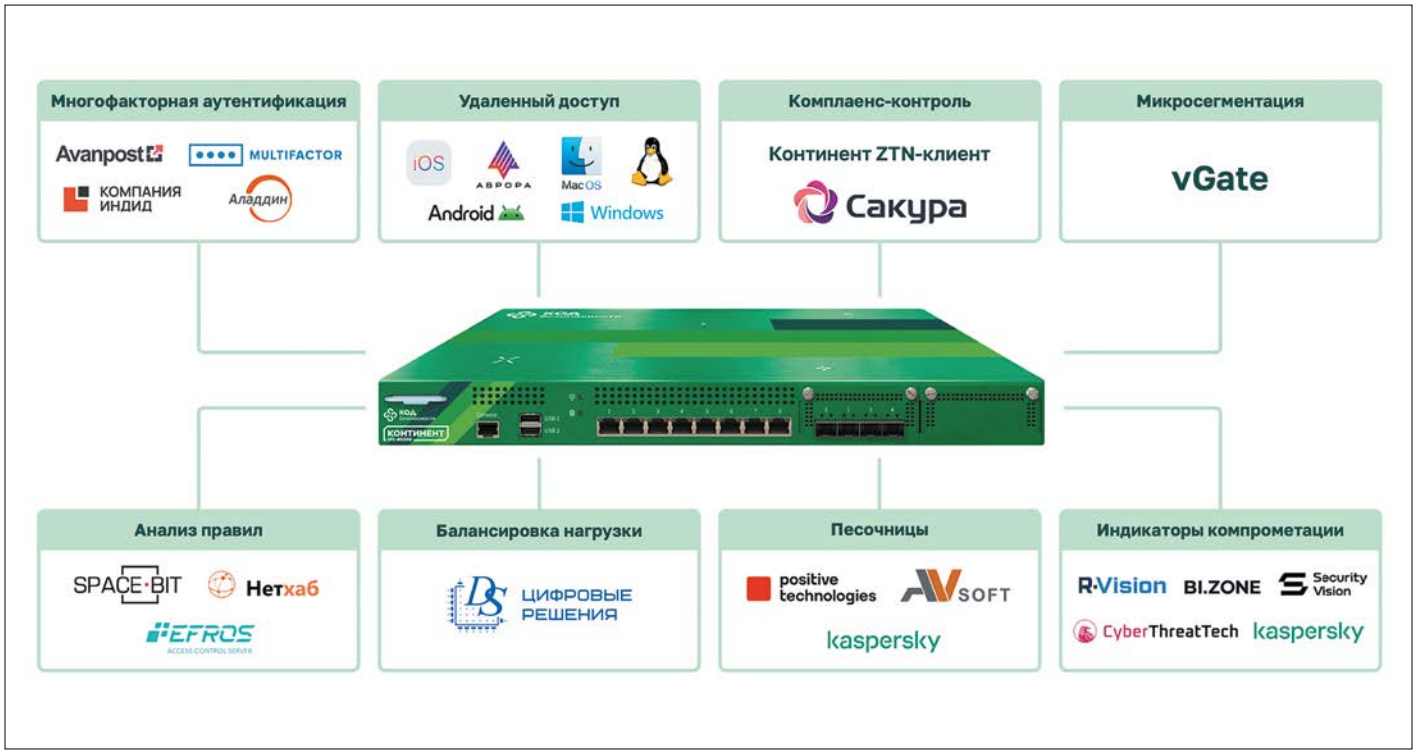


Рисунок 1. Ядром КиберАльянса выступает NGFW «Континент 4» от «Кода Безопасности», вокруг которого формируются контуры защиты

сегментов. Ядром выступает NGFW «Континент 4» от «Кода Безопасности», вокруг которого формируются контуры защиты (рис. 1).

На примере «Континент 4» мы разберём, в каких именно направлениях вендоры NGFW могли бы наращивать совместную экспертизу. В «Коде Безопасности» мы видим **три ключевых сегмента:**

1. Защищённый удалённый доступ.
2. Интеграция с инфраструктурными сервисами.
3. Расширенная безопасность.

ЗАЩИЩЁННЫЙ УДАЛЁННЫЙ ДОСТУП

В этой сфере существует две основные проблемы. Первая: для подключения к корпоративным ресурсам удалённые сотрудники используют личные устройства, которые порой слабо защищены. Вторая — использование незащищённых каналов связи. Без шифрования хакеры могут перехватить трафик, а ведь в нём передаются критичные данные.

Чтобы организовать безопасный удалённый доступ, необходимо следовать трём правилам:

- шифровать трафик;
- контролировать трафик от удалённых пользователей механизмами безопасности;
- безопасно аутентифицировать пользователей.

Выполнить первый пункт на NGFW легко — с помощью организации VPN-туннеля. А вот контроль трафика и аутентификация доступны не во всех продуктах, но это можно решить несколькими способами.

Разграничение доступа

Необходимо определить политики для VPN: какой пользователь на какой корпоративный ресурс, по каким протоколам может подключаться. Притом что корпоративные ресурсы бывают разные: к одним нужен постоянный доступ, к другим — только в определённое время. «Код Безопасности» видит три подхода организации политик удалённого доступа:

1. Стандартный доступ пользователей к корпоративным ресурсам.
2. Доступ пользователей к критически важным ресурсам предприятия.
3. Фильтрация всего трафика удалённых пользователей.

Выбор подхода зависит от конкретных сценариев. При доступе к критически важным ресурсам можно запретить все незащищённые соединения от удалённого пользователя, в другом сценарии — фильтровать весь трафик удалённого пользователя на корпоративном NGFW.

Контроль состояния

Если ПК пользователя заражён, то вредонос может попасть в защищаемую сеть. Этого можно избежать, если контролировать состояние ПК сотрудника:

- проверка последнего обновления ОС;
- чёрный и белый списки установленного ПО;
- обновление антивирусных баз;
- проверка запущенных служб.

Например, можно отключать от VPN пользователей, у которых в процессе подключения «упал» антивирус.

Механизмы аутентификации

Статические пароли — самый простой способ аутентификации, но не самый безопасный, поскольку пароли уязвимы перед хакерами. Для сегментов ИТ-инфраструктуры используется три варианта аутентификации:

1. Логин/пароль.
2. Сертификаты.
3. Многофакторная аутентификация.

Крупные корпорации «смешивают» варианты вместе, наиболее часто встречаются две комбинации: логин/пароль + одноразовый код (OTP) или push-уведомление и сертификат + токен.

Примеры систем для организации защищённого удалённого доступа:

1. Многофакторная утентификация.

- Континент ZTN-клиент + Рутокен ЭЦП = сертификат + токен
- Континент ZTN-клиент + Multifactor = логин/пароль + push-уведомление
- Континент ZTN-клиент + Avanpost MFA+ = логин/пароль + push-уведомление

2. Клиенты для удалённого доступа.

- VPN-клиент Континент ZTN-клиент устанавливается на ОС: Windows, Linux, MacOS, iOS, Android, «Аврора».

3. Комплаенс-контроль.

- Континент ZTN-клиент — встроенный комплаенс-контроль
- «САКУРА» — централизованный комплаенс-контроль

ИНТЕГРАЦИИ С ИНФРАСТРУКТУРНЫМИ СЕРВИСАМИ

Крупным предприятиям сложно организовать защиту ядра сети из-за **трёх факторов:** производительность, аудит конфигураций, сеть виртуализации.

Производительность NGFW

Внутри сети надо сегментировать десятки и сотни гигабит, но NGFW не всегда имеет нужную пропускную способность. Однако это решается через горизонтальное масштабирование, то есть интеграцию с внешними балансировщиками. Например, подключаем к балансировщикам два NGFW со скоростью обработки 10 Гбит/сек каждый и получаем 20 Гбит/сек. Если нужно увеличить цифру, подключаем дополнительный NGFW.

Недавно эксперты «Кода Безопасности» протестировали ферму из 16 NGFW «Континент 4» и двух брокеров сетевых пакетов DS Integrity NG. Итоговый результат фильтрации трафика — 400 Гбит/сек.

Аудит конфигураций и политики безопасности

В крупных предприятиях необходимо контролировать сотни сетевых устройств. В случае с NGFW этот контроль заключается в двух задачах: аудит конфигурации устройств и централизованное внесение изменений в конфигурацию.

На NGFW могут быть настроены тысячи правил межсетевого экранирования, которые устаревают, конфликтуют между собой и так далее. Всё это влияет на безопасность и производительность. Проблемы можно увидеть и решить через выделенные системы контроля конфигураций, например российские EFROS DO и Netopia.

Защита сети виртуализации

Виртуализация имеет свою сеть, которая связывает виртуальные машины (ВМ) и физические серверы. Трафик может «ходить» между ВМ (паттерн запад — восток) и от ВМ до физических или облачных ресурсов (паттерн север — юг).

Межсетевые экраны уровня гипервизора умеют защищать сети виртуализации. Они используют политики безопасности для конкретных ВМ. В случае с фильтрацией трафика по паттерну запад — восток пропадает необходимость передавать этот трафик на физические межсетевые экраны. Но для межсетевых экранов уровня гипервизора необходим функционал NGFW: контроль приложений, IDS/IPS, индикаторы компрометации.

Такие устройства называются распределённые FW/NGFW. В «Коде Безопасности» это отдельный продукт — vGate.

РАСШИРЕННАЯ БЕЗОПАСНОСТЬ

Раньше для корпоративных межсетевых экранов требовалась интеграция с системами IDS/IPS. Сейчас требования изменились, поэтому в NGFW нужен встроенный функционал «песочницы», антивируса и защиты от фишинга и ботов. Последние две функции реализуемы в NGFW, а вот «песочницы» — не всегда, поэтому современные NGFW должны уметь интегрироваться со сторонними продуктами.

NGFW «Континент 4» умеет интегрироваться с отечественными песочницами:

- PT Sandbox;
- KATAP;
- ATHENA.

Другой принцип расширенной безопасности — использование индикаторов компрометации, то есть данных о вредоносных ресурсах и ПО. Индикаторами нужно делиться со всеми сегментами ИТ-инфраструктуры, что решается через выделенные системы Threat Intelligence Platform. Такие системы агрегируют информацию об индикаторах с нескольких ресурсов и распространяются на средства защиты.

Индикаторы компрометации в «Континент 4»:

1. Встроенные базы:

- «Код Безопасности»;
- Лаборатория Касперского;
- Центральный Банк (ФинЦЕРТ);
- RST-cloud.

2. Интегрируемые базы:

- Security Vision;
- R-Vision;
- пользовательские.

ВЫВОД

Указанные направления интеграции с NGFW крайне актуальны и востребованы на рынке. Наращивание экспертного опыта в этих областях позволит вендорам создать более качественный продукт и удовлетворить спрос заказчиков.

1. Организация защищённого удалённого доступа снизит вероятность проникновения через компрометацию удалённого пользователя.
2. Интеграция NGFW с сервисами снизит вероятность взлома внутренней инфраструктуры.
3. Расширенная безопасность NGFW своевременно обнаружит актуальные и ранее неизвестные угрозы.

ВЫБИРАЕМ NGFW

КАК НАЙТИ ТОТ, ПРОИЗВОДИТЕЛЬНОСТЬ КОТОРОГО ВАС УСТРОИТ

Алексей ДАНИЛОВ
руководитель продуктового направления ИнфоТеКС

Один из основных параметров, на который обращают внимание заказчики при выборе NGFW, — производительность. Однако сравнить продукты разных вендоров по этому параметру на основании только маркетинговых материалов практически невозможно. Дело в том, что каждый производитель использует собственную методику измерения производительности и результаты одного производителя нельзя сравнивать с результатами другого без анализа и сопоставления этих методик. Что же делать заказчику?

УНИВЕРСАЛЬНЫЕ И НЕЗАВИСИМЫЕ МЕТОДИКИ

Ещё в начале 2010-х на сайтах производителей публиковали показатели производительности, не раскрывая детали того, как и при каких условиях получен результат тестирования. Но постепенно рынок и требования стали меняться, это привело к тому, что вендоры начали публиковать показатели производительности своего продукта с дополнительными разъяснениями о том, как именно получены результаты. Разнообразие данных было значительным, поэтому появилась потребность в разработке универсальных и независимых методик.

Запрос на разработку таких методик был принят и воплощён в жизнь компанией NSS Labs — независимой организацией из США, с 1991 года занимающейся исследованиями и тестированием решений в области безопасности. Большинство мировых производителей, являющихся лидерами в этой области, передавали свои продукты на исследование в NSS Labs, где проводилось тестирование по собственной единой методике, что позволило считать сравнимыми те результаты, которые NSS Labs публиковала в своих отчётах.

Одной из первых распространённых методик, изначально предназначавшейся для измерения производительности маршрутизаторов, но успешно применённой для тестирования шлюзов безопасности, стала RFC-2544. Через некоторое время мировое сообщество признало себе, что стандарт RFC-2544 морально устарел и отрасли требуется новая методика, в результате чего появился документ RFC-9411. Он разработан для тестирования шлюзов безопасности, а не маршрутизаторов и описывает множество тонких моментов, которые важно учитывать при тестировании именно данного типа продуктов.

КАКИЕ МЕТОДИКИ ИСПОЛЬЗУЕТ ИНФОТЕКС ПРИ ПРОВЕДЕНИИ ТЕСТИРОВАНИЯ NGFW И ПОЧЕМУ

Мы используем систему тестирования производительности, функционала и совместимости сетей и сетевых приложений — компактное двухслотовое шасси Ixia XM2.

В своих тестах берём за основу:

- RFC-2544;
- RFC-9411;
- методики NSS Labs для NGFW.

Почему мы используем методики NSS Labs? Потому что мы можем их воспроизвести и сравнить результаты. Мы используем инструменты для проведения тестов той же фирмы Ixia, что использовала NSS Labs, и мы можем сравнить наши результаты с результатами NSS Labs для других производителей.

Помимо основных целей и задач наших испытаний — выявлять возможности нашего продукта и контролировать его качество и стабильность работы, — мы можем сравнить себя с конкурентами и определить, к чему стремиться, чтобы сделать продукт лучше.

ПРОФИЛЬ ТРАФИКА — ВАЖНАЯ ЧАСТЬ МЕТОДИКИ

Производительность шлюза безопасности кардинально зависит от того, какой тип трафика и какой сетевой протокол обрабатываются шлюзом безопасности. В реальных сетях мы сталкиваемся с множеством разнородного трафика. Мы имеем так называемые мультисервисные сети, то есть сети, в которых одновременно работает множество сервисов. И у каждого заказчика собственный набор сервисов в сети.

Одним из первых производителей, задумавшихся над задачей выявления пропускной способности в мультисервисных сетях, был Juniper, который в своих публикациях стал указывать производительность для трафика IMIX (Internet MIX). IMIX — это такой усреднённый трафик в магистральных сетях. Для его подсчёта сообщество проанализировало весь трафик интернета (когда-то на момент разработки IMIX) и выявило долю пакета типового размера в общем объёме. Получилось примерно так: в одной порции трафика есть 1 пакет размером 1500 байт (8,3 %), 7 пакетов размером 40 байт (58,3 %) и 4 пакета размером 576 байт (33,3 %). Все пакеты включают размер заголовка. Вероятно, это было началом, но не итоговым результатом в борьбе потребителей за публикацию сопоставимой информации о производительности.

Да, IMIX-трафик изменил цифры в разделе «производительность» на сайтах вендоров, покупатели стали задумываться, как такие результаты интерпретировать и применять к своим задачам. Это привело к появлению нового термина Enterprise MIX (EMIX) — смесь трафика корпоративных заказчиков. Но, во-первых, у каждой компании он оказался свои и уникальным, во-вторых, закрытым (непубличным), и никто не хотел им делиться.

НА ЧТО СТОИТ ОБРАТИТЬ ВНИМАНИЕ ЗАКАЗЧИКУ. НАШИ РЕКОМЕНДАЦИИ

Количество правил. Когда публикуют данные о производительности, редко кто указывает, сколько правил фильтрации было активно в момент тестирования. Например, Check Point в своей методике SPU (Security Power Unit) заявляет 100 правил фильтрации. Достаточно ли этого? Казалось бы, да, ведь если тестирование проводится согласно RFC-2544, то правило фильтрации в тесте одно: всем всё разрешено. А тут в 100 раз больше.

Но RFC-9411 предполагает использование 562 правил фильтрации/доступа, это в 5 раз больше. Может быть этого достаточно для проведения тестирования? Правильный ответ отсутствует. У нас есть заказчик, у которого на старте пилотного проекта было 5 тысяч правил фильтрации/доступа, а через год их стало 10 461.

Что же делать заказчику? Важно ли количество правил при тестировании и потом в работе? Как показывает опыт, количество правил — важный параметр и он серьёзно влияет на производительность шлюза безопасности. Поэтому если вы понимаете, что у вас свой случай, то нужно обсуждать его с производителем.

Профиль трафика. Лучшее из решений — создать свой профиль трафика и попросить производителя провести с ним тестирование. Если это невозможно, то постараться понять, какой профиль трафика у производителя используется для его тестов, как он соотносится с вашим, и пробовать аппроксимировать эти данные. Та ещё задача...

Журналирование. При анализе данных о производительности никто не задаётся вопросом, включено ли журналирование. Как показывает практика, задача журналирования всего происходящего в шлюзе безопасности достаточно ресурсоёмкая. В методике RFC-2544 это учтено, в RFC-9411 тоже. Правда, первая методика не определяет действие, а значит, журналирование при испытаниях можно и не включать, вторая же требует включения журналирования, но не описывает уровень детализации. Поэтому если вендор декларирует, что тесты проводятся по RFC-9411, то журналирование включено, однако уровень детализации при этом неизвестен. А если по RFC-2544 — то журналирование точно выключено. Если используется собственная методика, детали нужно выяснять у производителя. При этом не стоит забывать, что требования заказчика обычно включают в себя журналирование всего.

ВЫВОДЫ

Все производители честны со своими заказчиками, опубликованные производителем параметры получились при использовании собственных методик тестирования продукта. Ваши реальные условия всегда будут отличаться от тех, которые были выставлены вендором при внутреннем тестировании. Насколько именно, зависит от целого ряда факторов. Именно поэтому вы не сможете точно оценить, подходит ли производительность устройства для решения вашей задачи, только по листовке или по данным с сайта производителя.

Прежде чем покупать продукт, обратитесь к интегратору или к вендору, чтобы они провели тестирование в условиях, максимально приближенных к вашим реальным.

ПРИМЕР ИЗ ПРАКТИКИ ИНФОТЕКС

Пример из нашей практики. Потенциальный заказчик проводит тестирование шлюзов безопасности. В рамках тестирования было запланировано проведение в том числе нагрузочного тестирования. Для проведения тестов использовалось оборудование Ixia, была разработана методика тестирования и использовался профиль трафика заказчика.

По условиям испытания необходимо было предоставить шлюз безопасности с пропускной способностью 1 Гбит/сек. Мы передали шлюз, который, согласно нашим измерениям, демонстрирует пропускную способность до 250 Мбит/сек. Потенциальный заказчик выразил недоумение по этому поводу, но допустил нас до испытаний. В процессе испытаний наш шлюз безопасности продемонстрировал пропускную способность 920 Мбит/сек.

На вопрос заказчика, почему мы в официальных документах публикуем показатель 250 Мбит/сек, а устройство при этом демонстрирует более высокие показатели, мы ответили, что всё дело в методике, а точнее в использованном на испытаниях профиле трафика, который на 90 % состоит из http/https-трафика, что является лёгкой задачей для шлюзов безопасности. Мы используем свою методику и свой профиль трафика, так как считаем их универсальными, то есть подходящими большинству покупателей. Да, допустима дискуссия о том, что http/https-трафик «разный», нужно смотреть размер транзакции, требуется ли так называемый SSL decrypt и т.д. Но, собственно, все эти нюансы и есть методика тестирования.

ЧТО УЧЕСТЬ ПРИ ПЕРЕХОДЕ НА ОТЕЧЕСТВЕННЫЕ NGFW

Роман АСАЕВ
руководитель группы сетевой безопасности центра ИБ, «Инфосистемы Джет»

Последняя пара лет стала настоящим технологическим скачком для отечественных производителей: активно развиваются отечественные операционные системы, офисные программы, облачные сервисы. Рынок NGFW не исключение. После ухода зарубежных вендоров из России возникла необходимость миграции NGFW на отечественные аналоги — чаще всего этот процесс сопровождается сложностями. «Инфосистемы Джет», которая внедрила более 50 отечественных NGFW, делится своим опытом.

ОСНОВНЫЕ СЛОЖНОСТИ

В 90% проектов «Инфосистемы Джет», связанных с переходом на отечественные NGFW, использовались решения следующих вендоров:

- UserGate;
- Код Безопасности;
- ИнфоТеКС;
- Ideco.

С середины 2022 года мы выполнили более 250 пресейлов по миграции и успешно завершили более 50 проектов. Благодаря полученному опыту получилось выделить четыре кластера основных сложностей:

- принципиально разная архитектура у зарубежных вендоров;
- неоптимальная архитектура сети до миграции;
- более низкая производительность по сравнению с западными решениями с тем же набором функций;
- невозможность автоматического переноса настроек и «политик».

Проиллюстрируем их конкретными примерами.

ПРИНЦИПИАЛЬНО РАЗНАЯ АРХИТЕКТУРА У РАЗНЫХ ВЕНДОРОВ

Задача. Заменить текущий заграничный NGFW на отечественный, учитывая, что в конфигурации зарубежного использовался необычный способ трансляции адресов: транслировались адреса всех устройств, а хосты, которым NAT (Network Address Translation) не требовался, исключались с помощью гибкого и удобного механизма — правил no-nat.

Сложность. В отечественном NGFW возможность использовать правила no-nat штатными средствами не заложена.

Решение. Проблема может быть решена путём создания правил с инвертированием адресов источника и назначения, а подчас и инвертированием зон. Главная идея состоит в том, чтобы заданные инвертированные критерии в правиле совпали, а само правило не отработало и трансляция адресов не произошла. Дойдя до конца списка NAT-правил, отечественный NGFW перейдёт к обработке трафика следующим модулем и трансляция адресов выполнена не будет. Такой способ можно использовать для реализации переноса конфигурации 1 в 1 при достаточном количестве условий для правила NAT. В случаях, когда в критериях правил источника или назначения указана не определённая, а произвольная зона и нет дополнительного уточнения адресов, то исключения будет невозможно выполнить.

НЕОПТИМАЛЬНАЯ АРХИТЕКТУРА СЕТИ ДО МИГРАЦИИ

Задача. Мигрировать WAN-модуль и перенести несколько DMZ-подсетей (/29) с публичными адресами и публичными сервисами за кластер NGFW. При этом любой трафик, покидающий DMZ-подсеть, должен проходить через межсетевой экран.

Сложность. Адресное пространство в подсетях распределено между серверами, в каждой подсети свободен только один ip-адрес, который может выступать в качестве шлюза по умолчанию и может быть назначен на кластерном интерфейсе межсетевого экрана. Для сборки кластерного интерфейса выбранному отечественному NGFW требуется не один, а три ip-адреса из одной подсети. Приватные адреса как дополнительные для кластеризации при основном публичном он не поддерживает. Выделить дополнительные публичные ip-адреса в переносимых DMZ-подсетях для того, чтобы назначить адресами кластеризации межсетевого экрана, невозможно.

Решение. При проведении работ по миграции на L3-коммутаторе между WAN-блоком и сегментом DMZ был включён функционал VRF-Lite. С помощью данного функционала таблицы маршрутизации изолировались друг от друга. В каждом экземпляре VRF создан виртуальный интерфейс в соответствующей DMZ-подсети и виртуальный интерфейс в стыковочной подсети между коммутатором и NGFW. Для стыковочной подсети использованы приватные ip-адреса. С помощью маршрутизации настроена связность между NGFW и сегментом DMZ. Схема позволила обойти ограничения описания выше и разместить сегмент DMZ за NGFW.

БОЛЕЕ НИЗКАЯ ПРОИЗВОДИТЕЛЬНОСТЬ ПО СРАВНЕНИЮ С ЗАПАДНЫМИ РЕШЕНИЯМИ С ТЕМ ЖЕ НАБОРОМ ФУНКЦИОНАЛА

Задача. Заменить зарубежное решение на отечественное при миграции ядрового NGFW.

Сложность. Задачу невозможно решить линейной миграцией с одного устройства на другое, поскольку производительность отечественного аналога меньше, чем у зарубежного.

Решение. Использовать совместно с NGFW пакетные брокеры. Архитектура при замене подразумевает использование нескольких независимых единиц межсетевых экранов по схеме N+1. С помощью такой архитектуры удаётся добиться необходимой производительности, сопоставимой с производительностью текущего NGFW или превышающей её. Брокеры сетевых пакетов в этой архитектуре выполняют функции балансировки трафика между узлами by session. Также при такой схеме решается вопрос масштабируемости: при использовании пакетных брокеров всегда можно добавить дополнительные независимые NGFW.

НЕВОЗМОЖНОСТЬ АВТОМАТИЧЕСКОГО ПЕРЕНОСА НАСТРОЕК

Задача. Заменить NGFW с богатой историей эксплуатации.

Поскольку отечественные NGFW не являются на 100% аналогами зарубежных, то сложности при переходе неизбежны. Важно подходить к задаче комплексно и использовать разные решения от разных производителей на различных сегментах сети передачи данных

Сложность. При миграции организация столкнулась с проблемой, что на Cisco ASA много контекстов и тысячи правил. Предлагаемые вендором скрипты для переноса правил работают некорректно.

Решение. Разработан скрипт, обеспечивающий формирование списков объектов и правил из произвольного числа контекстов. Скрипт проверит наличие задублированных объектов и правил в конфигурациях, обеспечивает их переименование, если совпадение частичное: например, одинаковое название группы, но разный состав и игнорирование дубликатов при полном совпадении. Также скрипт умеет оптимизировать правила — формировать одно правило вместо нескольких с одинаковыми адресами назначения и портами, но разными адресами источника. Этот скрипт увеличивает скорость работы команды внедрения и экономит множество сил и времени на внедрение нового NGFW.

ЧЕМУ СТОИТ УДЕЛИТЬ ВНИМАНИЕ НА ПРОЕКТЕ ПО ИМПОРТОЗАМЕЩЕНИЮ НА РЫНКЕ СЕТЕВОЙ БЕЗОПАСНОСТИ

Рассмотрим пример типового проекта по миграции на отечественные NGFW. Средняя длительность проекта по нашему опыту составляет от 6 до 12 месяцев, основные этапы выглядят так:

- обследование;
- разработка архитектуры и концепции сегментации с учётом актуальных угроз;
- проектирование и внедрение;
- переключение трафика;
- передача на сервис.

Отдельно остановимся на переключении трафика на новую инсталляцию, когда интегратор совместно с заказчиком переводит тестовый сегмент для отработки всех взаимодействий на целевом NGFW. Отработав переключение на тестовом сегменте, начинается перевод боевых сегментов и одновременно проверка критичных сервисов при данном переводе. Особое внимание стоит уделить проверке критичных сегментов и систем, причём к работам необходимо подойти осознанно не только интегратору, но и организации-заказчику: желательно привлечь всех владельцев бизнес-систем. Если забыть об этом, бизнес может остановиться в самый неподходящий момент.

Поскольку отечественные NGFW не являются на 100% аналогами зарубежных, то сложности при переходе неизбежны. Важно подходить к задаче комплексно и использовать разные решения от разных производителей на различных сегментах сети передачи данных.

Если осознанно подойти к процессу, то от перехода на отечественные NGFW можно выиграть:

- улучшить архитектуру и осознанный подход к построению сети;
- актуализировать проектную и рабочую документацию;
- оптимизировать политики NGFW;
- интегрироваться с российской экосистемой ИБ и ИТ;
- создать зоны безопасности NGFW, актуальные угрозам.

ТЕРАБИТНЫЙ NGFW

ВЫЗОВЫ ДЛЯ СЕТЕВОЙ БЕЗОПАСНОСТИ

Сергей ПЛОТКО
директор по аналитике и интеграции компании «Цифровые решения»

Российский высокопроизводительный кластер NGFW: миф или реальность? Как решить задачу по защите высокоскоростных каналов передачи трафика?

Одной из основных задач разработчиков современных российских NGFW остаётся наращивание производительности для защиты инфраструктур с высокоскоростными каналами связи. При этом для надёжной сетевой защиты в современных условиях необходима инспекция, фильтрация и анализ трафика на уровне приложений (L7 — седьмой уровень модели OSI).

Чем глубже NGFW разбирает входящий трафик и чем больше функций задействуется, тем меньше становится производительность решения. В результате у всех межсетевых экранов в режиме IPS (предотвращение вторжений) производительность падает почти в 3 раза, а в режиме NGFW — в 5–7 раз. Каким же образом обеспечивать защиту высокоскоростных каналов с полноценным анализом трафика?

УВЕЛИЧЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ: МИРОВОЙ ОПЫТ

Существует два основных способа повышения производительности NGFW при работе с высокоскоростными каналами:

1. Применение для обработки специализированных микросхем (ASIC) или программируемой логики (FPGA). Они обеспечивают высокую производительность и эффективность, но требуют значительных финансовых и временных инвестиций в разработку.

2. Формирование кластера NGFW за счёт балансировки (распределения) нагрузки отдельным устройством или модулем. Кластеризация позволяет использовать уже имеющиеся решения и гибко наращивать производительность в процессе эксплуатации.

Palo Alto Networks и Fortinet выбрали использование ASIC/FPGA, в то время как Check Point пошёл вторым путём. Оба подхода имеют свои преимущества и недостатки как в реализации, так и в эксплуатации.

КЛАСТЕРИЗАЦИЯ NGFW: ЗАДАЧИ, ФУНКЦИИ, МАКСИМАЛЬНАЯ ПРОИЗВОДИТЕЛЬНОСТЬ

Основными задачами кластеризации являются балансировка нагрузки и обеспечение отказоустойчивости. Для их решения применяются специализированные устройства, такие как балансировщики нагрузки и брокеры сетевых пакетов. Единственный российский брокер, занесённый в реестр Минпромторга России, — DS Integrity от компании «Цифровые решения».

Рассмотрим простой пример: если один NGFW может обработать максимум 10 Гбит/с трафика, а необходимо защитить канал 40 Гбит/с, то можно взять четыре устройства и равномерно распределить поток на них с помощью балансировщика нагрузки или брокера сетевых пакетов. Таким образом, на каждый NGFW будет поступать посильная для него нагрузка.

В части балансировки есть много возможностей.

- Разделение по хешам — самый простой способ, при котором законы больших чисел при большинстве профилей трафика обеспечат равномерность распределения нагрузки.
- Равномерное распределение сессий — отслеживание и обеспечение одинакового количества сессий на каждом NGFW.
- Равномерное распределение нагрузки — отправка новых сессий на наименее нагруженные устройства, что помогает учитывать большую неравномерность потоков в трафике и избегать превышения пропускной полосы.

Однако при решении задачи по балансировке трафика необходимо учитывать ряд важных аспектов. Для того чтобы обеспечить корректную обработку трафика на уровне L7, важно передавать пакеты одной сессии в один и тот же NGFW независимо от направления.

Задача распределения нагрузки весьма ресурсоёмкая, и она определяет общую производительность кластера. Возможности всего кластера будут определяться производительностью балансировщика нагрузки, в то время как от производительности каждого отдельного NGFW будет зависеть только количество необходимых устройств в кластере.

Построение кластера также решает задачу по обеспечению отказоустойчивости, ведь NGFW может выйти из строя или его потребуется перезагрузить для обновления ПО. При этом ни общая защита периметра, ни клиентский сервис не должны пострадать, а нагрузка должна быть перераспределена по оставшимся устройствам.

Существуют два основных типа кластеров: active-passive (активный-пассивный) и active-active (активный-активный).

Самый простой вариант кластера с точки зрения отказоустойчивости — **active-passive**. Такой тип кластера обеспечивает надёжность и отказоустойчивость путём переключения всего потока трафика с вышедшего из строя устройства на резервное. *Active-passive*-кластер позволяет обеспечить непрерывность работы сети, но не повышает производительность.

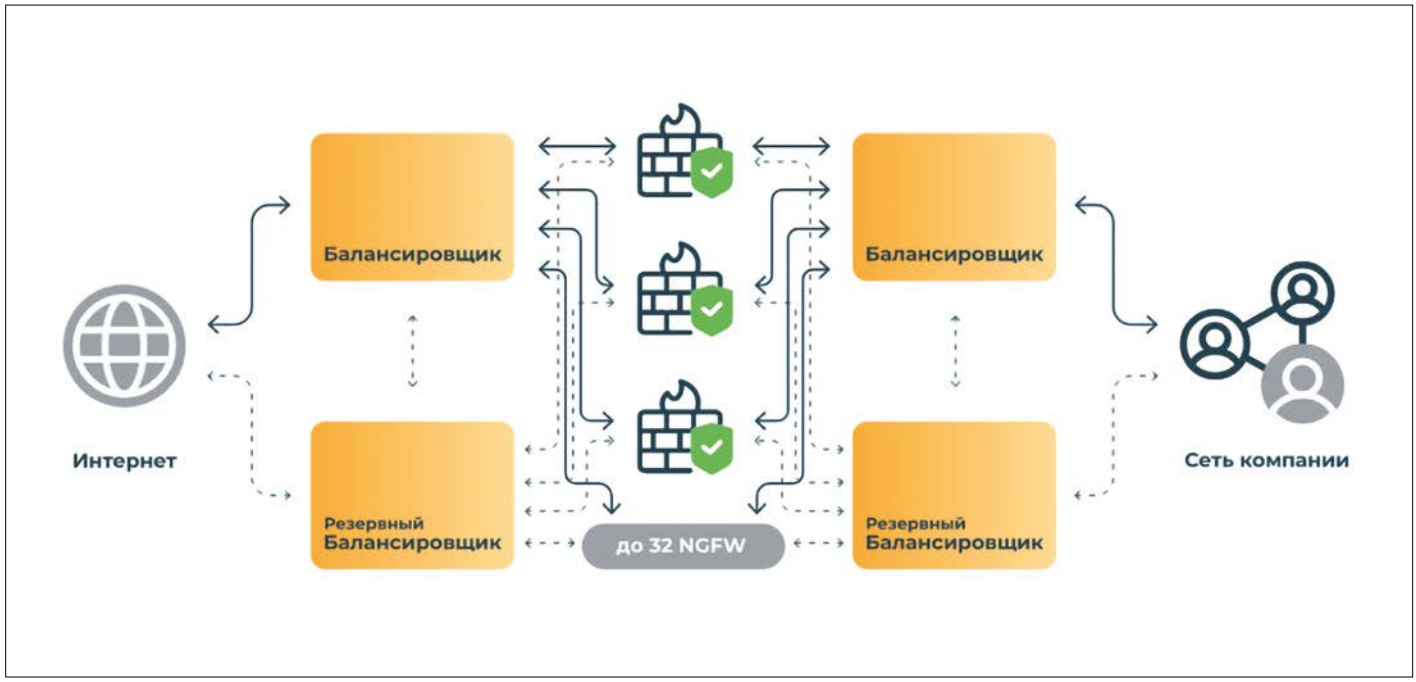


Рисунок 1. Схема резервирования N+1

Для обеспечения отказоустойчивости с одновременным увеличением производительности используется кластер active-active. При такой схеме кластеризации внедряется от трёх устройств NGFW. Вероятность одновременного выхода из строя нескольких устройств на порядок ниже, чем одного, что позволяет использовать схему резервирования N+1 (рисунок 1).

Строить кластер active-active на два устройства нецелесообразно. Если производительности одного NGFW достаточно, то проще построить кластер active-passive. Если же для обработки потока необходимо задействовать оба устройства, то в случае отказа одного из них сервис деградирует и бизнес-процессы начнут работать с перебоями.

КАК РАБОТАЕТ БАЛАНСИРОВЩИК НАГРУЗКИ

Балансировщик нагрузки может контролировать работоспособность отдельных NGFW и при необходимости перенаправлять трафик на рабочие устройства. NGFW анализирует сессию с момента её установки, и для того, чтобы резервное устройство её не заблокировало, результаты анализа должны передаваться на резервные устройства.

Нужно отметить, что для большинства современных приложений это не проблема. Они автоматически устанавливают новую сессию через резервный NGFW. Но для ряда приложений это критично, и NGFW должны синхронизировать между собой состояние сессии.

Даже у мировых лидеров синхронизация сессий реализована с ограничениями. При SSL-инспекции синхронизация не работает ни у одного производителя. Это означает, что при переключении трафика на резервное устройство в любом случае будет кратковременный обрыв связи и ошибка в приложении, если оно не умеет обрабатывать такие события.

И да, балансировщики нагрузки тоже нужно резервировать.

ВИДИМОСТЬ КЛАСТЕРА КАК ЕДИНОГО УСТРОЙСТВА С ОДНИМ АДРЕСОМ

Если балансировщик нагрузки скрывает кластер за своим адресом, представляя для внешней инфраструктуры кластер одним устройством, то это упрощает его настройку и эксплуатацию.

Есть альтернативный вариант: инфраструктура общается только с одним NGFW, а стоящий в прозрачном режиме балансировщик нагрузки распределяет трафик по всем оставшимся устройствам незаметно для соседних коммутаторов и маршрутизаторов.

«А ЧТО В РОССИИ?»

Российские компании сейчас проходят путь, который у иностранных вендоров занял десятилетия. Построение высокопроизводительных NGFW в виде кластера с балансировкой позволяет использовать уже проверенные решения и существенно снизить сроки разработки. Это актуально и для потребителей, которые при такой архитектуре могут наращивать производительность кластера постепенно.

В инфраструктурах российских компаний с 2023 года работают схемы кластеризации NGFW при помощи брокеров сетевых пакетов DS Integrity от компании «Цифровые решения». Российский высокопроизводительный NGFW на 800 Гбит/с уже стал реальностью.

Текущие цели, к которым мы идём вместе с нашими технологическими партнёрами, — добиться пропускной способности кластера выше терабита, создать единую систему управления и обеспечить возможность плавно вводить и выводить устройства из кластера. И мы их скоро достигнем!

«NGFW — ТЕХНОЛОГИЧЕСКИ ОДИН ИЗ САМЫХ СЛОЖНЫХ ПРОДУКТОВ, ЕГО НЕЛЬЗЯ ВЫПУСТИТЬ ЗА ГОД ИЛИ ДВА»

Иван ЧЕРНОВ
руководитель технического маркетинга UserGate

Сегодня порядка 50 российских компаний занимаются разработкой межсетевых экранов нового поколения. Многие ли дойдут до финиша и каким требованиям заказчиков должен удовлетворять NGFW? На вопросы BIS Journal отвечает Иван Чернов.

— На прошедшем в сентябре BIS Summit 2024 заместитель директора ФСТЭК России В. Лютиков заявил, что в стране порядка 50 компаний занимаются разработкой межсетевых экранов нового поколения (NGFW), но до конца года будут сертифицированы продукты только двух вендоров. Как вы оцениваете ситуацию на столь конкурентном рынке?

— Если посмотреть на историю российской сетевой безопасности, то до 2022 г. на рынке было всего три отечественных игрока, один из которых UserGate. Зарубежные производители фактически монополизировали этот рынок, но с их уходом российские компании, так или иначе связанные с ИБ, оживились и решили занять образовавшуюся нишу. В результате появилось множество производителей NGFW. Существенно больше, чем сейчас необходимо рынку. Это переходный этап, который нужно пройти.

Безусловно, рынка NGFW не хватит на всех игроков, и многим придется уйти. К тому же NGFW — технологически один из самых сложных продуктов в кибербезе, его нельзя выпустить за год или два. Требуются RnD-проекты, разработка, тестирование, исправление ошибок — огромное число итераций. Нужно пройти долгий путь, чтобы получить зрелый продукт.

Раньше мы соревновались с западными конкурентами, продававшими решения по всему миру и имевшими огромную инсталляционную базу. Количество реализованных ими проектов было кратно больше, чем весь российский рынок. А это значит, что их опыт в создании и усовершенствовании своих продуктов на основании полученной от заказчиков обратной связи был значительно больше. Для российских производителей доступ к пулу заказчиков открылся после 2022 г. К этому моменту мы уже прошли длинный путь: разработали целую линейку продуктов на основе собственной операционной системы UG OS, наладили собственное производство на территории России, сотрудничали с большинством системных интеграторов и имели в своем пуле ряд крупных заказчиков. Мы занимали свою долю рынка и успешно конкурировали с глобальными вендорами.

В ситуации, когда западные производители спешно покинули Россию, оставив своих заказчиков без обновлений и техподдержки, мы были одними из немногих, кто смог принять этот вызов. Нагрузка была колоссальная. Но это был и очень большой опыт, который способствовал нашему стремительному росту как в технологическом плане, так и в плане работы с заказчиками, понимания их нужд и потребностей. Он не прошел даром. За последние два года мы проделали огромную работу, вывели наши продукты на новый уровень качества.

Сейчас вместе с новыми российскими продуктами появились и новые «Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети», разработанные при участии представителей отрасли кибербеза и утвержденные приказом ФСТЭК России. Этот документ — усредненное видение отрасли состава NGFW.

Два производителя NGFW уже проходят сертификацию на соответствие требованиям, другие вендоры готовят документы. Вскоре появится несколько сертифицированных решений. Вместе с ними сформулируются и требования по использованию многофункциональных межсетевых экранов (ММЭ).

Несертифицированный продукт также может решать задачи пользователей, которым нужна только часть функций устройства. Но получить сертификат ФСТЭК, в конечном итоге, будет необходимо.

— С 1 января 2025 г. вступают в силу действия закона по импортозамещению, и заказчики ринутся покупать сертифицированные устройства. Сколько времени уйдет на замену оборудования с учётом миграции на отечественные решения?

— Те, кто начнут заниматься этим после вступления закона в силу, уже не успеют. Процесс перехода долгий. В законе прописаны требования не использовать устройства из недружественных стран, а на рынке есть достаточно сертифицированных се-

тевых экранов, систем обнаружения вторжения и иных решений, которые входят в реестр ФСТЭК России и уже сейчас могут придти на замену иностранным.

— Давайте посмотрим на рынок глазами потребителя, у которого всё работает, но обстоятельства требуют смены оборудования. И он стоит перед выбором нового решения, не понимая, с чего начать.

— Посмотрим на вопрос шире, с точки зрения требований Указов № 166, 250 в редакции 2024 г. и проблем импортозамещения. За 2022–2023 гг. в процессе работы над более чем 5 тыс. проектов мы выработали наиболее безболезненный процесс миграции. Знаем проблемы заказчиков, оставшихся без поддержки вендоров, и можем им помочь. Это сильно упрощает жизнь действующим и потенциальным клиентам.

По опыту, заказчика интересует широта функционала, совместимость с имеющимся оборудованием. Построенная ранее ИТ-инфраструктура должна работать. ИБ это производная функция от ИТ, а ИТ — производная от бизнеса. В процессе импортозамещения заказчику важна непрерывность основного бизнес-процесса без потери функционала.

Следующий вопрос — реальная защита, идет исследование функций защиты. После встает вопрос миграции. Это особенно важно в крупных компаниях, где в подразделениях стоят разнообразные устройства, а для миграции нужны руки и ресурсы.

Не все отечественные вендоры имеют большой опыт реализации таких проектов, а заказчик ищет надёжных технологических партнеров, которые умеют работать с новым оборудованием и правильно мигрировать, имеют инструментарий по переносу политик, что помогает облегчить процесс перехода.

Важно окружение вендора: авторизованные партнёры, техническая документация и учебные материалы, потому что вслед за миграцией идет процесс эксплуатации. Многие российские специалисты, имеющие сертификаты иностранных производителей, переживают определённый стресс, когда сталкиваются с новыми устройствами. И курсы подготовки по работе с оборудованием — большой плюс вендора.

Эти четыре шага помогают успешно провести импортозамещение. И выбор поставщика NGFW у заказчика существенно сужается при переходе в практическую плоскость.

Еще один аспект совместимости — одновременная работа старой и новой инфраструктуры при последовательном импортозамещении в рамках большой компании. Физически невозможно одномоментно поменять все старое оборудование

— Импортозамещение происходит не только в кибербезе, но и в ИТ-инфраструктуре. Как вы учитываете этот момент при работе с заказчиком?

— Замещение ИТ-ландшафта бросает вызовы. Порой, приходя к заказчику, мы узнаем об отказе от Microsoft, что нужны версии под российский Linux, что вместо AD требуется FreeIPA. Это нормально и привычно. В силу такой специфики можно сказать, что российские вендоры NGFW сильнее зарубежных, поскольку умеют работать и с 1С, и с Astra Linux, и с CISCO. Раньше мы разрабатывали вспомогательные инструменты для NGFW и планировали, в первую очередь, выпустить версию на Windows, сейчас начинаем с релиза под Astra Linux.

Еще один аспект совместимости — одновременная работа старой и новой инфраструктуры при последовательном импортозамещении в рамках большой компании. Физически невозможно одномоментно поменять все старое оборудование, в процессе миграции важно поддерживать совместимость с ним. Поэтому перед стартом следует детально обсудить все нюансы.

Исходя из опыта работы с большим количеством проектов, мы добавляли инструменты, которые позволяют реализовывать ряд функций, например создание защищённых тоннелей. Раньше их конфигурировали буквально тремя настройками. Сейчас настроек много, что позволяет гибко реализовывать такие связи.

— Какие функции безопасности должен реализовать «правильный» МЭ?

— Джентльменский набор NGFW это краткий список функциональностей, который выстраивает базовый уровень защиты и позволяет защитить от массовых потенциальных атак:

- идентификация приложений в сетевом трафике, технология DPI;
- идентификация пользователей. NGFW должен видеть активность каждого пользователя на уровне identity, что облегчает написание политик безопасности и расследование инцидента при необходимости;
- встроенная система обнаружения вторжения. Без СОВ межсетевой экран не может называться NGFW.

Но NGFW не является панацеей в ландшафте угроз. Это базовое средство защиты, но для борьбы с целевыми атаками одного NGFW недостаточно.

— Панели управления российских решений отличаются от иностранных, что часто вызывает неприязнь пользователей. Учитывают ли это вендоры и пы-

таются ли сохранить привычный многим интерфейс?

— Сила привычки — мощный фактор, недовольство возникает даже при переходе с оборудования одного западного вендора на другое. Когда люди переходят на новые решения под влиянием внешних факторов, они хотят, чтобы было как раньше. Но такого больше не будет.

Мы считаем, что нужно учиться, и специалисты понимают ценность образования. UserGate подготовил систему курсов и сертификаций, чтобы облегчить переход к новой архитектуре устройства и другой системе управления.

Мы также собираем обратную связь и, при необходимости, редактируем пункты меню.

— На презентациях вендоры NGFW делают ставку на высокую производительность. Важна ли она для небольших компаний?

— Производительность редко является ключевым критерием для небольших компаний. Если посмотреть по срезу используемых каналов, то средняя производительность на уровне 1 Гбит/сек. Запредельные скорости нужны единицам, например, банкам и телекоммуникационным компаниям федерального уровня. У малого бизнеса таких потребностей нет.

Битва за производительность — состязание инженерных потенциалов и борьба за крупных заказчиков. Последние требуют максимум скорости и приносят больше всего денег, поэтому обеспечивать высокую производительность для них необходимо, но не для массового потребителя.

— Если мы затронули вопрос денег, то на BIS Summit 2024 регуляторы говорили о высокой стоимости отечественных решений, а представители сообщества утверждали, что рост цен выше уровня инфляции...

— То, что мы наблюдаем по своим продуктам, — это действительно история про перекрытие уровня инфляции и стоимости зарубежных комплектующих, которые покупаются за валюту по курсу.

Как человек, отвечающий в том числе и за ценообразование в компании, подтверждаю: мы не проводим повышения стоимости по принципу «завтра будем продавать дороже». Проходит индексация, а мы вынуждены покупать комплектующие на рынке.

Жалобы регуляторам понятны. Компании годами выстраивали свои сети, финансируя работы частями. Сегодня в короткие сроки нужно поменять все. Цена складывается из множества факторов, средства нужно выложить сразу, это психологически некомфортно. По сравнению с западными решениями у российских есть точки роста. В совокупности это вызывает недовольство. Но многие при выборе российского вендора выбирают партнера на долгосрочную перспективу, чтобы инвестиции себя оправдали.

— Отечественный рынок небольшой по объему и в принципе ограничен. Есть ли у российских решений перспектива выйти на международный рынок?

— Глобальный мир, к которому привыкли, изменился на два полумира: глобальный Юг и глобальный Запад. Мы оказались на глобальном Юге, и потенциальный рынок сбыта — это азиатские и африканские страны, Латинская Америка.

У нас есть проекты во всех этих регионах. Потенциал там высокий, и мы за него поборемся. Как минимум, это технологический вызов. Бренд «Сделано в России» только формируется, и мы в этом процессе участвуем.

Нас не ждут в США и Европе. Но даже глобальные американские корпорации с офисами по всему миру, в т.ч. в странах, оказавшихся под санкциями, лишаются поддержки своих поставщиков. И закупают наше оборудование во все филиалы, потому что боятся массовых отключений. Это прецедент доверия. Ситуация, когда производитель отключает средства защиты, — вопиющий случай в мировой истории. И иностранные компании приглядываются к вендорам, которые не бросают заказчиков в экстренной ситуации.

— В сентябре компания UserGate представила новые версии ММЭ UserGate NGFW 7.1.2 и единого центра управления UserGate MC7.1.2. Что нового появилось в этих решениях?

— Ключевой фокус в разработке — удовлетворение потребностей заказчиков с точки зрения качества, стабильности и производительности. Мы расставили приоритеты и собираем обратную связь, исправляем недочёты и улучшаем производительность.

В ходе последнего обновления система обнаружения вторжения повысила скорость почти на 20%. Это хороший показатель улучшения производительности. Исправлено много недочётов, недоработок, багов.

В новом релизе мы добавили возможность обновления части библиотек на усмотрение пользователей. Это связано с оптимизацией для платформ младших моделей, которые менее технически оснащены и более доступны по ценам. Мы выяснили, что ряд библиотек редко используется заказчиками, но при этом создают нагрузку на устройства. Поэтому библиотеки, которые мы посчитали необязательными, поставили на загрузку по выбору потребителя. Мы сохраняем обязательства по наполнению этих библиотек. Часть библиотек, которые непосредственно влияют на безопасность, остались обязательными.

UserGate NGFW 7.1.2 входит в экосистему SUMMA. Мы являемся сторонниками открытой системы и изначально проектируем продукты с учетом совместимости. Есть централизованное управление и сбор событий, предусмотрена интеграция продуктов друг с другом. Ряд вспомогательных систем разрабатывают наши партнеры. Эти продукты встраиваются в экосистему SUMMA по открытому протоколу.

В будущих версиях мы готовим новую функциональность и дополнительные модули для использования. Но об этом мы расскажем позднее.

Беседовала
Марина Бродская

NGFW С DNS-ФИЛЬТРАЦИЕЙ

НОВАЯ НЕОБХОДИМОСТЬ ДЛЯ ЗАЩИТЫ ENTERPRISE-СЕГМЕНТА

Дмитрий ХОМУТОВ
директор Ideco

Современный киберпреступник не брезгует никакими методами: фишинг, ботнеты, вредоносные сайты — всё это скрывается за обычными ссылками, которые легко пропустить. И несмотря на наличие современных NGFW, защита DNS становится более важной. С Дмитрием Хомутовым, директором Ideco, разберём, как NGFW и DNS защищает сетевой периметр компании.

По данным Ideco, почти 88% компаний ежегодно подвергаются кибератакам, и около трети из них можно предотвратить на уровне DNS. Это подтверждает актуальность защиты от DNS-угроз и объясняет, почему крупные компании, такие как Cisco и CheckPoint, вкладывают значительные средства в развитие своих продуктов DNS Protection. А 31 июля 2024 года специалисты по информационной безопасности из Infoblox и Eclypsium обнаружили масштабную киберугрозу: злоумышленники захватили контроль над более чем 35 тысячами доменов, не имея доступа к учётным записям их владельцев.

УГРОЗЫ БЕЗОПАСНОСТИ НА DNS-УРОВНЕ

DNS — основа современного интернета, но она же становится мишенью для злоумышленников. Открытый порт 53/UDP на сетевых устройствах делает DNS уязвимым для атаки, так как пакеты поступают без предварительной проверки. Злоумышленникам легче создать и обновлять домены для своих целей, чем использовать IP-адреса. Современные системы защиты информации (СЗИ) часто основаны на белых и чёрных списках доменов. Злоумышленники обходят их, регистрируя случайные домены с коротким временем жизни, что не позволяет СЗИ заблокировать их. Таким образом, ботнет может связываться с устройствами в сети через DNS, даже если эти устройства не имеют доступа в интернет. По мнению экспертов NIST и CISA, DNS является первым уровнем защиты сети, и её безопасность крайне важна.

РАЗВИТИЕ IDECO NGFW: ИСПОЛЬЗОВАНИЕ DNS SECURITY В ЗАЩИТЕ ENTERPRISE-СЕГМЕНТА

Ideco NGFW с модулем DNS Security предлагает улучшенную защиту от DGA-атак с помощью анализа N-грамм и обнаружения аномалий, блокируя домены, которые не попадают под классическую фильтрацию. Он также предотвращает обход DNS-фильтрации за счёт блокировки как злоумышленников, так и внутренних устройств, пытающихся использовать сервисы DoH. Модуль прост в настройке и интегрируется с Ideco NGFW через настройки DNS-сервера, а в будущем будет доступен в центральной консоли Ideco Center. Важной особенностью DNS-фильтрации является её быстрое и простое внедрение — всего за полчаса. Кроме того, DNS предоставляет возможность блокировать контент и приложения с помощью 65 категорий и имеет обширную базу данных, которая покрывает почти 99% видимой части интернета и обновляется ежедневно.

Новый вектор развития в защите компаний на уровне DNS — использование ИИ, где включаются более 120 классификаторов и языковых моделей, чтобы обеспечить надёжную защиту от разнообразных угроз. Более того, интеграция с ICANN позволяет получать информацию о новых зарегистрированных доменах в реальном времени, что позволяет своевременно выявлять потенциальные угрозы. Как правило, в базах собраны исторические данные о владельцах доменов и их взаимосвязях, что позволяет анализировать каждый запрос и выявлять возможные угрозы. Для защиты компании рекомендуем использовать алгоритмы, основанные на расстоянии Ливенштайна, чтобы защитить от туннелирования внутри DNS-трафика, что позволит отслеживать домены, которые пытаются маскироваться под известные марки и бренды, и блокировать их запросы.

Например, Sky Security использует проактивный подход к защите от новых угроз, анализируя недавно зарегистрированные домены. Вместо блокировки всех новых доменов превентивно Sky Security собирает информацию о них и строит графы связанности, чтобы определить их историю и связь с известными сетями. Это позволяет выявлять потенциально вредоносные домены ещё до того, как они станут активными, основываясь на их связи с известными злоумышленниками. Таким образом, они блокируют домены, регистрируемые на сетях, известных своей вредоносной активностью.

БОЕВОЙ ПУТЬ

КАК РАЗРАБАТЫВАЛСЯ ФУНКЦИОНАЛ СТАТИЧЕСКОЙ И ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ В COREBIT.NGFW

Алексей ГРОМОВ
руководитель отдела разработки компании КорБит (входит в Холдинг ЦИКАДА)

Любой современный межсетевой экран, а тем более многофункциональный межсетевой экран уровня сети, не может нести гордое имя NGFW без функций статической и динамической маршрутизации сетевого трафика. Поэтому перед нашей командой разработки CoreBit.NGFW встали задачи исследования и реализации данных функциональных блоков. Основной проблемой было то, что задачи необходимо было решать в существующем ядре системы. На момент проработки этого вопроса ядро системы представляло собой инструмент глубокого анализа пакетов (DPI), позволяющий выстроить высокопроизводительный и масштабируемый конвейер фильтрации пакетной и сессионной нагрузки на всех уровнях МВОС.

DPDK — КРАЕУГОЛЬНЫЙ КАМЕНЬ

Когда мы разрабатывали ядро системы, то сразу отказались от использования стандартного сетевого стека Linux. Основных причин было две: это недостаточная пропускная способность (throughput), приводящая к потерям сетевых пакетов, а также большие задержки при прохождении сетевых пакетов (latency). Механизмы пакетирования на разных уровнях сетевого стека частично решали проблему с пропускной способностью, но не решали, а даже усугубляли проблему с задержками. К счастью, для преодоления этих трудностей стали появляться специализированные API обхода ядра сетевого стека Linux (kernel bypass). Одно из таких решений — DPDK, которое и стало краеугольным камнем при разработке архитектуры системы.

Благодаря DPDK мы смогли исключить указанные недостатки за счёт значительного уменьшения количества системных вызовов, изоляции ядер процессора, использования процессорного кеша, RSS-балансировки, а также разделения программной архитектуры на две плоскости — управления и передачи данных.

МЕТАДАННЫЕ ПАКЕТОВ

В плоскости передачи данных нами были разработаны специализированные блоки принятия решения, построенные на основе работы не с самими сетевыми пакетами, а с их метаданными, что позволило существенно увеличить скорость принятия решения о фильтрации пакетной и сессионной нагрузки. Для работы с метаданными пакетов разработаны собственные оптимизированные сборщики, используемые нами для обработки протоколов уровней L2–L4.

АЛГОРИТМЫ МАРШРУТИЗАЦИИ

Алгоритмы принятия решений о маршрутах прохождения пакетов, разработаны с использованием структур DPDK, позволяющих хранить данные в хеш-таблицах RTE_HASH. Поиск данных осуществляется с использованием алгоритма LPM (Longest prefix match), реализованного в API «RTE_FIB».

МЕХАНИЗМЫ ЗАЩИТЫ

При имплементации протоколов сетевого взаимодействия ARP и ICMP возникла необходимость разработки механизмов защиты сети от известных сетевых атак, таких как ARP-poisoning и ICMP-flood.

Учитывая, что весь функционал, связанный с обработкой сетевого трафика, разработан в плоскости передачи данных, нам пришлось имплементировать алгоритмы DHCP-клиента и DHCP-сервера, не забыв при этом разработать механизмы защиты от атак, направленных на этот протокол, таких как DHCP-starvation и DHCP-spoofing.

ДИАГНОСТИЧЕСКИЕ ИНСТРУМЕНТЫ

В дополнение к основным функциям межсетевого экрана в него были также включены инструменты проверки целостности и качества соединения (аналог утилиты Ping), а также функционал записи сетевых дампов, которые разрабатывались для внутренних процессов отладки. Мы посчитали, что было бы полезно добавить эти функции в качестве диагностических инструментов для наших клиентов.

ФУНКЦИОНАЛ NAT

В ходе выполнения проекта была проведена значительная работа по разработке механизмов преобразования и обратного преобразования IP-адресов, а также проброса портов протоколов транспортного уровня в локальную сеть и из неё. С использованием Generic flow API был разработан алгоритм агрегации прямого сетевого потока из локальной сети, а также алгоритм балансировки обратного сетевого потока в локальную сеть с использованием технологии Receive Side Scaling. Предложенный подход позволил внедрить механизмы NAT без снижения производительности функционала маршрутизации сетевых потоков.

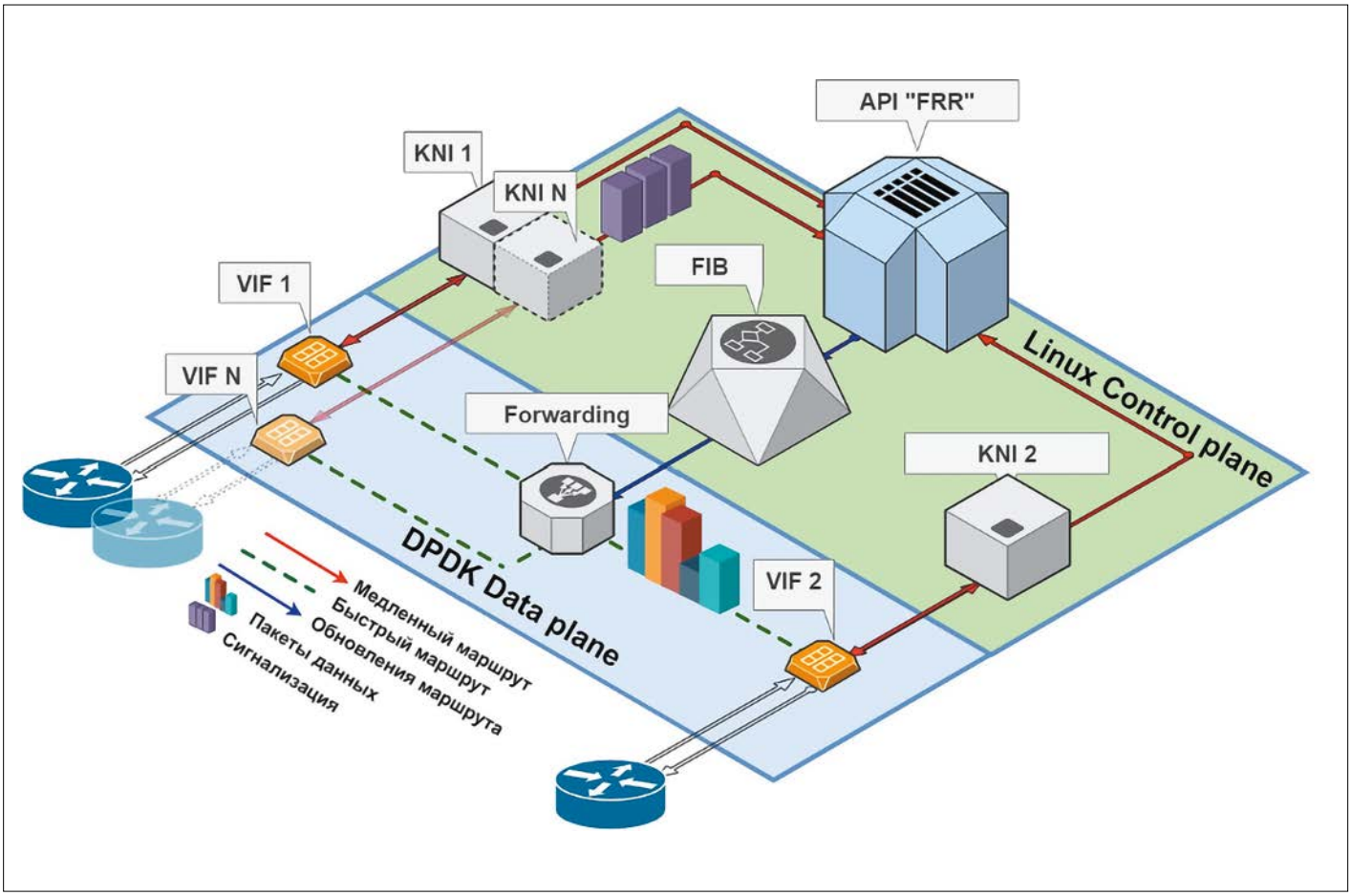


Рисунок 1. Схема взаимодействия DPDK и FRR

СИСТЕМНЫЕ ПРЕРЫВАНИЯ

Благодаря использованию аппаратных возможностей сетевых адаптеров в задачах снятия/добавления идентификаторов VLAN, подсчёта контрольных сумм протоколов транспортного уровня и протоколов межсетевого взаимодействия удалось исключить системные прерывания, вызываемые в программных блоках ядра системы для выполнения указанных операций.

ДИНАМИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Мы не стали повторять подвиг реализации алгоритмов статической маршрутизации для протоколов динамической маршрутизации. Проведя анализ существующих открытых API, мы остановили свой выбор на API «FRR». Интеграция FRR осуществлялась с использованием DPDK kernel NIC (KNI) с доступом к сетевому трафику через плоскость управления Linux, непосредственно используя разделяемую FIFO-память. Это позволило получить более высокие показатели за счёт сокращения количества системных вызовов и возможностей нулевого копирования пакета из разделяемой памяти.

Особенность работы API «FRR» с KNI заключается в том, что для приёма и передачи сетевого трафика по протоколам BGP и OSPF создаются отдельные виртуальные интерфейсы (VIF). В тот момент, когда API «FRR» получает данные о маршруте, он отправляет их на интерфейс FIB push, а VIF прослушивает этот интерфейс на предмет обновлений маршрутов и заносит изменённые данные в таблицу маршрутизации. Обновления маршрутов предписывают ядру плоскости данных (Data plane) перенаправлять трафик в соответствующий VIF. Благодаря этому сигнализация протоколов маршрутизации следует по медленному пути через KNI к API «FRR», но при этом весь сетевой трафик передаётся по быстрому пути через плоскость управления данных. Интеграция API «FRR» позволила реализовать функционал динамической маршрутизации сетевых потоков по протоколам BGP и OSPF без ухудшения ключевых показателей эффективности функционирования нашего продукта (рис. 1).

ОЦЕНКА РЕАЛИЗАЦИИ АЛГОРИТМОВ

Стоит отметить, что все оценки практических реализаций наших алгоритмов, используемых при разработке статической и динамической маршрутизаций, мы проводим по собственным методикам нагрузочного и стресс-тестирования с применением ПО IxNetwork и нагрузочных карт тест-центра IXIA с сетевыми интерфейсами 100GE, а также на трафике реальных вторичных сетей передачи данных.

Мы готовы предоставлять решение на пилот нашим заказчикам уже с IV квартала 2024 года.

ОТЕЧЕСТВЕННЫЕ СРЕДСТВА СЕТЕВОЙ ЗАЩИТЫ

КРИТЕРИИ ОЦЕНКИ ТАКТИКО-ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК И ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ

Илья ШАРАПОВ
генеральный директор компании ТСС

После ухода зарубежных вендоров стало очевидным, что отечественные средства сетевой защиты не идеальны, обладают недостатками и реализуют достаточно ограниченный набор функций безопасности.

В настоящее время для средств сетевой защиты используют различные названия: UTM, NGFW, USG, Enterprise firewall. Сегодня разделение продуктов условное, а их название, как правило, чисто маркетинговый ход. Многие, по крайней мере в России, такие продукты называют NGFW, что не мешает другим вендорам в зависимости от реализуемых функций безопасности давать им другие названия. Например, у Check Point существует четыре готовых набора функций безопасности, каждый из которых зовут по-разному: NGFW, SWG, NGTP, NGDP.

Очевидно, что на практике могут использоваться продукты, все функции безопасности которых или только некоторые из них прошли процедуру сертификации, а также средства, которые на сертификацию не представлялись или только находятся в процессе сертифицирования.

Например, компания ТСС в настоящее время разрабатывает и производит следующие продукты.

- МКСЗ Diamond VPN/FW — программный, программно-аппаратный многофункциональный комплекс сетевой защиты, представляющий собой UTM-решение, объединяющее в своём составе функционал криптографической защиты информации в каналах связи (СКЗИ), межсетевого экранирования (МЭ) и обнаружения вторжений (СОВ).
- МКСЗ Diamond NEXT — программный, программно-аппаратный многофункциональный комплекс сетевой защиты, являющийся дальнейшим развитием МКСЗ Diamond VPN/FW. В настоящее время комплекс включает в свой состав функционал СКЗИ, МЭ, СОВ, а также отражения атак (СОА). СКЗИ, вошедшее в состав комплекса, имеет сертификат ФСБ России, остальные средства готовятся для их представления на сертификацию в ФСТЭК России и ФСБ России. В дальнейшем в комплекс будут включаться другие средства и механизмы защиты.
- МКСЗ Diamond NEXT FW — программно-аппаратный многофункциональный комплекс сетевой защиты, являющийся дальнейшим развитием МКСЗ Diamond VPN/FW. Комплекс включает в свой состав средства и механизмы защиты информации, удовлетворяющие требованиям ФСБ России и ФСТЭК России, включая «Требования по безопасности информации к многофункциональным межсетевым экранам уровня сети».

Функции безопасности, требования к которым не установлены в нормативно-методических документах ФСТЭК России, должны указываться в задании по безопасности и проходить оценку соответствия установленным порядком.

Возникает вопрос: на базе каких критериев осуществлять сравнение и выбор комплексов NGFW? Очевидно, что для одной группы пользователей все критерии являются необязательными, для других обязательные критерии определены в нормативно-правовых и методических документах РФ.

Очевидно, что для одной группы пользователей все критерии являются необязательными, для других обязательные критерии определены в нормативно-правовых и методических документах РФ

КРИТЕРИИ

1. Функционал комплекса и сведения о его сертификации

Должен быть представлен перечень входящих в состав комплекса средств и механизмов защиты информации с указанием сведений о сертифика-

ции — по каким требованиям проводилась сертификация.

Должен быть представлен план развития и сертификации комплекса.

Должна быть представлена информация о возможности поставки комплекса за границу.

Выводы о целесообразности применения комплекса пользователь может сделать из соображений соответствия комплекса модели угроз.

2. Функциональные характеристики средств и механизмов защиты комплекса

Должны быть представлены функциональные характеристики декларируемых средств и механизмов защиты информации. Например, для МЭ: фильтрация в режиме l2 (в режиме коммутатора), фильтрация в режиме l3 (в режиме маршрутизатора), фильтрация по расписанию, синхронизация правил фильтрации с централизованной платформой управления, группировка сетевых адресов/сетевых портов, логирование правил фильтрации, фильтрация по доменному имени, возможность создания независимых контекстов фильтрации с персональными правилами фильтрации для заданной группы, возможность фильтрации ipv6, экспорт/импорт политик фильтрации в формат xml; для СОВ: работа с трафиком в активном (спв) и пассивном (сов) режимах, еженедельные обновления базы разрешающих правил (более 35 000 активных сигнатур), возможность написания собственных сигнатурных правил, централизованное и локальное обновление сигнатур, интеграция с механизмами межсетевого экранирования, возможность записывать сетевой трафик с атакой в формате pcap.

3. Дополнительные возможности комплекса

Учитывая, что комплекс — сетевое устройство, дополнительные возможности его использования в сети связи являются крайне важной характеристикой комплекса и должны быть представлены в полном объёме с планом развития комплекса, например:

- поддержка технологий Layer2: поддержка Vlan(802.1q)/Q-in-Q (802.3ad), поддержка LACP(803.3ad)/XOR, поддержка L2overL3, поддержка работы сетевых интерфейсов, в режиме bridge, поддержка STP;
- отказоустойчивость и резервирование: поддержка отказоустойчивого кластера, синхронизация между группами, поддержка нескольких провайдеров, поддержка режима bypass, резервирование питания;
- поддержка технологий Layer3: поддержка статической маршрутизации, динамической маршрутизации (OSPFv2, OSPFv3, RIPv2, RIPng, BGPv4, BGPv6, IS-IS, PIM, PIMv6, BFD, LDP), маршуртизация multicast (PIM/IGMP), Policy-based routing/virtual routing and forwarding, маршрутизация по дополнительным критериям (сетевой адрес источника, сетевой интерфейс источника, combo);
- сопутствующие технологии и протоколы: поддержка DHCP, DHCP Relay, DHCP Client, поддержка NTP, поддержка SNMP, поддержка Rsyslog, поддержка GRE tunnel, поддержка VxLan, поддержка Link aggregation (Round-robin, Active-Backup, Broadcast, XOR), разграничение прав доступа, логирование действия пользователей, поддержка ролевых политик, поддержка балансировки трафика между несколькими провайдерами, планировщик задач, NAT/PAT (Static, dynamic, port-forwarding, twice-nat), Backup настроек, поддержка совместимости с тонким клиентом.

4. Тактико-технические характеристики средств и механизмов защиты комплекса

Должны быть представлены основные тактико-технические характеристики средств и механизмов защиты информации комплекса, методики тестирования и программно-аппаратные, программные измерительные средства. К основным характеристикам комплексов относится скорость и вносимые задержки. Должны быть представлены значения данных параметров на пакетах различной длины. Для МЭ дополнительно необходимо указывать, для какого количества правил фильтрации зафиксирована скорость. Должна быть обеспечена возможность демонстрации и проверки декларируемых параметров на стендах.

5. Аппаратные платформы

В зависимости от условий эксплуатации, пропускной способности каналов связи, тактико-технических характеристик комплексов могут использоваться различные по мощности аппаратные платформы (сетевые сервера) или их совокупность. Таким образом, должны быть отдельно представлены как результаты тестирования каждого средства защиты или механизма защиты на каждой из представляемых платформ, так и результаты тестирования комплекса на аппаратной платформе на одном или нескольких серверов в целом. При этом должна быть представлена стоимость как комплекса, так и стоимость владения таким комплексом при его эксплуатации.

6. Адаптация комплекса

Должна быть обеспечена возможность: совместной работы (интеграции) с другими системами безопасности, работы в различных условиях эксплуатации (в сетях связи разного качества и стабильности работы), работы сетях связи разной топологии, в виртуальных средах и т.п.

7. Система управления комплекса

Немаловажный фактор — удобство системы управления комплексом. Центр управления должен поддерживать централизованное управление всеми компонентами системы, обеспечивать мониторинг состояния, а также возможность оперативного реагирования на угрозы. Поддержка ролей и разграничения прав доступа также играет важную роль для обеспечения безопасности.

* * *

Таким образом, выбор отечественного NGFW — это сложный и ответственный процесс, который требует учёта множества факторов, начиная от функциональности и сертификации продукта и заканчивая его техническими характеристиками и возможностями адаптации под нужды конкретного предприятия.

***Видимость** — это непосредственное наблюдение отдельных явлений, в то время как **реальность** — это система результатов наблюдений, связанных между собой*
Г. Галилей

НАБЛЮДАЕМОСТЬ NGFW

ОДНИМ ИЗ КЛЮЧЕВЫХ АСПЕКТОВ ОБЕСПЕЧЕНИЯ НАДЁЖНОСТИ И ЭФФЕКТИВНОСТИ ЯВЛЯЕТСЯ НАБЛЮДАЕМОСТЬ СИСТЕМЫ. РАССМОТРИМ ЭТУ ТЕМУ НА ПРИМЕРЕ NGFW

Игорь ХМЕЛЁВ
руководитель группы KK,
НПО «Эшелон»

ОПРЕДЕЛЕНИЕ НАБЛЮДАТЕЛЬНОСТИ СИСТЕМЫ

Термин «наблюдаемость» встречается в различных научных дисциплинах, таких как философия, математика, физика, химия, биология и теория управления. Он связан с состоянием системы, которое можно оценить с помощью прямых или косвенных методов. Прямой метод исследования предполагает непосредственное наблюдение или измерение объекта. Косвенный метод предполагает получение информации через промежуточные источники или интерпретацию без прямого доступа к объекту изучения. Например, прямой метод — когда мы самостоятельно следим за системой и знаем её состояние, а косвенный — когда пользователи системы сообщают нам о проблеме.

Наблюдаемость — это свойство, которое описывает состояние системы и включает в себя:

- мониторинг — постоянное наблюдение за состоянием системы;
- метрики — количественные показатели для оценки состояния системы;
- трассировка — установка причинно-следственных связей.

Повышение наблюдаемости переводит состояние системы из чёрного ящика в белый ящик, то есть процессы, происходящие в системе, становятся более открытыми и предсказуемыми (рис. 1).

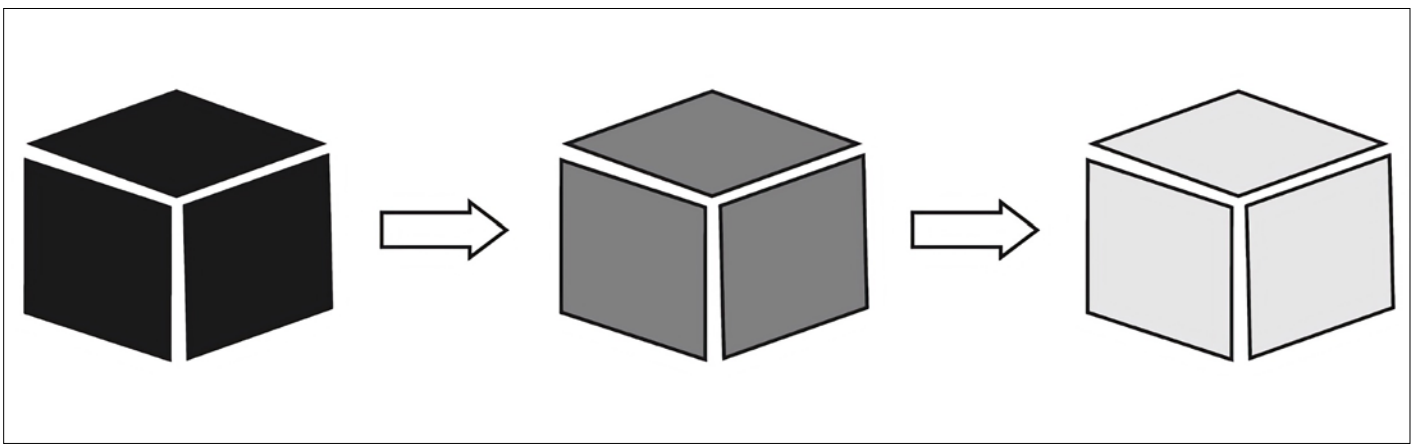


Рисунок 1. Повышение наблюдаемости переводит состояние системы из чёрного ящика в белый ящик, то есть процессы, происходящие в системе, становятся более открытыми и предсказуемыми

Согласно теории управления, можно контролировать только ту систему, которая поддаётся наблюдению. Если работа системы не соответствует нашим ожиданиям, то благодаря наблюдаемости мы можем выявить проблему и возможную причину её появления.

ЗНАЧЕНИЕ НАБЛЮДАЕМОСТИ В NGFW

NGFW, помимо функций безопасности и защиты периметра, также обеспечивает сетевые функции, поэтому любые сбои или замедления в его работе могут негативно сказаться на бизнес-процессах организации.

При настройке и эксплуатации NGFW могут встречаться следующие проблемы:

- проблемы в каналах связи (повреждения кабеля, ошибки автосогласования, ухудшение характеристик оптических линий связи, недоступность шлюза, ухудшение пропускной способности каналов связи);
- неточности в настройке сетевых функций (IP-адресация, таблица маршрутизации и пр.);
- проблемы в интеграции с внешними системами (динамическая маршрутизация, построение туннелей, доступность DNS, доступность каталога с пользователями и пр.);
- не оптимизированные и избыточные настройки межсетевого экрана, а также средств контроля и анализа сетевого трафика, которые могут приводить к ложным срабатываниям, а также негативно влиять на производительность NGFW;
- отсутствие данных о текущей загрузке NGFW и запаса его производительности;
- отсутствие информации о влиянии настроек компонентов анализа сетевого трафика и количества активных сигнатур на производительность NGFW;
- отсутствие информации о синхронизации между устройствами кластера NGFW, а также возможности быстрого переключения на резервный в случае отказа основного;
- неизвестность фактического состояния оборудования и вероятности его отказа;
- отсутствие независимого хранения актуальных бэкапов конфигурации NGFW;
- избыточное журналирование событий, которое может приводить к увеличению нагрузки на диск и, как следствие, влиять на работу всей системы;
- неверно настроенное время хранения журналов и их ротации может привести к уменьшению времени хранения записей или же к переполнению диска;
- нехватка информации о состоянии системы затрудняет поиск и устранение проблемы, поэтому её решение занимает больше времени;
- отсутствие уведомлений администратора о возможных сбоях, аномалиях или атаках может приводить к увеличению времени реакции на инцидент;
- сложность отслеживания причины и следствий, из-за чего процесс настройки становится итеративным. На каждом этапе настройки необходимо производить оценку его влияния на систему.

Поскольку NGFW представляет собой сложную систему из множества компонентов, свойства которых могут повлиять на функционирование NGFW, параметры наблюдаемости можно разделить на следующие группы:

- функционирование компонентов NGFW;
- настройка компонентов NGFW;
- оценка состояния отказоустойчивости NGFW;
- наличие обновлений для компонентов NGFW;
- нагрузка на аппаратные компоненты (CPU, ОЗУ, ПЗУ, сетевых адаптеров, температура);
- заполнение жёсткого диска;
- контроль системы питания (резервирование, состояние ИБП);
- переполнение очереди обработки сетевых пакетов в компонентах NGFW;
- данные о сетевом трафике с разным уровнем детализации;
- состояние аппаратных компонентов системы (наработка на отказ, эффективность работы системы охлаждения и пр.);
- состояние сетевой коммутации и интеграция с внешними системами.

Чем больше параметров мы можем контролировать, тем выше у нас наблюдаемость. При высокой наблюдаемости мы можем добиться следующих результатов:

- упростить управление системой можно с помощью отслеживания её функционирования после обновлений или изменений в настройках, которые могут ухудшить работу системы;
- улучшить понимание внутреннего состояния системы и её компонентов, что позволит более эффективно осуществлять управление;
- быстро обнаруживать и устранять проблемы, что позволит минимизировать простой в бизнес-процессах;
- выявлять проблемы и их причины, что позволяет предотвращать их возникновение в будущем и обеспечить стабильную работу системы, повысить её надёжность и эффективность;
- выявлять потенциальные проблемы до того, как они становятся критическими;
- предоставлять производителю NGFW более подробную информацию о выявленной проблеме и увеличивать скорость реакции технической поддержки;
- выявлять узкие места в функционировании системы;
- предсказывать поведение системы в различных ситуациях;
- оптимизировать настройки; имея полную картину работы системы, можно легко определить, какие настройки нуждаются в оптимизации;
- выполнять оценку загрузки оборудования, что позволяет определить, насколько эффективно используется существующее оборудование;
- выполнять оценку запаса по производительности, что помогает понять, какой объём работы может выполнить система без снижения качества обслуживания пользователей; это особенно важно при планировании расширения бизнеса или внедрении новых функций, когда необходимо обеспечить достаточную производительность системы для удовлетворения растущих потребностей;

◆ выявлять подозрительную активность и предотвращать атаки;

◆ выявлять аномалии в функционировании системы в нештатных режимах работы — это важный этап в обеспечении надёжности и стабильности информационных систем, поскольку аномалии могут проявляться в виде неожиданных ошибок, сбоев, замедления работы системы или других проблем. Они могут быть вызваны различными факторами, такими как неправильная настройка, ошибки в программном обеспечении, проблемы с оборудованием и пр.;

◆ упрощение процесса оценки соответствия системы требованиям нормативных документов, что позволяет быстрее и эффективнее проводить проверку на соответствие законодательным и отраслевым стандартам; это особенно важно для организаций, которые должны соблюдать строгие правила и нормы в своей деятельности;

◆ автоматизация процессов диагностики и предупреждения отказов позволяет высвободить человеческие ресурсы; это даёт возможность сотрудникам сосредоточиться на более сложных и творческих задачах.

СЛОЖНОСТИ, СВЯЗАННЫЕ С НАБЛЮДАЕМОСТЬЮ

При выборе критериев наблюдаемости необходимо отталкиваться от специфики объекта, определить важные параметры и соблюсти баланс между их количеством и необходимостью. Эти параметры напрямую связаны с требованиями к объекту, где функционирует NGFW. Избыточное количество контролируемых параметров усложнит их хранение и работу с ними, а недостаточное — снизит наблюдаемость системы.

Реализация наблюдаемости в NGFW может быть сложной задачей, которая требует тщательного планирования и выполнения. Вот некоторые из проблем, с которыми можно столкнуться при внедрении наблюдаемости.

◆ Выбор метрик. Необходимо определить, какие именно метрики будут использоваться для наблюдения за системой.

◆ Сложность найти минимальный набор данных, который необходим для обеспечения достаточной наблюдаемости. Такой набор может оказаться достаточно большим, что приведёт к усложнению системы мониторинга.

◆ Проблема полноты: недостаточно данных о функционировании системы из-за их отсутствия или невозможности их собрать.

◆ Проблема актуальности: данные могут быть устаревшими, например, получены от старой версии до обновления.

◆ Проблема валидации: данные могут описывать неактуальное состояние системы, например, при другой конфигурации.

◆ Сложность анализа, которая может быть связана с большим объёмом данных.

◆ Сложность анализа, которая может быть связана с неопределённостью и вероятностными характеристиками измеряемых величин, например, сетевой трафик может меняться в широком диапазоне.

◆ Сложность анализа, которая может быть связана с высокой степенью связанности между данными, полученными от разных компонентов NGFW. Например, замедление пропускной способности может быть связано с троттлингом процессора (уменьшением частоты), вызванным повышением его температуры из-за увеличения нагрузки на процессор, которую создал компонент NGFW после обновления базы сигнатур, а также по причине неэффективной системы охлаждения.

◆ Сложность в определении причины возникновения проблемы, которая заключается в необходимости проведения детального анализа большого количества данных и выявления взаимосвязи между ними.

◆ Часть параметров невозможно измерить без вывода NGFW из эксплуатации. К таким параметрам относится, например, износ оборудования.

◆ Для эффективного мониторинга и анализа работы системы необходимо разбираться в архитектуре системы.

РАЗВИТИЕ НАБЛЮДАЕМОСТИ NGFW

В развитии наблюдаемости NGFW можно выделить несколько ключевых направлений:

◆ определение минимального необходимого набора ключевых параметров, которые позволяют оценить состояние системы;

◆ унификация формата данных, передаваемых в систему мониторинга, что позволяет упростить их обработку и анализ;

◆ разработка типовых методик для проверки функционирования, диагностики, измерения производительности и безопасности NGFW;

◆ расширение возможностей мониторинга NGFW с учётом бизнес-процессов, которое обеспечит связывание функционирование NGFW и показателей бизнес-процесса;

◆ использование искусственного интеллекта (AI) и машинного обучения (ML) для выявления аномалий и предсказывания потенциальных проблем, что повысит надёжность функционирования NGFW;

◆ автоматизация процессов диагностики и предупреждения отказов, возникающих в NGFW.

Одним из направлений развития наблюдаемости может стать не только отслеживание текущего состояния системы, но и прогнозирование будущих проблем. Это позволит автоматизировать процессы обнаружения и устранения неполадок, а также интегрировать наблюдаемость во все аспекты IT-инфраструктуры и бизнес-процессов.

ЗАКЛЮЧЕНИЕ

Наблюдаемость играет важную роль в обеспечении эффективной работы NGFW. Несмотря на сложности, связанные с её реализацией, она позволяет администраторам оперативно реагировать на инциденты безопасности, оптимизировать настройки NGFW, следить за его функционированием, повышать надёжность, а также упрощать проверку соответствия настроек NGFW требованиям нормативных документов.

RA VPN, NAC, ZTNA… ПОРА РАЗОБРАТЬСЯ

ОБЗОР ТЕХНОЛОГИЙ И ДОСТУПНЫХ РЕШЕНИЙ

Евгений ОЛЬКОВ
технический директор TS Solution

За последние пару лет аббревиатура VPN прочно вошла в нашу жизнь. И если раньше эта технология была уделом «гиков» или только высокотехнологичных компаний, то сейчас этим пользуются практически все. Причина простая – удалёнка. С началом пандемии большинство компаний были вынуждены в срочном порядке «высаживать» сотрудников домой и организовать им удалённую работу.

Вскоре все осознали, что период удалёнки «немного» затянется (а у кого-то и вовсе стал стандартом) и, кроме быстрого развёртывания удалённого доступа, нужно ещё думать и о безопасности в условиях новой реальности. И этот вызов куда серьёзнее для любого ИБ-специалиста. Пользователи могут подключаться откуда угодно и с чего угодно. А если их учётная запись будет скомпрометирована, то под угрозой оказывается вся корпоративная сеть.

Все эти проблемы, конечно же, решаемы, и существует множество инструментов и классов средств защиты. На этой волне уже долгое время в ИБ-медиапространстве звучат такие термины, как RA VPN, ZTNA, 2FA, PAM и т.д. Неподготовленному человеку довольно трудно сразу разобраться во всех этих терминах. Что они означают, когда и как их применяют и в чём их преимущества? Чтобы расставить все точки над i, мы и создали эту небольшую статью. Помимо обзора этих технологий, мы также акцентируем внимание на доступных на сегодняшний день решениях, так как после февраля 2022 года выбор существенно уменьшился.

REMOTE ACCESS VPN

VPN (Virtual Private Network) – виртуальная частная сеть, как пишут в «Википедии». Здесь важно сразу разделять две большие категории этого самого VPN:

- **Site-to-Site VPN** применяется для объединения нескольких офисов. Классический пример: сотрудникам филиалов требуется доступ к ресурсам центрального офиса.

Если говорить простым языком, то Site-to-Site VPN позволяет организовать защищённый (шифрованный) канал или туннель между офисами через публичную сеть Интернет. Это быстро, удобно и дёшево (в отличие от организации выделенного кана-

ла, что и не всегда возможно). Чаще всего для этого используются технологии IPSec, которые поддерживаются практически любым маршрутизируемым сетевым устройством (Cisco, D-Link, Mikrotik и т.д.).

◆ **Remote Access VPN (RA VPN)** — тот самый VPN для организации удалённого доступа пользователей к сервисам компании.

Здесь уже строится защищённый туннель между конкретным устройством пользователя и VPN-шлюзом. Удалённый сотрудник может подключаться с компьютера (Windows, Linux, MacOS) или мобильного устройства (Android, iOS). Обычно на устройство устанавливается специальный VPN-клиент, и чаще всего он работает, используя всё тот же IPSec или же более «модный» SSL. В качестве VPN-шлюза может выступать межсетевой экран или маршрутизатор, которые поддерживают IPSec/SSL.

Мы не сможем в рамках одной небольшой статьи рассмотреть оба варианта. Поэтому давай сконцентрируемся на особенностях RA VPN. И начнём, пожалуй, с вопроса: «А на чём раньше строили RA VPN?» Раньше — до февраля 2022-го. И тут есть несколько безоговорочных лидеров:

1. **Cisco AnyConnect + Cisco ASA** (а иногда и + Cisco ISE). Решение корпоративного уровня. До сих пор во многом является эталоном в сфере RA VPN.

2. **OpenVPN/Wireguard.** Бесплатный вариант. Причём WireGuard становится всё более популярным. Клиенту требуется установка специального VPN-клиента.

3. **Встроенный функционал** сетевых устройств **RA VPN**. Как писал выше, практически все маршрутизаторы / межсетевые экраны поддерживают работу в качестве VPN-шлюза (IPSec). Для подключения пользователь может использовать встроенные функции операционной системы (native-vpn-клиент).

Также довольно большой популярностью пользовались решения Fortinet, Palo Alto и Check Point (последний до сих пор доступен на отечественном рынке).

С недавних пор рынок изменился, а потребность в RA VPN только растёт. Кто-то использует VPN исключительно для админов, кто-то и для обычных пользователей, предоставляя им доступ к корпоративным ресурсам. Какие же типовые требования традиционно предъявляли для решений по организации RA VPN?

1. Аутентификация и авторизация. Необходима поддержка интеграции с AD, Radius и системами двухфакторной аутентификации (2FA).

2. Гибкие политики доступа на основе групп, ролей, профилей.

3. Поддержка современных протоколов шифрования (IPSec, TLS и т.д.).

4. Детализированное журналирование и мониторинг состояния.

5. Поддержка различных платформ (WIndows, Linux, MacOS, Android, iOS).

6. Отказоустойчивость (поддержка различных технологий кластеризации).

Здесь важно понимать, что сам концепт RA VPN довольно стар и появился несколько десятков лет назад. В связи с этим традиционные требования уже не отвечают современным потребностям, так как существует ряд проблем:

1. В большинстве случаев доступ удалённым пользователям предоставляется на L3 уровне, то есть открывается полный доступ до конкретного ip-адреса или (даже чаще) до целых подсетей. Это, в свою очередь, увеличивает площадь возможной атаки в случае компрометации учётной записи или устройства пользователя.

2. Пользователи могут подключаться к корпоративной сети со своих устройств (BYOD), которые не всегда соответствуют стандартам безопасности. Компьютер удалённого сотрудника может быть банально заражён (кейлогер, шифровальщик, криптомайнер), а это может привести к распространению вирусов уже в корпоративную сеть или утечке конфиденциальных данных.

3. Для подключения требуется VPN-клиент, что может вызвать трудности при его распространении на большое количество пользователей с различными операционными системами. Даже сейчас довольно трудно найти решение, которое поддерживало бы все виды и все версии ОС.

4. Нет возможности мониторить или запрещать действия удалённого пользователя в рамках VPN-трафика. Вы просто НЕ видите, что происходит после подключения удалённого пользователя.

Часть проблем удаётся решить, часть остаётся открытыми. К примеру, одним из наиболее важных дополнений к классическому RA VPN являются NAC-системы.

NAC

Network Access Control (NAC) — система, которая позволяет выполнять проверку рабочей станции перед подключением к корпоративной сети. NAC может работать как без специальных агентов (802.1x), так и с агентами. Второй вариант чаще всего применяется именно для RA VPN, когда перед подключением удалённого пользователя его компьютер может быть проверен на:

◆ наличие критических обновлений системы;
◆ наличие антивирусного ПО;
◆ наличие необходимого ПО;
◆ запрещённые системные процессы;
◆ хеш-суммы отдельных файлов;
◆ и т.д.

Сам концепт NAC существует очень давно, и решения данного класса применяются не только для RA VPN, но и для проводного/беспроводного доступа внутри корпоративной сети. Наиболее популярные решения:

◆ Cisco ISE;
◆ ForeScout;
◆ PortNox;
◆ TruNAC (доступен в России).

На отечественном рынке выбор значительно меньше:

◆ Efros Defence Operations;
◆ AxelNAC

Несмотря на то что NAC-решения позволяют существенно повысить безопасность и управляемость удалённого доступа, всё же ещё остаются серьёзные проблемы:

◆ всё ещё регулирование на уровне сетей;

- отсутствие мониторинга после подключения;
- отсутствие контроля действий в рамках разрешённого трафика.

Решить эти и многие другие проблемы можно в рамках ZTNA.

ZTNA

Zero Trust Network Access (ZTNA) — принцип нулевого доверия в сетевом доступе. Первое, что нужно здесь усвоить, — ZTNA — это не технология, это концепт. Причём этот концепт используется не только в рамках RA VPN, но и внутри корпоративных сетей, внутри баз данных, внутри микросервисных архитектур и т.д. Мы рассмотрим этот концепт в рамках задачи RA VPN.

Главная предпосылка зарождения ZTNA — уход от исключительно периметральной защиты к защите индивидуальных транзакций. Такой подход ещё называют SDP (software defined perimeter) или «программно определяемый периметр». Концепт ZTNA был сформулирован в далёком 2004 году в публикациях компании Forrester (да-да, не всё идёт от Gartner!).

Так как это концепт, разные компании могут по-разному реализовать данный принцип. Есть компании, которые внедряют ZTNA в рамках одного решения от одного вендора. Другие могут реализовать ZTNA на нескольких решениях. Главное, чтобы по итогу вы могли делать следующее:

1. Проверка пользователя

- интеграция с AD/LDAP/Radius;
- 2fa (SMS/OTP/Email/Token).

2. Проверка устройства

Так называемый постчуринг или комплаенс:

- Device ID;
- наличие обновлений/антивируса;
- наличие/отсутствие процессов;
- время подключения;
- место подключения;
- и т.д.

Если хост прошёл проверку, это не значит, что ему можно доверять. Его нужно всё время перепроверять!

3. Применение политики минимального доступа

Политика минимально необходимого доступа:

- доступ только по сервису (например, tcp 22, 80, 443 порт);
- доступ к приложению (публикация на портале);
- ограничение по времени;
- запрет определённых действий в рамках активного подключения (например, блокировка сторонних VPN или открытия CLI).

Один из принципов ZTNA: доступ к одному ресурсу не гарантирует доступ к другому. Авторизации подвергается каждое сетевое взаимодействие!

Если попробовать резюмировать, то получим, что ZTNA и RA VPN — это два разных подхода к обеспечению безопасного удалённого доступа к корпоративным ресурсам и информации. ZTNA реализует более гранулированный доступ, с контролем рабочих станций и сессий. RA VPN более простое решение по обеспечению удалённого доступа, на базе обычных сетевых взаимодействий.

Выбор между ZTNA и RA VPN зависит от конкретных потребностей вашей организации, уровня безопасности, масштабируемости и архитектурных предпочтений. Многие организации также могут рассматривать комбинированный подход, чтобы обеспечить максимальную безопасность и удобство для пользователей.

ZTNA НА ОТЕЧЕСТВЕННОМ РЫНКЕ

Как обстоят дела с RA VPN и ZTNA-решениями на отечественном рынке? Если коротко, пока не очень. После ухода зарубежных вендоров стало совершенно очевидно, что российские разработки нуждаются в очень серьёзной доработке под современные требования клиентов.

Давайте рассмотрим возможности наиболее заметных игроков рынка корпоративного сегмента на российском рынке (на сентябрь 2024 года):

«Континент» («Код Безопасности»):

- «Континент АП» (работает с 3.x, 4.X) — классический VPN;
- бесклиентский VPN («Континент TLS»);
- ZTN-клиент («Континент АП» + TLS);
- есть комплаенс проверки, но только перед подключением (NAC через скрипт);
- нет централизованного управления;
- есть интересная интеграция с «Сакура» (ближе к концепту ZTNA);
- Split Tunneling / Default route;
- интеграция с 2fa («Мультифактор», Indeed AM, Avanpost).

UserGate:

- нативные клиенты (Win, Linux, MacOS) + бесклиентский;
- UG Client (работает с UserGate 7.1);
- дорабатывается, пока только Windows;
- постоянная проверка станций + централизованное управление;
- есть Firewall / URL Filtering;
- базовый функционал EDR (сбор телеметрии);
- Split Tunneling / Default route;
- интеграция с 2fa («Мультифактор», Indeed AM, Avanpost).

Check Point:

- Mobile Access — классический VPN (Win, Mac), SSL-портал;
- интеграция с 2fa («Мультифактор», Indeed AM и т.д.);
- есть возможность проверки хоста (SCV), без централизованного управления;
- нет профилей;
- Harmony Endpoint — VPN, Compliance, EDR, AV, Firewall, App Control, Disk Encryption и т.д.;
- наиболее комплексное и зрелое решение;
- локальное и облачное управление;
- Quantum SASE (Perimeter 81).

Как видим, выбор невелик, но он всё же есть.

ЗАКЛЮЧЕНИЕ

Как уже было сказано, ZTNA — это всего лишь концепт без применения каких-то конкретных технологий. Этот концепт позволяет существенно повысить защищённость корпоративной сети, но не решает всех проблем. Надеюсь, мы сможем рассмотреть решения класса **SASE** в наших следующих статьях.

МЕТОДИКА СРАВНЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ NGFW

КАК ВЫБРАТЬ ОПТИМАЛЬНОЕ РЕШЕНИЕ ДЛЯ ВАШЕЙ СЕТИ

Денис БАТРАНКОВ
директор по продуктам ИБ ИКС Холдинг

Многие компании после приобретения межсетевого экрана нового поколения (NGFW) обнаруживают, что его реальная производительность в их сети отличается от заявленных в рекламных материалах значений. Почему это происходит, и как выбрать подходящую модель NGFW до покупки? Какими критериями лучше руководствоваться при выборе?

ЕСТЬ 5 СПОСОБОВ ПОДБОРА NGFW

1. Правильный: провести тестирование NGFW на собственном сетевом трафике.

2. Легкий: заказать тест производительности с учетом ваших параметров у производителя NGFW или его партнера.

3. Сложный: арендовать генератор трафика и самостоятельно протестировать NGFW в максимальных режимах на пилотном проекте.

4. Неверный: выбрать устройство, основываясь только на официальных маркетинговых материалах.

5. Быстрый: изучить результаты тестов, проведенных независимыми лабораториями.

ЧЕТЫРЕ КЛЮЧЕВЫХ ПАРАМЕТРА ОЦЕНКИ ПРОИЗВОДИТЕЛЬНОСТИ NGFW

1. Connections Per Second (CPS): максимальное количество новых соединений, которые NGFW может принять на анализ за одну секунду.

2. Concurrent Connections (CC): максимальное количество одновременных соединений в секунду с включенным анализом приложений и функциями защиты.

3. Total Throughput (TT): максимальная общая производительность устройства в битах в секунду.

4. Число заблокированных атак: эффективность системы предотвращения вторжений (IPS).

CONNECTIONS PER SECOND (CPS)

CPS показывает количество новых соединений, которые NGFW может обработать за секунду. Это критически важный параметр, так как для каждого нового соединения выделяется память и запускаются процессы анализа. Опыт показывает, что именно этот параметр часто становится узким местом в работе NGFW, особенно в финансовых организациях (рис. 1).

CONCURRENT CONNECTIONS (CC)

CC отражает максимальное количество одновременных соединений, которые NGFW может поддерживать с включенным анализом приложений и функциями защиты. Этот параметр зависит от объема оперативной памяти, производительности процессоров и включенного функционала. Включение дополнительных модулей анализа трафика может существенно снизить это значение. Для примера (см. рис. 1) в тестах pfSense количество одновременных сессий в режиме без инспекции — 2 600 000, в режиме с инспекцией — 1 200 000, а в режиме IPS — уже 270 000, т.е. снижение в 10 раз. Это не страшно. Из опыта, даже в очень больших сетях редко 1 000 000 соединений одновременно. Заметьте, что также снижается и CPS.

TOTAL THROUGHPUT (TT)

TT показывает максимальную общую производительность устройства, измеряемую в битах в секунду. Это суммарный объем входящего и исходящего трафика со всех интерфейсов NGFW при работающих функциях каждую секунду.

Во-первых, TT зависит от сложности анализируемого трафика и включенных функций анализа. Например, анализ SMB-трафика требует больше ресурсов из-за мультиплексирования файлов, а DNS-трафик может показывать низкий TT из-за большого числа коротких транзакций.

Во-вторых, TT напрямую коррелирует с количеством и типом проверок, применяемых к сетевому трафику. Рассмотрим следующие сценарии:

1. Базовая конфигурация: при активации только системы распознавания приложений L7 предотвращения вторжений (IPS) для HTTP-трафика наблюдается минимальное влияние на производительность.

2. Расширенная проверка файлов: внедрение антивирусного сканирования и анализа в песочнице для фай-

pfSense	B2B	Router mode	FW mode	IPS mode
HTTP CC	2.6M	2.6M	1.2M	270K
HTTP CPS stable	40K	40K	12.5K	2.0K
Attacks only	--	--	--	528/945
Attacks + HTTP CPS 2.0K	--	--	--	394/945

Рисунок 1. Значения параметров CC, CPS межсетевого экрана pfSense. Каждая строчка — отдельный тест с разным трафиком и разными режимами: маршрутизатор, firewall, IPS.

лов, передаваемых по HTTP и другим протоколам, существенно увеличивает нагрузку на систему.

3. Максимальная нагрузка: наиболее ресурсоемкими операциями являются расшифрование SSL-трафика (SSL Decrypt), применение технологий предотвращения утечки данных (DLP).

ЭФФЕКТИВНОСТЬ ЗАЩИТЫ

Число заблокированных атак является ключевым показателем эффективности NGFW. Важно помнить, что высокие значения производительности теряют смысл, если устройство не обеспечивает должный уровень защиты. Некоторые производители могут отключать функции безопасности для достижения высоких показателей производительности, что превращает NGFW в дорогостоящий маршрутизатор.

Посмотрите на иллюстрации (см. рис. 1): при включении системы предотвращения атак и подаче максимального трафика устройство снизило качество защиты. 528 атак оно остановило в спокойном режиме, и всего 394 под нагрузкой.

ЖУРНАЛИРОВАНИЕ

Журналирование оказывает значительное влияние на производительность NGFW, так как требует обработки большого объема текстовых данных. Часто производители тестируют скорость работы устройств с выключенным журналированием, что может привести к существенному снижению производительности при его включении в реальных условиях.

МЕТОДИКА ПРАВИЛЬНОГО ТЕСТИРОВАНИЯ NGFW

Для корректной оценки производительности NGFW необходимо измерять параметры CPS, CC и TT на реальном трафике вашей компании при включении всех необходимых функций безопасности. Рекомендуется следующий подход:

1. Использовать сетевой брокер для подачи трафика на NGFW. Это обеспечивает более точное тестирование по сравнению с использованием SPAN-портов, которые могут терять пакеты. Сетевой брокер позволяет протестировать и другие сетевые устройства безопасности, например, NDR, сетевой DLP или сетевую защиту баз данных. Вы можете подключить несколько различных NGFW на один сетевой брокер и этим обеспечить справедливый тест: на все устройства будет подаваться одинаковый трафик. Вам останется только включить в NGFW модули защиты.

2. После подключения NGFW через сетевой брокер или в разрыв сети, вы можете анализировать в реальном времени значения CC, CPS, TT, число заблокированных атак и загрузку процессоров и памяти в системе управления. Попросите написать нужное вам число правил безопасности по имени пользователя и приложению, например, 10000 правил. Если во время теста процессоры или память загружены на 100%, то вам нужно более мощное устройство. Рекомендуется учитывать ежегодный рост трафика в сети. И поэтому нужно взять устройство с запасом.

3. Часть функционала можно протестировать только в разрыв. Это функционал маршрутизации, NAT, QoS, трансляции VLAN, SSL Decrypt, Captive Portal, High Availability и другой. Для тестирования SSL Decrypt вам нужно будет сгенерировать специальные SSL сертификаты и сделать так, чтобы клиентские устройства им доверяли. Связано это с тем, что для работы функционала требуется делать подмену сертификата на NGFW. К сожалению, половину SSL трафика не получится расшифровать, поскольку многие приложения используют SSL pinning и проверку клиентских сертификатов. То есть механизм MITM уже не работает. Поэтому этот функционал часто тестируют, все-таки в лаборатории, хотя там уже будет искусственный трафик.

ИСКУССТВЕННЫЕ МЕТОДИКИ ТЕСТИРОВАНИЯ

Для лабораторного тестирования часто используются специализированные устройства, такие как IXIA BreakingPoint, которые генерируют различные типы трафика и атак. Существует два основных подхода к генерации трафика:

1. Подача однотипного трафика (например, HTTP-запросы и ответы с файлами 64 КБ).

Если вы изучаете официальный datasheet, внимательно читайте сноски: на каком именно трафике получены заявленные значения скорости и какие модули анализа трафика были включены

2. Подача разнородного трафика (Application Mix или Enterprise Mix — EMIX).

Оба подхода описаны в RFC9411, опубликованном в 2023 году. Проект NetSecOpen и компания CyberRatings (бывший NSS Labs) также публикуют методики тестирования NGFW. В России есть несколько тестовых лабораторий и публикаций.

Методики тестирования, которые создаются компаниями обычно длиной от 30 до 90 страниц, поскольку часто включают функциональные тесты. И прохождение всех тестов может занимать до 2 месяцев.

Учтите, что в лабораториях все тесты искусственные и в вашей сети трафик будет другой.

Если вы изучаете официальный datasheet, внимательно читайте сноски: на каком именно трафике получены заявленные значения скорости и какие модули анализа трафика были включены. Рекомендуется смотреть в поле Threat Prevention или Threat Protection, это значит, что в данном тесте точно включен IPS и контроль приложений. Еще рекомендуется узнать все ли сигнатуры IPS включены или только часть. Каждая сигнатура IPS влияет на скорость анализа. Обычно вендор тестирует на подмножестве сигнатур, которое называется default или optimized. Опять же для того, чтобы показать себя с лучшей стороны по производительности, а не по качеству защиты.

Стоит реагировать негативно, когда вам говорят про тестирование NGFW на UDP трафике. Это чисто маркетинговая задумка, потому трафик в вашей сети точно никогда не будет 100% на UDP, хотя на этом трафике NGFW выглядит как очень быстрый. На этом трафике NGFW в роли роутера, то есть устройство не анализирует контент UDP датаграмм. Тест на UDP показывает скорость работы сетевых карт, но никак не нагружает процессоры, которые отвечают за анализ контента. Расчет на то, что в datasheet будет смотреть человек, который не разбирается, что NGFW создан для анализа другого трафика.

Иногда в datasheet публикуются задержки трафика. Это прекрасно, что в лаборатории достигли 2 микросекунды задержки у пакетов UDP в режиме «все выключено». Но в вашей сети будет другой трафик, плюс вы включите защиту и задержки будут сильно больше.

ВАЖНЫЕ АСПЕКТЫ ПРИ АНАЛИЗЕ РЕЗУЛЬТАТОВ ТЕСТИРОВАНИЯ

Обращайте внимание на размер транзакции в тестах. Тесты на HTTP с размером транзакции 64 КБ обычно дают адекватное представление о будущей производительности NGFW в реальной сети. Если вам покажут тесты на HTTP 256Кб, то и общая пропускная способность будет в 4 раза больше чем на транзакциях 64Кб. Часто размер транзакции не указывают.

Кстати говоря, никто никогда не говорит, а что за файлы скачиваются в тестовом трафике: будет ли это картинка PNG или HTML с javascript или просто нули. Это типичная уловка тестов, ведь подавая одни нули в файле вы автоматически помогаете быстрее работать функционалу IPS, антивируса и другим движкам анализа. А если подать javascript, да еще с обфускацией — там NGFW придется потрудиться, а это нагрузка на процессор.

Если вы изучаете официальный datasheet, внимательно читайте сноски: на каком именно трафике получены заявленные значения скорости и какие модули анализа трафика были включены.

Помните, что тесты максимальных значений CPS, CC, TT и других параметров часто проводятся в искусственных условиях на однотипном трафике и не отражают реальную производительность устройства в смешанном трафике. В вашей сети это устройство точно выдаст другие значения CPS и TT, потому что там будет разнородный трафик.

ВСЮ ЛИ ФУНКЦИОНАЛЬНОСТЬ МОЖНО ПРОВЕРИТЬ В ЛАБОРАТОРИИ

У вашего NGFW будут внешние сервисы, с которыми идет взаимодействие: сервера Active Directory, LDAP, DNS, NTP, OCSP, CA, сервера обновлений, TI, системы аутентификации, MFA, API, ICAP, SIEM, SOAR. Они все вместе будут замедлять работу устройства.

Можно ли подключить и протестировать все эти сервисы в испытательной лаборатории? Вряд ли. Воспользуйтесь QR-кодом, чтобы посмотреть видеоролик про то, как проводят тестирования:

В РЕЗУЛЬТАТЕ

При выборе NGFW важно задавать конкретные вопросы о производительности устройства с учетом всех включенных функций защиты, типа трафика и размера транзакций. Например: «Какова производительность вашего NGFW со всеми включенными функциями защиты для HTTP-трафика с размером транзакции 64 КБ и с журналированием всех событий и типов файлов?»

Правильный подход к тестированию и оценке производительности NGFW поможет выбрать оптимальное решение, соответствующее реальным потребностям вашей сети.

РУТЕСТ
ООО «РУТЕСТ»
ИНН 9704189077
119019, РОССИЯ, г. МОСКВА,
ул. НОВЫЙ АРБАТ, ДОМ 10, оф. 47
sales@rutest.zone
8 (800) 777 22 88

Независимое нагрузочное тестирование L2-7 для ИТ и ИБ задач

Поставка оборудования и ПО ведущих производителей тестовых комплексов

Аренда решений и профессиональные услуги по тестированию

ixia spirent XINERTEL

- Собственная лаборатория и широкий спектр решений для демо и аренды
- 17 лет инженерной экспертизы, заказчики и партнеры в РФ и странах СНГ
- Независимая лаборатория, международные практики тестирования
- Уникальные услуги: лаборатория из облака, нагрузочное тестирование WiFi
- Решения на любой бюджет: аренда, подписки, спецпредложения
- Гарантия на оборудование и техническая поддержка: консультации, обучение, обновления

Преимущества

Аппаратные и виртуализированные тестовые решения от 1G до 800G

Функциональное, нагрузочное тестирование, а также тестирование реализации протоколов на соответствие RFC

Нагрузочное тестирование 4/5G и Wi-Fi (БС, транспорт, ядро, ИБ)

Тестирование эффективности и стабильности работы систем ИБ под нагрузкой в реальных сценариях

Тестирование L2-3, симуляция полного спектра протоколов сетевого транспорта и эмуляторы характеристик каналов связи

Максимальная повторяемость результатов, реалистичный трафик принятия взвешенных решений на основе реальных цифр производительности, емкости и эффективности

Решаемые задачи

- Выбор поставщика и импортозамещение
- Аргументация выделения бюджета на ИТ/ИБ проекты
- Сравнение и проверка конфигураций и дизайна
- Тонкий тюнинг ранее закупленных решений
- Проверка обновлений до их установки на сеть
- Внедрение новых технологий
- Контроль качества выпускаемой продукции
- Эффективные демо решений и проектов
- Поиск причин и ускорение решения проблем
- Проверка навыков и тренировка персонала

ЛЕДОКОЛ РОССИЙСКОГО КИБЕРБЕЗА

НА ВОПРОСЫ BIS JOURNAL ОТВЕЧАЕТ ВИЦЕ-ПРЕЗИДЕНТ ПО КИБЕРБЕЗОПАСНОСТИ СБЕРА СЕРГЕЙ ЛЕБЕДЬ

О КАДРАХ

— В Сбере мощная Служба кибербезопасности: есть Лаборатория кибербезопасности, RedTeam, SOC и множество других подразделений. Как вы закрываете кадровые вопросы? Где берёте специалистов в условиях всеобщего дефицита?

— Проблема дефицита кадров в сфере кибербезопасности является глобальной, выходящей за рамки России. Причина — тотальная цифровизация мира и общества и неразрывно связанные с ней риски и угрозы.

В Сбере функционирует ряд ключевых направлений: киберзащита инфраструктуры, DevSecOps, противодействие мошенничеству, защита персональных данных и конфиденциальной информации, криптография, экспертиза и методология, разработка и развитие новых продуктов кибербезопасности. Чтобы действовать на опережение, созданы Центр аналитики и Лаборатория кибербезопасности. Для каждого из этих направлений нужны свои уникальные эксперты, потому что универсального кибербезопасника найти или подготовить — задача очень сложная. Однако есть общий фундамент для всех. Это — ИТ.

Сегодня специалист по кибербезопасности — это прежде всего эксперт в ИТ со своей узкопрофильной специализацией в кибербезопасности. Причём иногда эта специализация выходит за рамки сферы кибербезопасности: финансисты, разработчики моделей искусственного интеллекта, математики, инженеры данных. Совместная работа специалистов с разными навыками и знаниями в нашей команде позволяет достигать синергетического эффекта и успешно реализовывать сложные комплексные проекты. В частности, разрабатывать инновационные сервисы кибербезопасности для клиентов, которые доступны в нашем мобильном приложении.

В любом случае мы отдаём себе отчёт в том, что хороший специалист в любой сфере — это штучный товар, за такими людьми идёт охота. Мы набираем экспертов разных уровней: junior, middle и senior.

JUNIOR, MIDDLE, SENIOR

Начинающих специалистов мы привлекаем в основном через программу стажировок студентов вузов. Ежегодно более 100 человек проходит стажировку или практику в Службе кибербезопасности Сбера. У нас работают выпускники почти 300 вузов страны: от Калининграда до Камчатки.

При найме новых сотрудников уровня middle мы обращаем внимание на образование и практический опыт, полученный в других компаниях. Для нас важно, чтобы кандидат стремился постоянно повышать компетенции, хорошо разбирался в современных технологиях. Не менее половины таких сотрудников мы готовим внутри Сбера. У многих этот путь занимает 3–4 года, поэтому кибербезопасность Сбера — отличная площадка для развития карьеры.

Крайне непросто найти на рынке специалиста senior, который бы удовлетворял требованиям, скажем, исполнительного директора или руководителя отдела. Таких людей мы нанимаем от 3 до 5 в год. Поиск специалиста с нужными компетенциями занимает до полугода, приходится проводить десятки собеседований. Время показало, наиболее эффективный способ — подготовка внутри самой Службы кибербезопасности. Для этого у нас есть все условия: в первую очередь это грамотные наставники, передающие свой опыт молодым сотрудникам, а также созданная внутри компании культура непрерывного обучения персонала — это и возможность как обучаться внутри Сбера, так и получать дополнительное образование на внешних площадках за счёт работодателя.

КНОПКА «ХОЧУ В КОМАНДУ»

Отдельно хочу отметить, что мы подготовили специальную карьерную страницу для со-

искателей, которая опубликована на портале Сбера по киберграмотности «Кибрарий» в разделе «Экспертам». Соискателю необходимо лишь нажать кнопку «Хочу в команду», оставить контактные данные и указать интересующее направление работы. Заявку оперативно рассмотрят и подберут подходящую под специалиста вакансию. После будут назначены собеседования с рекрутером и представителем команды экспертов по кибербезопасности. Уровень экспертного опыта будет проверяться на техническом интервью и в ходе выполнения тестового задания. Каждый третий сотрудник команды кибербезопасности начал свой путь с позиции стажёра, поэтому заявить о себе на нашей карьерной странице могут и начинающие специалисты. Команда кибербезопасности Сбера работает не только в Москве, но и в Санкт-Петербурге, Воронеже, Самаре, Нижнем Новгороде, Екатеринбурге, Новосибирске, Хабаровске, поэтому нам нужны профессионалы и в этих регионах.

КАРТА ЗНАНИЙ CISO

— Кстати, недавно на «Кибрарии» опубликована карта знаний CISO. Что это такое и с какой целью вы её сделали?

— Несмотря на бурный рост цифровизации общества и рост кибератак на организации с началом СВО, большая часть руководителей до сих пор не осознаёт всю важность построения качественной системы киберзащиты и не думает о последствиях её отсутствия. Главы компаний часто не имеют базовых знаний о рисках и угрозах в сфере кибербезопасности, не умеют им противостоять. И конечно же, вся нагрузка в парировании угроз кибербезопасности должна ложиться на плечи CISO.

При этом проблема для многих компаний — нанять хорошего CISO. Но вопрос в том, кто и по каким критериям оценит знания кандидатов, кто в конкретной структуре понимает, что должен знать и уметь CISO сегодняшнего дня, и, исходя из этого, собеседовать кандидатов.

Эти задачи и стали для нас импульсом к созданию карты знаний CISO. Карта, по нашему замыслу, позволяет руководителям кибербезопасности проводить самооценку и выявлять западающие компетенции, руководителям организаций, служб ИТ и HR — проводить собеседования, а молодым специалистам планировать треки профессионального развития. Мы систематизировали и структурировали различные области профессиональных знаний — учли требования российских регуляторов и весь опыт Группы Сбер, который дополнили лучшими мировыми практиками. При этом мы отдаём себе отчёт в том, что владеть полным спектром знаний из карты CISO — недостижимая мечта. Но она ориентир, к которому нужно стремиться, чтобы быть лучшим в сфере кибербезопасности.

УСТРАШАЮЩИЙ РАЗРЫВ

— Ни для кого не секрет, что существует большой разрыв между требованиями отрасли к специалистам по КБ и знаниями выпускников. Что делает Сбер, чтобы изменить ситуацию?

— На мой взгляд, интеграция академических знаний с отраслевой экспертизой поможет сократить разрыв между требованиями рынка и знаниями выпускников. Сбер вносит большой вклад в устранение этого разрыва. Мы, как и другие лидеры рынка, осознаём свою ответственность в этом вопросе.

Так, в 2022–2023 гг. порядка 1000 преподавателей из 160 вузов и 50 средних специальных учебных заведений страны повысили квалификацию на программе трека «Кибербезопасность» в рамках Летней цифровой школы. Наши эксперты делились опытом построения системы кибербезопасности современной цифровой организации, погружали в такие темы, как «Современный

SOC», «Практики безопасной разработки DevSecOps», «Управление угрозами и уязвимостями», «Технологии искусственного интеллекта в задачах кибербезопасности». Все полученные материалы и знания преподаватели могут использовать для обучения студентов. Кроме того, при поддержке экспертов Сбера в СПбГУ проводится магистерская программа «Информационное право и защита данных»: наши специалисты в области защиты персональных данных проводят лекции, семинары, мастер-классы и делятся со студентами своими знаниями и экспертным опытом.

АМБИЦИОЗНАЯ ЗАДАЧА

Мы поставили себе амбициозную задачу — создать эталонные учебно-методические материалы по предметным областям кибербезопасности на основе интеграции академических знаний с отраслевым экспертным опытом рынка и сделать их доступными для всего профессионального сообщества.

Для решения этой задачи в 2023 году Сбер совместно с одним из ведущих вузов страны открыл магистерскую программу «Кибербезопасность». Мы проработали содержание каждой дисциплины, в том числе и с учётом нашего практического опыта, создали карты знаний в виде иерархических структур и рассчитывали, что в итоге получим качественный методический материал, которым можно поделиться с другими вузами. Но столкнулись с противостоянием новой и старой школы. К сожалению, от развития совместного проекта, на которое мы рассчитывали, пришлось отказаться. Это крайне важный вопрос, поэтому мы его заостряем, публично акцентируем на нём внимание и продолжаем искать партнёров.

Мы видим, что в большинстве вузов сильные преподаватели приходят на кафедры с одной целью — готовить молодых специалистов для своих компаний или проектов. Проблема качества, мотивации преподавательского состава вузов, по крайней мере в сфере кибербезопасности, — одна из ключевых в задаче подготовки выпускников. Проблема подготовки кадров для кибербезопасности много лет остаётся сложной и, к сожалению, имеет тренд на обострение. Видимо, поэтому ряд экспертов полагают, что подготовка кибербезопасников — тупиковый путь, поэтому нужно готовить специалистов в ИТ после вуза и проводить дообучение в одном или нескольких направлениях кибербезопасности.

ВПЕРЁД В БУДУЩЕЕ

— Сегодня для обеспечения кибербезопасности клиентов Сбера и самого банка используются сотни моделей искусственного интеллекта (ИИ, AI), AI-помощники, которые могут выявлять угрозы и мошеннические звонки и вместо клиента отвечать на них, искать ошибке в коде, предоставлять экспертную поддержку специалистам. В планах до 2030 г., которыми вы поделились на конференции GigaConf 2024, — создание AI-аватаров, которые придут на помощь сотрудникам по ИБ или вовсе заменят их. Насколько реалистично такое развитие событий? В технологических процессах ИИ со временем останется только как вспомогательная функция, облегчающая работу человека?

— Это не фантазии, а реальная перспектива ближайших лет. Искусственный интеллект в кибербезопасности не заменит человека, а придаст импульс появлению новых профессий. В их числе оператор кибераватара, тренер моделей, конструктор агентов, специалист по знаниям. Я не вижу в этом ничего фантастического, более того, это жизненная необходимость в условиях увеличения технологической сложности работы Сбера и всей финансовой системы и на фоне роста AI-угроз. Ежедневно SOC Сбера обрабатывает около 500 млрд событий кибербезопасности — в 10 раз больше, чем четыре года назад. За это же время в 2,5 раза выросло ежемесячное количество транзакций, а число изменений в цифровых продуктах увеличилось более чем в 11 раз. Уследить за всем этим человеку просто невозможно.

Сейчас мне видится три варианта построения процессов кибербезопасности с использованием AI-технологий:

- традиционные процессы, сконструированные людьми, — AI-агенты будут исполнять их и сообщать об отклонениях в их выполнении;
- AI самостоятельно конструирует и выполняет новые процессы, а человек берёт на себя роль конструктора «мозга» искусственного интеллекта;
- наиболее футуристический вариант: человек декларативно ставит задачу и оценивает результативность, AI-система сама от и до определяет, как будет решена задача.

При этом ключевым умением AI должно быть самообучение и переход от процесса обработки данных к применению знаний. Это значит, что AI должен уметь познавать и получать опыт, обобщать его. То есть, по сути,

самостоятельно принимать верные решения и совершать верные действия в каждом конкретном случае.

О ПЕРСОНАЛЬНЫХ ДАННЫХ НА ГОСУДАРСТВЕННОМ УРОВНЕ

— Правительство завершило правовое оформление перевода государственных и окологосударственных информационных систем на единую облачную платформу, постановление об утверждении положения о «Гособлаке» было подписано главой правительства в июле этого года. С 1 января 2025 г. платформа вводится в постоянную эксплуатацию. Одновременно в ИБ-сообществе говорят о новой версии поправок в закон «О персональных данных», которые касаются оборота обезличенных данных и упростят работу с данными и получение доступа к информации. Новый подход отразится на безопасности и работоспособности Сбера?

— На безопасности и работоспособности Сбера принятые решения не отразятся. Ещё на этапе обсуждения мы провели экспертизу законопроекта и отметили возможные риски деобезличивания и утечки персональных данных. Чтобы минимизировать эти риски, мы предложили поправки в закон «О персональных данных» № 152-ФЗ, которые были приняты в августе этого года. Поправки установили ограничения на передачу в составе обезличенных данных информации, доступ к которой уже ограничен отраслевыми федеральными законами. Например, что касается именно финансовой сферы: в соответствии с Законом «О банковской тайне», передача обезличенных персональных данных клиентов банков в «Гособлако» будет являться нарушением. Аналогичные ограничения действуют в отношении тайны связи, сведений о состоянии здоровья и так далее.

О СЕТЕВЫХ ЭКРАНАХ

— Сейчас на рынке множество российских поставщиков межсетевых экранов. Если вы их уже смотрели, то насколько они отвечают потребностям банка? Если нет, то в чём причина сложившейся ситуации?

— Мы активно работаем со всеми разработчиками межсетевых экранов, большинство их продуктов мы тестировали. К сожалению, сейчас на российском рынке отсутствуют высокопроизводительные решения, способные в полной мере удовлетворить нашим требованиям как по производительности, так и по функциональным возможностям.

Такая ситуация сложилась потому, что отсутствует необходимая российская элементная база и специализированные операционные системы для сетевых средств защиты. Также не хватает компетенций и экспертного опыта у российских разработчиков, особенно это ощущается на фоне массового импортозамещения. Большинство решений использует компоненты с открытым исходным кодом, зачастую с минимальными изменениями, что не позволяет получить решения с требуемыми характеристиками как по производительности, так и по функционалу. При этом сравнительный анализ показал, что отечественные межсетевые экраны при худших функциональных возможностях в 5–7 раз дороже западных.

О ТЕЛЕФОННЫХ МОШЕННИКАХ

— Перейдём к более народной теме: как обстоят дела с мошенническими обзвонами? Их число росло год от года, изменилась ли как-то эта тенденция сейчас, в чём причины этого тренда? Какие меры принимает Сбер для противодействия мошенничеству?

— Число мошеннических обзвонов снизилось почти в 3 раза — с 20 млн в сутки в начале года до 6 млн сейчас. Увы, этот позитивный тренд не повлиял на общую сумму ущерба, она продолжает расти. Схемы становятся более изощрёнными, таргетированными и многоэтапными, сценарии общения с жертвами мошенничества — более эффективными.

Активность телефонных мошенников уменьшилась в связи с отменой отсрочки для сотрудников кол-центров и снижением числа самих кол-центров в несколько раз. Вывод из строя большой части энергетической инфраструктуры на Украине и противодействие использованию сим-боксов в России со стороны МВД также внесли свой вклад в процесс снижения мошеннической активности.

Большую роль играют меры на стороне операторов сотовой связи и банков.

Благодаря бесплатным сервисам кибербезопасности в мобильном приложении «Сбербанк Онлайн» наши клиенты, к примеру, могут включить проверку телефонных звонков, чтобы знать, когда звонит мошенник, — наш определитель уже активировали несколько миллионов человек. Реализована возможность включения блокировки мошеннических звонков, в том числе в мессенджерах. Можно подключить сервис «Совместные уведомления»,

который позволяет получать информацию об операциях по карте близкого человека, например, контролировать расходы ребёнка или родственника. Есть возможность сообщить о мошенническом сайте, номере телефона или банковской карте, активировать антивирус, моментально закрыть доступ к счёту и карте, если ваши данные попали к злоумышленникам. Всего более 20 различных сервисов, позволяющих клиенту гибко настроить необходимый ему уровень безопасности.

В Сбере работает система антифрода, которая автоматически выявляет и приостанавливает мошеннические операции, её эффективность в этом году достигла 99,8%.

Большую роль сыграло повышение уровня киберграмотности россиян. Эту работу ведут многие организации и ведомства. На портале Сбера «Кибрарий» собрана актуальная информация о киберугрозах, с которыми сталкиваются россияне, о методах противодействия этим угрозам. Также на нём много полезной информации для экспертов в сфере кибербезопасности.

Благодаря комплексному подходу к вопросу обеспечения кибербезопасности наших клиентов мы сохранили от мошенников более 200 млрд рублей с начала года.

ОБ УТЕЧКАХ

— Возможность совершать звонки у мошенников имеется благодаря доступу к персональным данным. Основываясь на криминальной хронике, обыватели делают выводы, что аферисты чаще звонят тем, у кого есть средства на счетах. Эти данные они получают непосредственно из банков. Так ли это? У Сбера есть экспертность в вопросе сохранности персданных, делитесь ли вы ей?

— Основные утечки идут не из банков. Сегодня российские банки — одни из самых защищённых в мире, так как они являются самыми атакуемыми целями в текущей геополитической обстановке. И конечно, персональные данные клиентов Сбера надёжно защищены. Однако надо понимать, что клиенты Сбера — это клиенты и других организаций. Лидер по утечкам за последние три года — ретейл: 42% персональных данных попадают в доступ из торговых сетей, 11% — из сферы услуг, 8% — из соцсетей. При этом мы понимаем, что в случае утечки атакованы будут в первую очередь финансовые сервисы, которыми пользуются люди. Поэтому и создаётся впечатление, что утечки идут якобы из банков.

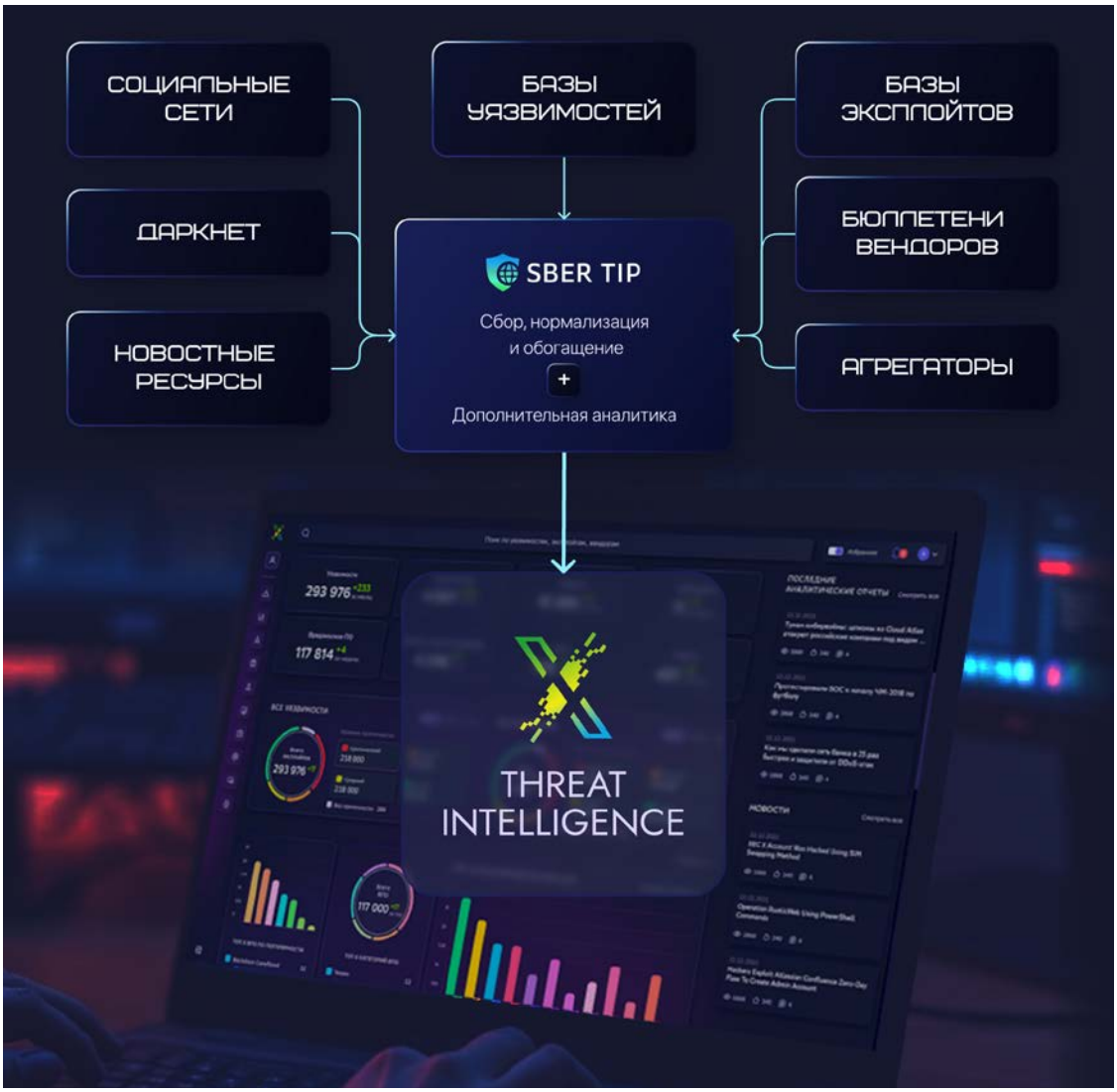
Сбер с 2020 года ведёт мониторинг утечек персональных данных, которые появляются в приватных каналах и публичном поле. Банку известно более 1000 источников информации, в которых хранятся свыше 3 млрд записей о гражданах России. Причём в 2020 году было порядка 500 млн таких записей, за 2022-й прирост более миллиарда записей, в 2023-м — 1,5 млрд. То есть за 4 года произошёл почти шестикратный рост объёмов утечек.

ТРЕТИЙ КАТАЛОГ, КУРС ЗАЩИТЫ ПД, SBER BANK PRIVACY

Украденные персональные данные — это фундамент, на котором строят свою преступную деятельность телефонные мошенники. В этом году Сбер выпустил третий каталог с 200 схемами мошенничества. Мы видим, что реализация каждой из этих схем становится возможной только благодаря доступу мошенников к персональным данным. Минимум, который нужен злоумышленникам для «работы», — имя и номер телефона жертвы. Вся остальная информация — это подспорье, которое увеличивает шансы мошенников на успех. Как правило, в мошеннических базах содержится следующая информация: Ф. И. О., день рождения, номер телефона, email, адрес проживания.

К сожалению, многие люди легкомысленно относятся к вопросу сохранности своих персональных данных и не знают, как их защищать. Недавно мы разработали общедоступный и бесплатный онлайн-курс по защите персональных данных «Вселенная персональных данных» и разместили его на платформе финансовой грамотности «Сбер Сова». В нём простым языком рассказываются правила защиты персональных данных в интернете и предлагаются интерактивные тесты для проверки знаний. Менее чем за час можно научиться определять, что относится к персональным данным, разобраться, как обрабатываются ваши данные и как они могут попасть в интернет, а также узнать, что делать, если нарушены ваши права. Рекомендую пройти его и посоветовать сделать это родственникам и друзьям.

Закон обязывает нас информировать клиентов о том, как обрабатываются их данные. Мы сделали больше: Сбер является одной из немногих компаний, на сайте которой для обеспечения прозрачности работы с персональными данными создан ресурс, посвящённый вопросам защиты персональных данных, — Sber Bank Privacy. Там можно найти всё — от правил работы с персональными данными и рекомендаций по защите личных данных до целого экспертного блока материалов, где мы делимся опытом построения



эффективной системы защиты персональных данных и ежеквартально публикуем профессиональный журнал по вопросам приватности и безопасности персональных данных Sber Privacy Journal.

X-THREAT INTELLIGENCE PLATFORM

— Наш номер выходит в преддверии осенних SOC-мероприятий: SOC Tech 2024 и SOC-Форума — время подведения итогов. Пару слов: с какой основной темой Сбер выступит в этом году?

— В этом году мы будем презентовать профильному сообществу возможности платформы управления киберугрозами, разработанной Центром киберзащиты Сбера, — X-Threat Intelligence Platform, или сокращённо Sber X-TI. По сути, это единая платформа для обмена данными о киберугрозах, доступная для всех компаний страны. Она позволяет использовать накопленный опыт Сбера по управлению уязвимостями и другими атрибутами кибератак для повышения уровня защищённости организаций.

Ценность платформы в том, что она даёт доступ к самой полной и быстро обновляемой базе данных обо всех актуальных уязвимостях, а также предоставляет возможности для устранения выявленных уязвимостей.

Sber X-TI состоит из шести модулей: уязвимости, вредоносное ПО, группировки, тактики и техники, аналитические отчёты, новости. Каждый из этих модулей глубоко проработан и даёт широкий набор возможностей для решения задач по обеспечению кибербезопасности организации.

Что важно, доступ к этой платформе бесплатный, ей уже активно пользуются компании — партнёры Сбера и дают высокую оценку этому продукту. Таким образом, Сбер вносит вклад в создание национальной системы кибербезопасности в стране и объединение усилий в этой области с целью повышения уровня защищённости российских компаний.

Вопросы задавала Марина Бродская

ЦИФРОВОЙ СЛЕД ОРГАНИЗАЦИИ

И АТАКИ ЗА ПРЕДЕЛАМИ ИНФРАСТРУКТУРЫ

Артём ГРИБКОВ
заместитель директора Angara SOC по развитию бизнеса

Как правило, когда мы говорим об управлении киберрисками, мы затрагиваем в первую очередь вопросы обеспечения безопасности инфраструктуры, будь то инвентаризация активов и харденинг, управление уязвимостями, использование средств защиты информации, выстраивание процессов security operations или внедрение регламентов ИБ.

И на то есть причины. Ведь большинство тактик, техник и процедур злоумышленников эффективно детектируются и митигируются при их взаимодействии с атакуемой инфраструктурой. Несмотря на то что ни одно СЗИ и ни один подход к обеспечению ИБ не дают стопроцентной гарантии безопасности, их использование позволяет повысить шансы своевременного обнаружения действий злоумышленников до нанесения ущерба и снизить соответствующие киберриски: антивирусные средства и EDR обеспечивают обнаружение вредоносной активности на конечных хостах, «песочницы» анализируют вредоносную нагрузку, сетевое оборудование анализирует трафик, харденинг и сегментация ограничивают возможности горизонтального перемещения и эскалации привилегий, управление активами снижает риск эксплуатации уязвимостей и вероятность «забыть» о существовании этих активов, регулярное повышение осведомлённости пользователей снижает риск человеческого фактора (особенно при открытии фишинговых писем), а процессы security operations объединяют все эшелоны обороны воедино.

Если описывать действия злоумышленника через killchain, когда для проведения атаки он проходит несколько этапов, то все упомянутые меры нацелены на этапы от «Доставки» до «Нанесения ущерба» (рис. 1).

При этом за рамками контроля остаются как подготовительные этапы проведения атаки, так и угрозы, которые наносят ущерб вообще за пределами инфраструктуры организации. Поговорим про каждый из аспектов подробнее.

РАЗВЕДКА И АНАЛИЗ ЦИФРОВОГО СЛЕДА

На подготовительных этапах атаки задача злоумышленника — собрать как можно больше информации об инфраструктуре жертвы. При этом, исходя из тенденций как российского региона, так и мировой практики, основной упор делается на поиск утёкших секретов жертвы (логин/пароль пользователей системы, ключи, токены, фрагменты кода и т.д.). По некоторым оценкам, легитимные учётные данные использовались для первичного проникновения в инфраструктуру (T. 1078 MITRE ATT&CK®)

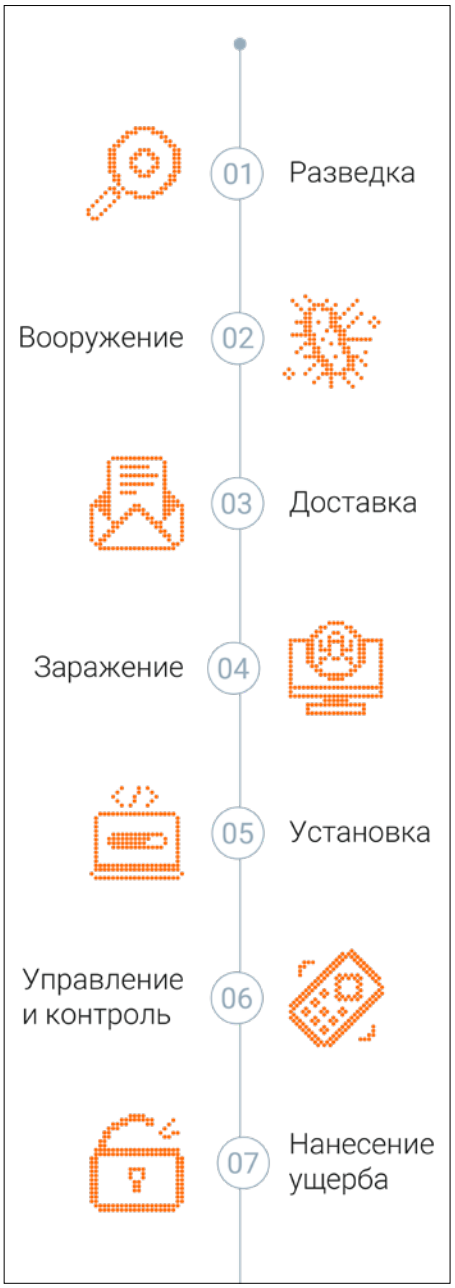


Рисунок 1. Действия злоумышленника через Kill Chain проходят несколько этапов

в 30% случаев от общего числа атак в 2024 году, а по сравнению с предыдущим годом их количество увеличилось на 70%.

Рост популярности подхода понятен: log in дешевле, чем hack in. Кроме того, обнаружить активность злоумышленника под легитимной учётной записью значительно сложнее. Ситуация усугубляется, если украденная УЗ обладает повышенными привилегиями. В этом случае значительно сокращается время от момента проникновения в инфраструктуру до нанесения ущерба, а некоторые этапы killchain могут и вовсе быть пропущены.

Источников утечек секретов множество. Их можно найти в репозиториях ИТ-подрядчиков (например, git), которые по каким-то причинам оказались публично доступны, или при передаче секретов через различные сервисы (например, Pastebin и Telegram). На теневых форумах и в telegram-каналах распространяются «слитые» базы интернет-ресурсов, в которых регулярно попадаются данные пользователей, использовавших для регистрации корпоративную почту и пароль. При этом пароли нередко хранятся в открытом виде.

Утечки информации через Telegram стоит отметить отдельно. Мессенджер популярен в России и часто используется для обсуждения в чатах рабочих вопросов, а иногда и передачи конфиденциальной информации. При некорректных настройках приватности такие чаты легко обнаружить по ключевым словам (названию организации или подрядной компании), и они доступны для просмотра третьим лицам.

Говоря про атаки через подрядные организации, необходимо упомянуть и набирающую популярность технику «Использование доверенных отношений» (T. 1199 MITRE ATT&CK®). На практике регулярно оказывается, что предоставляемые для подрядчика привилегии в инфраструктуре избыточны, его действия не контролируется, а при аутентификации не используется второй фактор. Всё это делает подрядные организации привлекательной целью для злоумышленников, так как компрометация одной организации ведёт к получению доступа сразу в несколько инфраструктур разных клиентов. Полученный доступ может быть передан другим заинтересованным лицам, и объявления о продаже можно обнаружить как в индексируемых, так и неиндексируемых сегментах сети Интернет.

Помимо упомянутых подходов к снижению рисков от T. 1199, возможно проведение у подрядчика комплексного анализа инфраструктуры для выявления следов её компрометации (Compromise Assessment).

С ростом популярности хактивизма чаще стали публиковаться массовые призывы к проведению атак против конкретных организаций. Сведения о планируемых кампаниях позволяют быстрее принять контрмеры и снизить риск ущерба.

На подготовительных этапах полезной для злоумышленника может быть совершенно разная информация. Например, если в утечках не обнаружено секретов для доступа к инфраструктуре, при проведении целевой атаки может быть использован фишинг (T. 1566 MITRE ATT&CK® по-прежнему входит в топ техник первичного проникновения в инфраструктуру). Для более качественного профилирования активности используется любая чувствительная информация об организации: данные о сотрудниках, должностных регламентах и зонах ответственности, внутренних процессах и многое другое. Чем больше информации, тем больше вероятность успеха атаки.

Пресс-релизы об «историях успеха» внедрения каких-либо решений, опубликованные внутренние документы могут быть использованы для планирования вектора атаки. Не пренебрегают такими данными и для проведения конкурентной разведки.

АТАКИ ЗА ПРЕДЕЛАМИ ИНФРАСТРУКТУРЫ

Для нанесения финансового или репутационного ущерба злоумышленнику далеко не всегда необходимо взаимодействовать с инфраструктурой жертвы. В первую очередь сюда относятся угрозы, связанные с защитой бренда.

Мошенники создают фишинговые ресурсы с использованием брендбука и атрибутов организации, которые могут использоваться для кражи конфиденциальных данных пользователя: логинов, паролей, данные банковских карт, персональных данных. На подложных ресурсах распространяется контрафакт и фиктивные услуги от лица легитимных компаний. Зачастую обманутые клиенты требуют компенсации собственных потерь у официальной компании.

Также важно помнить и про медиаатаки, связанные с распространением ложной информации об организации или её сотрудниках. Учитывая скорость и масштабы распространения информации в социальных сетях, мессенджерах и на новостных сайтах, такие действия злоумышленников могут нанести серьёзный ущерб репутации, который может быть довольно трудно восстановить.

В КАЧЕСТВЕ РЕЗЮМЕ

Обеспечение безопасности — непрерывный и повторяющийся процесс (PDCA/PDAR). Регулярный анализ и актуализация модели угроз, используемых средств, процессов и подходов позволяют снижать вероятность реализации киберрисков. Учитывая тенденции, характерные как для России, так и для мира в целом, сегодня необходимо уделять должное внимание контролю цифрового следа. Стоимость превентивных мер практически всегда в разы меньше стоимости реагирования на инциденты и устранение их последствий, особенно если в результате атаки были остановлены бизнес-процессы.

Сегодня на рынке представлены различные продукты и услуги, направленные на решение этой задачи. Одним из них является платформа Angara ECHO, с помощью которой можно автоматизировать процессы регулярного мониторинга цифрового следа и оперативно получать информацию о возникающих угрозах для оперативного принятия превентивных мер.

ПРОВЕРКА DOCKER-КОНТЕЙНЕРОВ С ПОМОЩЬЮ DR.WEB VXCUBE

СНИЖАЕТ РИСК ЦЕЛЕВЫХ АТАК НА ПРЕДПРИЯТИЯ

Василий СЕВОСТЬЯНОВ
начальник отдела технического сопровождения продаж компании «Доктор Веб»

Современные киберугрозы становятся всё более сложными и опасными, особенно с ростом числа целевых атак (APT — Advanced Persistent Threats[1]), которые направлены на конкретные организации. Эти атаки идут с применением продвинутых методов проникновения, могут оставаться незамеченными длительное время, и с помощью традиционных средств защиты выявить их крайне трудно. В таких условиях компании нуждаются в эффективных инструментах для глубокого анализа подозрительных объектов, которые могут быть частью сложных многоуровневых атак.

Песочница Dr.Web vxCube[2] — это передовое решение для интеллектуального анализа, позволяющее исследовать поведение подозрительных объектов и обнаруживать угрозы, которые обычные средства защиты могут распознать не всегда. Dr.Web vxCube играет ключевую роль в противодействии современным киберугрозам, включая APT.

Центры мониторинга и предотвращения атак (SOC) — основа защиты организаций от кибератак. Основная задача SOC заключается в выявлении и нейтрализации угроз на ранних этапах. Для таких центров крайне важно иметь инструменты, позволяющие оперативно анализировать подозрительные объекты и реагировать на инциденты в кратчайшие сроки.

Песочница Dr.Web vxCube идеально подходит для SOC, поскольку она обеспечивает как ручной, так и автоматизированный исчерпывающий анализ подозрительных файлов в изолированной среде. Это помогает выявлять скрытые угрозы и детализировать поведение вредоносного ПО, повышая эффективность противодействия ему. Применение песочницы не только сокращает время на принятие решений, но и снижает нагрузку на специалистов по безопасности. Благодаря поддержке различных операционных систем и приложений Dr.Web vxCube позволяет анализировать широкий спектр угроз, что делает его незаменимым инструментом для SOC.

Современные ИТ-инфраструктуры всё чаще полагаются на контейнерные технологии, в частности Docker. Такие контейнеры упрощают разработку, тестирование и развёртывание приложений, позволяя компаниям гибко масштабировать свои решения и ускорять цикл выпуска обновлений.

Docker-контейнеры представляют собой легковесные, изолированные среды для запуска приложений, и их использование быстро набирает популярность благодаря эффективности и удобству интеграции в инфраструктуру. Однако контейнеры, как и любая другая технология, имеют свои риски безопасности. Именно поэтому их анализ становится приоритетной задачей.

Одной из проблем использования контейнеров является распространённая практика применения при их сборке сторонних образов в качестве основы. Для ускорения разработки и развёртывания приложений многие компании используют готовые образы, предоставленные третьими лицами. Однако такие образы могут содержать уязвимости или вредоносные элементы, представляющие серьёзную угрозу для ИТ-инфраструктуры.

Использование непроверенных контейнеров увеличивает вероятность внедрения вредоносного ПО или недокументированных функций в корпоративные системы. По сути, это открывает возможность для реализации атаки на цепочку поставок (Supply Chain Compromise по классификации MITRE). Эти риски требу-

[1] Расширенные постоянные угрозы

[2] https://www.drweb.ru/vxcube/

ют тщательной проверки и анализа контейнеров перед их применением, что может стать серьёзным вызовом для специалистов по информационной безопасности.

В ответ на растущее число угроз, связанных с контейнерными технологиями, в песочницу Dr.Web vxCube была добавлена новая функциональность — анализ Docker-контейнеров. Теперь пользователи могут проводить детальный анализ контейнерных образов, выявляя возможные скрытые угрозы, недокументированные функции или вредоносные элементы.

Основные возможности анализа Docker-контейнеров в Dr.Web vxCube:

- проверка контейнерных образов в изолированной среде на наличие скрытых или вредоносных компонентов;
- анализ поведения контейнеров, включая сетевую активность и взаимодействие с системой;
- возможность выявления недокументированных функций, которые могут представлять угрозу безопасности;
- подробный отчёт о результатах анализа, включая информацию о подозрительных действиях контейнера.
- Использование Dr.Web vxCube для анализа Docker-контейнеров предоставляет ряд существенных преимуществ:
- повышение уровня безопасности контейнерных приложений за счёт тщательной проверки образов;
- снижение рисков для всей ИТ-инфраструктуры путём предотвращения внедрения вредоносного кода через непроверенные контейнеры;
- оптимизация процессов проверки и внедрения контейнеров, что ускоряет разработку и развёртывание приложений без компромиссов в области безопасности.

Эта функциональность позволяет снизить риски использования сторонних контейнерных образов за счёт проверки внедряемых в ИТ-инфраструктуру контейнеров на наличие опасных элементов.

Песочницы играют ключевую роль в защите ИТ-инфраструктур от современных сложных угроз, а Dr.Web vxCube — это передовое решение, которое позволяет эффективно анализировать не только файлы и программы, но и контейнерные образы. Благодаря новой возможности анализа Docker-контейнеров Dr.Web vxCube помогает снизить риски компрометации для компаний, использующих технологии контейнеризации.

Использование песочницы Dr.Web vxCube является важным элементом для построения надёжной системы информационной безопасности, особенно в условиях растущей сложности киберугроз и широкого распространения контейнерных технологий.

КАК НАСТРОИТЬ SIEM «ПОД СЕБЯ»

ПРОСТАЯ КАСТОМИЗАЦИЯ ПО ШАГАМ

Павел ПУГАЧ
системный аналитик «СёрчИнформ»

Любой проект внедрения SIEM индивидуальный, даже у компании с типовой инфраструктурой найдутся свои особенности, которые нужно учесть. Часто для кастомизации требуется помощь вендора или интегратора, потому что системы приходится буквально «писать под заказчика». Это удорожает и удлиняет проект. Как этого избежать? Выбрать систему, в которой есть удобные инструменты для кастомизации, не требующие специальных знаний, вмешательства вендора и труда программистов.

На примере «СёрчИнформ SIEM» расскажу, как ИБ-специалист может адаптировать систему самостоятельно.

КАК ПОДКЛЮЧИТЬ НЕТИПОВЫЕ ИСТОЧНИКИ

В SIEM сбором данных от источников в инфраструктуре занимаются коннекторы. Они вычитывают логи от средств ИБ, а также прикладного софта и оборудования.

К типовому «железу» и ПО в SIEM обычно есть готовые коннекторы. В «СёрчИнформ SIEM» их больше 40. Если их не хватает, на помощь приходят универсальные коннекторы на основе event log, syslog, NetFlow, SSH, SNMP. Эти протоколы подходят для большинства источников, но не всегда дают достаточно детализации: не передают всех нужных данных или, наоборот, «заваливают» SIEM лишней информацией. Наконец, есть самописные источники, которые не поддерживают перечисленные стандарты.

Для таких случаев в «СёрчИнформ SIEM» есть два инструмента.

CustomConnector позволяет подсоединить к SIEM любой источник с помощью скриптов на Windows PowerShell. Написать команду на PowerShell без усилий сможет рядовой системный администратор, то есть не понадобится помощь программистов. Вся работа со скриптом ведётся в интерфейсе SIEM, другие инструменты не нужны.

«СёрчИнформ SIEM» поставляется уже с готовыми образцами скриптов. Например, в комплекте есть шаблоны для работы с Kerio: выгрузка отчётов о входах, ошибках аутентификации, вторжениях в систему и т.п. Их можно персонализировать под свои задачи или адаптировать для другого оборудования и ПО.

DatabaseConnector подключается напрямую к произвольным базам данных, куда некоторые источники могут записывать логи вместо классических журналов. Но БД не обязательно должна быть с логами, подсоединить к SIEM можно любую. Также DatabaseConnector позволяет импортировать данные из БД выборочно. Например, когда нужно вычитать из баз антивируса только индикаторы компрометации или другую специфическую информацию.

Коннектор не требует написания скриптов: все настройки можно «накликать» в консоли SIEM. Достаточно задать тип СУБД и сервер, где она расположена, выбрать БД и что из неё нужно импортировать: вплоть до конкретных таблиц, столбцов в них или данных в ячейках.

КАК СКОРРЕЛИРОВАТЬ ПРОИЗВОЛЬНЫЕ СОБЫТИЯ

Чтобы выявить инциденты в потоке событий, SIEM опираются на правила корреляции — алгоритмы, которые обнаруживают угрозу по совокупности внешне рядовых признаков. В нашей системе предустановлены десятки правил для каждого источника, всего больше 400. Следующий уровень — сопоставлять события из нескольких разных источников. Это механизм кросс-корреляции.

Каждый источник передаёт события по-своему. Поэтому обычно написание правил корреляции и кросс-корреляции требует знания одного или нескольких языков программирования. К тому же понадобится доступ к коду SIEM. В «СёрчИнформ SIEM» этого не нужно: всё настраивается в интерактивном конструкторе через основную рабочую консоль.

Правило задаётся в три действия:

1. Выбираем нужные источники и события из них. Комбинировать можно любые события из любых источников, также доступна фильтрация:
   - по пользователю и его роли,
   - по устройству,
   - по IP-адресу и т.д.
2. Указываем объединяющие условия. Например, чтобы сообщения о событиях поступали с одного ПК или от одной учётной записи. Работают логические операторы:
   - «И», когда инцидентом считается обязательное совпадение событий;
   - «НЕ», то есть инцидентом будет случай, когда после определённого события не происходит другое (которое в нормальной ситуации должно произойти).
3. Задаём временные рамки: события будут считаться взаимосвязанными, если произойдут одно за другим в течение определённого периода.

Сервис работает по принципу «A + B = alert» (или «A — B = alert»). Правила можно комбинировать между собой. Таким образом, ИБ-специалист может прописать почти любой сценарий предполагаемого инцидента и настроить автоматическое обнаружение сложных атак.

КАК НАРАСТИТЬ НЕСТАНДАРТНЫЙ ФУНКЦИОНАЛ

Основная задача SIEM — мониторить инфраструктуру и находить инциденты. Но часто заказчику требуется пойти дальше: реагировать на угрозы, расследовать и прогнозировать их, и желательно в одном окне.

Вендоры отвечают на этот запрос по-разному, многие пытаются реализовать в SIEM максимум функционала смежных систем ИБ. Но потребности компаний неодинаковы. Поэтому мы оставляем «СёрчИнформ SIEM» в классической комплектации, а дополнительные возможности заказчики могут включить опционально.

Например, функционал реагирования у нас реализован через внешние приложения. SIEM их запускает и инструктирует, как поступить с угрозой. Автоматическая реакция включается при настройке правила корреляции, достаточно указать, какие данные об инциденте передавать в стороннее ПО. Например, антивирусу вместе с параметрами проверки нужно отдать список IP-адресов и имена ПК из поражённого сегмента сети. Тогда если SIEM зафиксирует заражение, то сможет запустить в антивирусе любое из возможных действий: удаление, сканирование или помещение зловреда в песочницу.

Для прогнозирования инцидентов у нас есть встроенный сканер уязвимостей. Но в работе он использует данные из внешних БДУ — сразу из девяти, включая базу ФСТЭК. Дополнительно можно подключить системы класса Vulnerability Management в качестве внешнего источника.

Расследования реализованы при помощи инструмента Task Management. Он создан для командной работы над инцидентами, ИБ-отдел может фиксировать ход дела самостоятельно или включить интеграцию с ГосСОПКА и IRP. Тогда SIEM поможет классифицировать инциденты по стандартам регулятора, «упакует» результаты в отчёт установленной формы и сразу направит его по адресу.

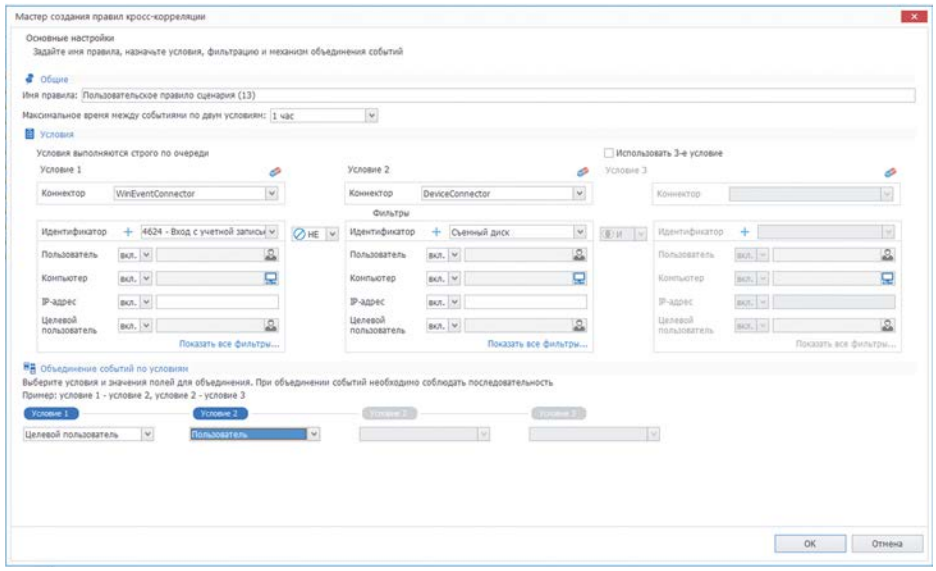


Рисунок. Мастер создания правил кросс-корреляции в «СёрчИнформ SIEM»

Кроме того, «СёрчИнформ SIEM» получает данные от всех ключевых ИБ-систем, от антивирусов до XDR, IDS, NGFW, различных TI-инструментов и т.д. В итоге любую нужную функцию можно подключить как коннектор, и не доплачивать за невостребованные «фичи».

ВЫВОД

Невозможно найти SIEM, которая бы идеально подошла всем сразу «из коробки». Поэтому надо быть готовым к кастомизации и выбирать для внедрения максимально гибкую систему. Такая SIEM должна:

- поддерживать источники, которые не передают данные стандартным способом;
- качественно фильтровать информацию от источников, чтобы обнаруживать нетиповые события ИБ;
- предоставлять удобные инструменты создания правил корреляции и кросс-корреляции событий;
- легко интегрироваться со сторонними ИБ-системами, способными расширить её возможности.

Тогда система удачно встроится в любую инфраструктуру и не потребует дополнительных вложений ни на старте, ни в процессе эксплуатации, когда у заказчика изменятся инфраструктура или задачи.

* * *

«СёрчИнформ SIEM» легко адаптируется под индивидуальные потребности компаний, при этом готова к работе с первого запуска и не перегружена функционалом под нехарактерные задачи. Эти возможности заказчик может нарастить в ней сам с помощью удобных инструментов кастомизации — без сторонней помощи и доплат. Попробовать, как это работает, можно бесплатно в течение 30 дней:

«КОЛИЧЕСТВО ЗАКАЗЧИКОВ MTC RED SOC ЗА ПОСЛЕДНИЙ ГОД ВЫРОСЛО В ДВА РАЗА»

Ильназ ГАТАУЛЛИН
технический руководитель центра мониторинга и реагирования на кибератаки MTC RED SOC

Компания MTC RED (ООО «Серенити Сайбер Секьюрити») появилась в августе 2022 г. Сегодня её SOC вышел на внешний рынок. На вопросы BIS Journal отвечает Ильназ Гатауллин.

— С начала года MTC RED SOC отразил более 70 тыс. хакерских атак — в полтора раза больше, чем за аналогичный период в прошлом году, говорят ваши отчёты. Повышенное внимание хакеры уделяют объектам КИИ, СМИ и ИТ-компаниям. Изменился ли характер атак или в них, как и в 2022 г., участвуют хактивисты, преследующие скорее медийные и политические цели, чем финансовую выгоду?

— Мы видим, что в целом растёт интенсивность атак практически на все отрасли, однако наиболее квалифицированные хакеры фокусируются на двух ключевых векторах: нанесение ущерба субъектам критической информационной инфраструктуры и максимальная заметность, «медийность» атак. В этом плане мало что изменилось: 65% высококритичных атак приходится на КИИ. Недавно мы зафиксировали очередной рост атак на СМИ, причём большая часть высококритичных инцидентов была зафиксирована в феврале, а пик пришёлся на 22 число. Всё это говорит о политизированности кибервоздействий на российские компании.

— В первом полугодии 2024 г. MTC RED SOC отразил на треть больше критичных атак на здравоохранение, чем за аналогичный период прошлого года. О росте атак на здравоохранение говорит и международный опыт. Означают ли эти показатели, что у MTC RED SOC увеличилось количество клиентов — медицинских организаций? Что должно произойти, чтобы социально значимые компании усилили меры безопасности?

— Дело в том, что злоумышленники прицельно охотятся за большими массивами персональных данных, которые обрабатываются в российских компаниях. Сектор здравоохранения в этом отношении — золотое дно. Он оперирует большими объёмами ПДн и при этом в целом относительно слабо защищён. После вала кибератак в 2022 г. большинство крупных операторов ПДн приняли серьёзные меры по повышению защищённости, но не все. Хакеры же направляют свои усилия на более уязвимые организации. Поэтому медицина — одна из максимально интересных мишеней.

Организации здравоохранения тоже усиливают меры защиты, внедряют процессы мониторинга и реагирования на кибератаки, в том числе на базе сервисов MTC RED SOC. Но повышение защищённости отрасли в целом — это длинный путь, и он пока не пройден в той мере, в которой его прошли, например, банки.

— Атаки через подрядчика стали чуть ли не главной проблемой этого года. Как часто MTC RED SOC сталкивается с такими инцидентами?

— Достаточно часто. Чтобы не быть обнаруженными, атакующие действуют очень изобретательно. Например, в ходе одной из атак на нашего заказчика через его подрядчика хакеры проявляли активность только в «технологические окна» — в те же временные промежутки, когда подрядчик обычно и производил работы по обновлению программного обеспечения у заказчика. Злоумышленники даже перемещались по тем же самым хостам, что и подрядчик. Обнаружить их удалось благодаря небольшим нестыковкам между временем записей в журналах работ подрядчика и временем аутентификации его учётной записи в системе.

Мы также видим, что ИТ-компании неизменно в топе самых атакуемых, и такие атаки тоже могут быть первым этапом атаки через подрядчика. Это узкое место, потому что даже очень зрелые в части информационной безопасности организации редко регламентируют и как-либо проверяют уровень защищённости подрядчиков. Это оставляет для хакеров возможность пройти «ниже радаров» стандартных средств защиты, маскируя вредоносные действия под легитимную активность ИТ-подрядчика. Поэтому мы рекомендуем всем заказчикам использовать решения, которые обеспечивают проведение аутсорсинговых работ в ИТ-инфраструктуре через промежуточный сервер, который фиксирует все действия подрядчиков. Так можно настроить мониторинг вплоть до

фиксации видеозаписи действия подрядчика и журналирования вводимых команд. Это существенно облегчает выявление и анализ кибератаки.

— Компания MTC RED (ООО «Серенити Сайбер Секьюрити») появилась в августе 2022 г., и её SOC вышел на внешний рынок. Какие изменения произошли за прошедшие два года с момента появления MTC RED SOC? Повлияли ли изменения в ландшафте киберугроз на рынок SOC и на работу MTC RED SOC?

— За это время мы серьёзно нарастили стек технологических партнёрств. Сегодня мы работаем со всеми ключевыми отечественными SIEM-системами, собираем события с любых классов решений от разных вендоров.

Недавно мы заключили партнёрское соглашение с компанией Xello. В инфраструктуре заказчика размещаются так называемые ловушки и приманки, которые с большой вероятностью будут задействованы в ходе кибератак. Это помогает нам ещё быстрее выявлять действия злоумышленников, которые уже обошли другие средства защиты и проникли в инфраструктуру заказчика.

И этот технологический рост, и непосредственно рост числа кибератак, о котором я говорил выше, способствовали тому, что количество заказчиков MTC RED SOC за последний год выросло в два раза. Мы усилили присутствие в ряде отраслей, появились и заказчики из новых сфер — госсектора, образовательных организаций, транспортных и девелоперских компаний, организации сферы туризма и других. Можно отметить, что, помимо крупных игроков, стало гораздо больше компаний из сегмента среднего бизнеса.

— Вы предлагаете своим клиентам различные форматы работы, в том числе гибридный SOC. Насколько популярна эта модель?

— Гибридная модель SOC очень востребована. Одно из преимуществ гибридной модели — огромный опыт взаимодействия MTC RED SOC с заказчиками из разных отраслей, компетенции в разработке корреляционных правил, широкий спектр детектирующей логики и практика реагирования.

Одно из преимуществ гибридной модели — огромный опыт взаимодействия MTC RED SOC с заказчиками из разных отраслей, компетенции в разработке корреляционных правил, широкий спектр детектирующей логики и практика реагирования

Например, если у заказчика уже есть SIEM-система и он нуждается в её поддержке и развитии, мы берём SIEM на сопровождение: подключаем источники событий, пишем и профилируем корреляционные правила, помогаем уменьшить число ложноположительных срабатываний, осуществляем мониторинг событий ИБ. Заказчик, имея собственную SIEM-систему в периметре, может быть уверен, что информация о событиях ИБ не покидает периметра организации, а также избавляется от сложностей, связанных с дефицитом квалифицированных кадров в отрасли.

Если же заказчик планирует строить собственный SOC, на то время, пока проект ещё не реализован, заказчик часто подключается к облачному SOC и таким образом сразу получает ядро SIEM в нашем облаке. На своей стороне ему останется только развернуть коллектор и брокера, которые собирают, агрегируют и нормализуют события.

— Расскажите о планах MTC RED SOC. Какие услуги и решения вы хотите предложить клиентам в ближайшей перспективе?

— Мы видим, что в части миграции в облака российский рынок повторяет международный опыт. Поэтому сейчас мы стремимся к тому, чтобы обеспечивать высочайший уровень защищённости для клиентов с гибридными инфраструктурами.

Кроме того, мы тестируем возможности искусственного интеллекта для автоматизации ряда процессов в нашем SOC, чтобы развивать его не только за счёт количества оказываемых сервисов, но и за счёт их качества.

В частности, с помощью ИИ мы можем автоматизировать рутинные задачи аналитиков, связанные с формированием карточки инцидента. Добившись снижения трудозатрат на эту процедуру, специалисты будут тратить больше времени на проведение валидации. Мы также тестируем гипотезы о применении ИИ при «тюнинге» правил корреляции под конкретного заказчика и формирования правил для снижения ложноположительных срабатываний.

ИИ может быть полезен и как инструмент автоматизированного сбора и систематизации дополнительной информации об инструментарии злоумышленника. Такая автоматизация позволяет аналитику сосредоточиться на наиболее интеллектуально трудоёмкой работе, а заказчик в результате получает более полный и детализированный отчёт об атаке в максимально короткие сроки. И наконец, мы исследуем возможности ИИ для автоматизации и повышения точности проактивного поиска киберугроз. Всё это может позволить нам быстрее подключать сервисы SOC, точнее и быстрее выявлять кибератаки на наших заказчиков.

Вопросы задавала
Марина Бродская

RUSIEM В SOC

Что делать, если в компании назрела необходимость в использовании SIEM-системы, а экспертизы нет, и какие требования предъявляют вендоры к MSSP-партнёрам, оказывающим услуги SOC, рассказывают специалисты RuSIEM, руководитель отдела предпродажной подготовки Даниил Вылегжанин и руководитель отдела по работе с партнёрами Любовь Евтифеева.

ЧТО НУЖНО ЗНАТЬ ЗАКАЗЧИКАМ...

Даниил ВЫЛЕГЖАНИН
руководитель отдела предпродажной подготовки RuSIEM

— Даниил, кому из заказчиков вы рекомендуете обращаться в коммерческий SOC?

— Любому заказчику, который понимает необходимость анализа событий безопасности или попадает под требования регуляторов, но ещё не созрел для полноценного внедрения SIEM в своей инфраструктуре.

Например, для финансового сектора действует ГОСТ Р 57580.1–2017, который говорит о необходимости организации мер по регистрации и управлению событиями безопасности. Практически всегда для обеспечения соответствия этим требованиям используется SIEM-система, как единая платформа для сбора, хранения и анализа событий с целью оперативного выявления инцидентов информационной безопасности. Однако не во всех финансовых организациях есть достаточное количество ресурсов для внедрения SIEM-системы, поэтому для них услуги SOC будут очень кстати. Такие заказчики смогут одним выстрелом убить двух зайцев: и обеспечить соответствие требованиям регуляторов, и повысить уровень информационной безопасности компании.

— Какие существуют варианты подключения к коммерческим SOC?

— Здесь всё зависит от исходных данных. Если у заказчика нет мощностей для развёртывания SIEM в своей инфраструктуре, но при этом есть необходимость использования системы мониторинга событий ИБ, то для таких организаций подойдёт вариант отправки своих событий в коммерческий SOC для анализа и выявления инцидентов.

Для предприятий, у которых достаточно ресурсов, но не хватает экспертности, рекомендуется гибридный вариант: когда SIEM разворачивается внутри инфраструктуры заказчика, а операции по расследованию и реагированию на инциденты осуществляют специалисты коммерческого SOC со строгим соблюдением SLA и полной отчётностью. Таким образом, все события не выходят за пределы организации и в случаях, когда заказчик понимает, что уже сам готов заниматься расследованием и реагированием на инциденты, он может отказаться от экспертизы SOC в пользу собственной без дополнительных затрат.

Также немаловажную роль при выборе модели подключения играет стоимость оказываемых услуг. Иногда, даже при наличии ресурсов для развёртывания SIEM локально, более интересным вариантом для компании является использование вычислительных мощностей и экспертизы стороннего SOC, так как это позволяет сберечь драгоценные ресурсы для других задач.

...И ПАРТНЁРАМ

Любовь ЕВТИФЕЕВА
руководитель отдела по работе с партнёрами RuSIEM

— Любовь, каковы основные преимущества RuSIEM для SOC-центров?

— RuSIEM — нишевой вендор, инвестирующий все ресурсы в развитие своего основного продукта, SIEM-системы RuSIEM, и дополнительных модулей, расширяющих его функционал. Помимо оперативной технической поддержки, у нас есть постоянно растущая база знаний RuSIEM, портал документации по решению, а также канал RuSIEM community в TG, позволяющие оперативно получать поддержку и помощь как от команды разработчика, так и от сообщества пользователей RuSIEM.

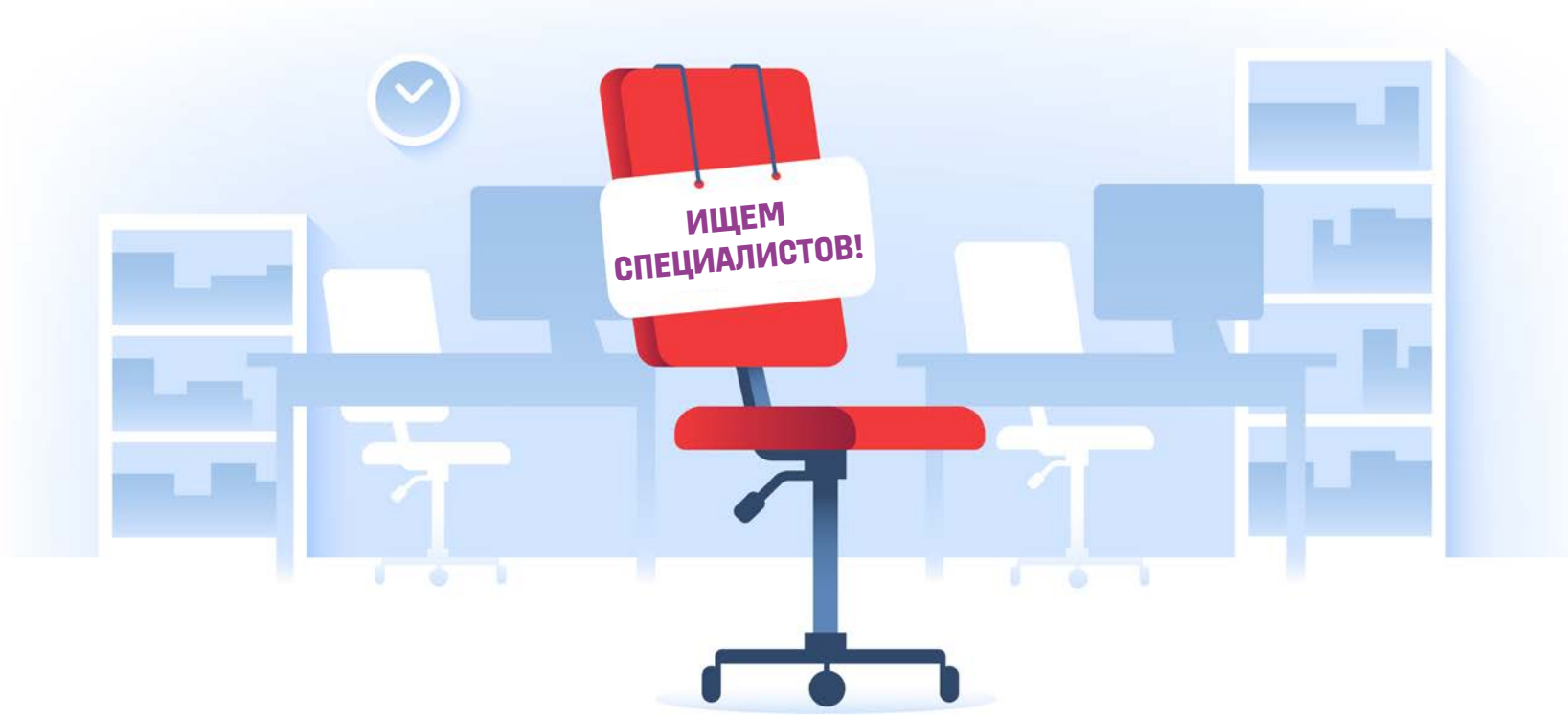
Кроме этого, мы предлагаем партнёрам гибкую систему лицензирования, оптимальное соотношение «цена — качество», возможность горячего расширения лицензии без необходимости отключения системы и приобретения дополнительных модулей.

— Есть ли требования к MSSP-партнёрам?

— Помимо наличия первой и второй линий технической поддержки клиентов, мы хотели бы, чтобы у партнёров были компетенции по нашему продукту, в том числе демостенд RuSIEM, а также обученные технические специалисты и sales-менеджеры.

На данный момент у нас пять авторизованных партнёров, которые оказывают услуги SOC на базе RuSIEM. Для того чтобы подать заявку и получить специальные условия для SOC-центров, необходимо отправить заявку на почту partners@rusiem.com.

МЕНЕДЖМЕНТ КАДРОВ В ИБ



Александр МАТВЕЕВ
директор центра мониторинга и противодействия кибератакам IZ:SOC компании «Информзащита»

Информационная безопасность — это крайне быстро развивающаяся сфера. И, как и все высокотехнологичные отрасли, сталкивается с проблемой дефицита кадров. По оценкам специалистов, сегодня в сфере ИБ заняты более 110 тыс. специалистов, при этом нехватка сотрудников составляет около 50 тыс., а к 2027 г. потребность в них может увеличиться в несколько раз.

Кадровая проблема затрагивает все направления информационной безопасности, включая SOC, поскольку именно в этой области наиболее остро ощущается нехватка высококвалифицированных специалистов. В условиях постоянного роста угроз и сложности атак крайне важно, чтобы CISO и руководители центров мониторинга ясно понимали причины текущего кадрового дефицита и обладали эффективными стратегиями управления командой, способными обеспечить оперативную и результативную работу.

КОГО НЕ ХВАТАЕТ SOC?

Создание центров мониторинга и противодействия киберугрозам или использование SOC как полноценного сервиса сегодня — это одни из самых востребованных услуг на рынке ИБ. Как и в других сферах информационной безопасности, здесь существует нехватка специалистов. Анализ вакансий показывает, что наибольший спрос среди специалистов в области SOC приходится на специалистов второй линии SOC (аналитики SOC L2, либо high grade L1) и администраторов средств защиты информации (СЗИ). То есть больше всего работодатели заинтересованы в специалистах среднего уровня квалификации (middle-специалистах), которые составляют около 50% всех открытых вакансий.

Количество открытых позиций для узкопрофильных специалистов меньше, но это не означает, что спрос на них ниже: их редкие и уникальные навыки требуются для решения специфических задач. Здесь речь идёт о сотрудниках третьей линии SOC (аналитики SOC L3), экспертах-форензиках, специалистах по киберразведке и др.

Трудности в поиске также разнятся. Если при поиске аналитиков SOC L1 вопрос стоит в общем количестве специалистов, подготовленных образовательной системой, а при поиске L2 возникает необходимость в наличии комплекса необходимых компетенций и практического опыта, то узкопрофильные эксперты — это сочетание многолетнего опыта и уникальных навыков, что делает их особенно ценными и востребованными. Проблема заключается не только в их ограниченном количестве на рынке, но и в высокой стоимости для работодателей, а также в необходимости разработать стратегии для их удержания в компании.

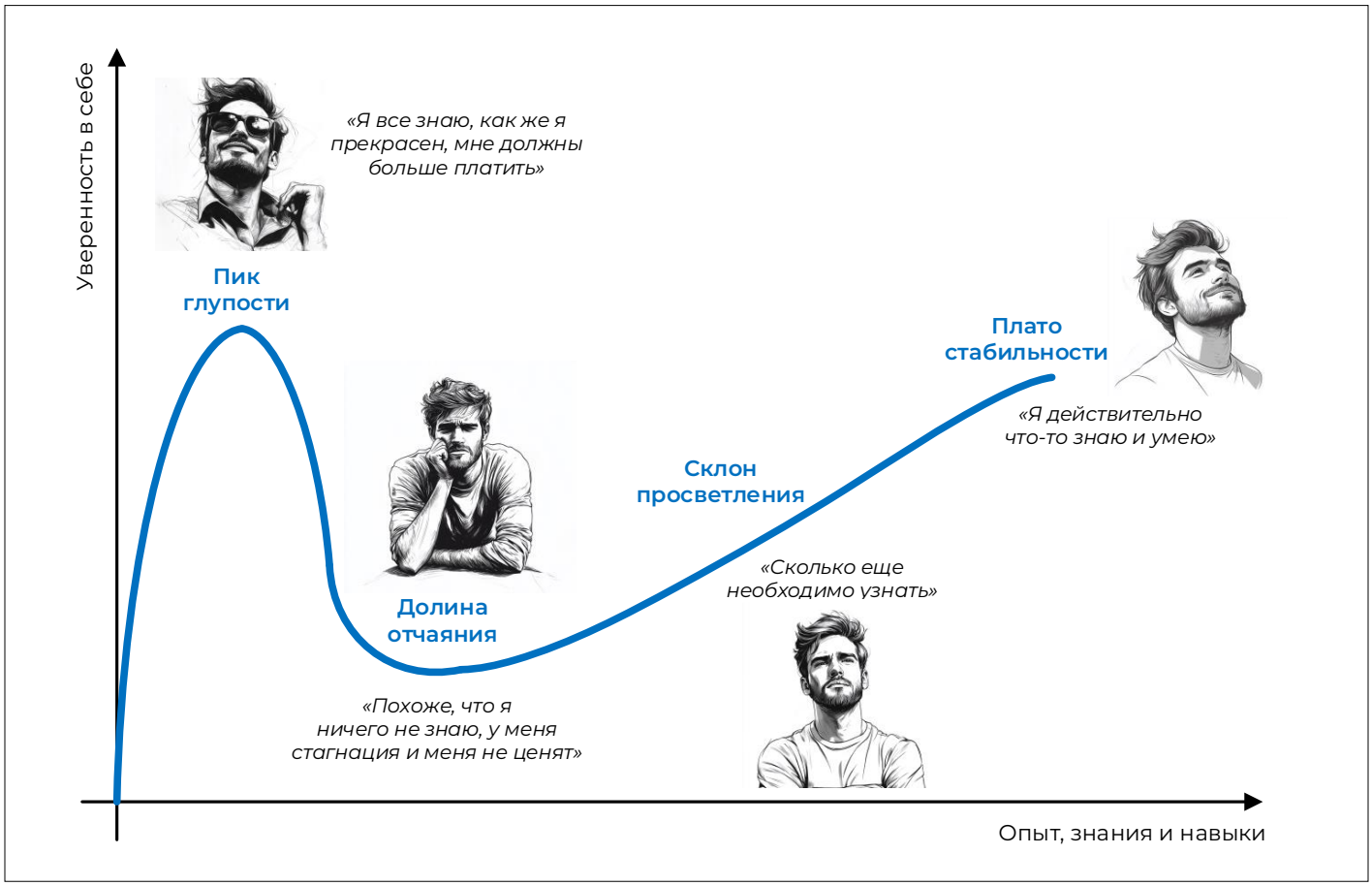


Рисунок 1. График Даннинга — Крюгера хорошо иллюстрирует проблему, когда middle-специалист начинает чувствовать стагнацию: ему кажется, что полученных навыков и опыта достаточно для шага вперёд, а он не происходит…

ПОЧЕМУ ВОЗНИКАЕТ ДЕФИЦИТ КАДРОВ?

Существует несколько основных причин, почему возникает недостаток специалистов:

◆ **Недостаток подготовленных кадров.** Российская образовательная система сегодня не готовит достаточное количество специалистов. По разным оценкам, количественно выпускники ИБ-программ российских вузов могут закрыть в лучшем случае 30% потребностей в кадрах. Более того, выпускники чаще всего имеют хороший теоретический уровень подготовки, но не обладают совсем рабочим опытом или имеют минимальный. Однако, как говорилось выше, работодатели наиболее активно ищут middle-специалистов, то есть тех, у кого есть опыт работы хотя бы от 1 до 3 лет. Следовательно, образовательная система сегодня не может подготовить достаточное количество необходимых кадров, особенно со спецификой работы на разных должностях в SOC.

◆ **Слабый менеджмент.** В современном SOC люди играют столь же важную роль, как технологии и процессы. Руководителю SOC как лидеру команды критически важно обладать высоким уровнем управленческих компетенций, чтобы эффективно формировать и развивать свою команду, учитывая, что многие из них являются уникальными профессионалами с высочайшим уровнем экспертного опыта. Для этого необходимо уметь грамотно обрисовывать карьерные перспективы сотрудников, предотвращать профессиональное выгорание и находить способы повторной мотивации тех, кто уже столкнулся с этим состоянием. Это требует отличных софт-скиллов, высоко развитых навыков эмпатии и способности управлять эмоциональным состоянием коллектива. Кроме выстраивания эффективного взаимодействия внутри команды, руководителю необходимо формировать чёткую рабочую структуру и стратегию, которая обеспечит достижение целей SOC. Это включает в себя внедрение передовых технологий и методов, которые позволят сотрудникам решать стоящие перед ними задачи наиболее эффективно. То есть руководитель SOC должен быть и высококлассным специалистом, полностью понимающим технологическую сторону работы, и первоклассным менеджером, знающим, как управлять людьми, слушать их и находить решения для проблем. Однако лишь немногие обладают по-настоящему качественным сочетанием этих навыков.

◆ **Переоценка своих навыков.** Здесь речь идёт о ситуации, когда middle-специалист начинает чувствовать стагнацию: ему кажется, что полученных навыков и опыта достаточно для шага вперёд, который не происходит в текущей организации. Хорошо иллюстрирует эту проблему график Даннинга — Крюгера (рис. 1).

Часто это происходит с аналитиками SOC L1, которые уже приобрели определённые знания и опыт, либо с аналитиками SOC L2, которые достаточно быстро перешли из первой линии во вторую, но следующий виток карьеры занимает больше времени. Из-за этого создаётся иллюзия, что в другой компании удастся сделать этот самый скачок, и они пытаются уйти, к примеру, в in-house SOC заказчика, где сталкиваются либо с недостатком собственной компетенции, либо с ограниченным количеством задач, ведущим к ещё большему выгоранию. В итоге специалист на определённое время останавливается в собственном развитии, что негативно влияет и на его карьеру, и на кадровую ситуацию на рынке.

КАК ПРЕОДОЛЕВАТЬ ДЕФИЦИТ?

Нехватка кадров заставляет рынок адаптироваться и искать способы преодоления дефицита. Компании на рынке прибегают к разным инструментам.

- **Стажировки в компаниях.** Многие игроки рынка запускают программы стажировок, чтобы компенсировать нехватку опыта и помочь в адаптации молодым специалистам. Такая программа есть и в компании «Информзащита». Здесь стажировка состоит из нескольких этапов: сначала кандидатов отбирают на основе тестовых заданий, далее в течение двух-трёх месяцев начинающие специалисты слушают лекции и выполняют практические задания, а после лучшие из них принимаются в отдел развития компетенций, где окончательно адаптируются в компании и профилируются. Такой подход позволяет получить специалистов с большим набором навыков и опытом, чем у простого выпускника вуза, более того, стажёры лояльнее компании, поскольку видят и ценят её вклад в их профессиональное развитие.
- **Подготовка руководителей.** Человек, стоящий во главе SOC, должен сочетать в себе навыки высококвалифицированного технического специалиста и полноценного менеджера, умеющего работать с людьми. Поэтому важно, чтобы они проходили подготовку в качестве руководителя: изучали психологические аспекты своей работы, развивали софт-скиллы, понимали, когда необходимо действовать как коллега, поддерживая равные отношения в команде, а когда проявлять лидерские качества, эффективно управляя процессами внутри SOC для достижения стратегических целей.
- **Аутсорсинг.** Вероятно, это главный инструмент преодоления дефицита специалистов. Такой формат работы позволяет закрывать недостаток собственных сотрудников за счёт экспертов сторонней компании, которые могут обслуживать нескольких клиентов одновременно. Например, Центр мониторинга и противодействия кибератакам «Информзащиты» IZ:SOC предлагает заказчикам услуги сервисного и гибридного SOC. В первом случае специалисты компании полностью выполняют функции центра в инфраструктуре клиента, осуществляют мониторинг, реагируют на киберугрозы и так далее. Во втором случае специалисты IZ:SOC закрывают недостающие позиции в собственном центре клиента, то есть выступают сторонними экспертами, помогающими полноценно функционировать инфраструктуре информационной безопасности заказчика.

  Также компании прибегают к использованию разовых услуг и отдают их на аутстафф. Например, расследованием киберинцидентов, или, иными словами, форензикой чаще всего привлекают заниматься сторонних специалистов, так как содержать такого эксперта дорого внутри собственной компании и зачастую нецелесообразно, ведь инциденты происходят не каждый день. К таким разовым, но экспертным услугам также относятся разработка правил корреляции и плейбуков, внедрение систем SIEM, IRP/SOAR, TIP, NTA, EDR, комплексный анализ защищённости, включающий Red Team, Purple Team и так далее.
- **Внедрение искусственного интеллекта.** Этот способ сегодня не находится на передовой, и ему предстоит пройти долгий путь развития. Однако эксперты считают, что уже сегодня ему стоит уделять внимание. Существует относительно распространённое мнение, что ИИ в будущем заменит аналитиков SOC L1 и L2, выполняющих рутинные и повторяющиеся задачи. Однако на практике это не совсем так. Вместо полной замены ИИ скорее станет мощным инструментом, который автоматизирует стандартные процессы, позволяя специалистам сосредоточиться на более сложных и аналитических задачах, требующих человеческого интеллекта и опыта. В результате изменится не потребность в этих специалистах, а характер их работы, что откроет новые перспективы для профессионального роста в управлении и оптимизации ИИ-систем.

ЧТО В ИТОГЕ?

Дефицит специалистов по информационной безопасности в целом и сотрудников SOC в частности — это реальность, с которой рынок должен мириться. Однако важно понимать, что существующие проблемы имеют различные пути решения, и те механизмы, которые возникли у рынка для преодоления дефицита, показывают свою эффективность. Одним из ключевых решений является использование сервисных моделей и аутстаффинга, которые позволяют привлекать внешних специалистов для выполнения конкретных задач или функций. Это помогает компаниям поддерживать необходимый уровень безопасности и гибкости в условиях ограниченного кадрового ресурса. Таким образом, борьба с недостатком специалистов должна включать не только увеличение числа работников, но и оптимизацию процессов через использование внешних ресурсов и услуг, что становится важным элементом стратегии обеспечения безопасности в постоянно растущем рынке.

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ МОЖЕТ ИСПОЛЬЗОВАТЬСЯ НЕ ТОЛЬКО ВО БЛАГО, НО И ВО ВРЕД, И ЭТО НУЖНО УЧЕСТЬ В ЗАКОНОДАТЕЛЬСТВЕ»

Василий ПИСКАРЕВ
председатель Комитета Государственной Думы по безопасности и противодействию коррупции

Единый день голосования в этом году не стал исключением. Наш противник, как и прежде, пытался вмешиваться в избирательную кампанию и использовать выборы для расшатывания ситуации в России. И одним из инструментов по-прежнему была вражеская пропаганда. Например, информационные ресурсы, входящие в структуру государственного Агентства США по глобальным медиа (а это русскоязычные подразделения «Радио Свобода», признанного в РФ нежелательной организацией) не только пытались дискредитировать выборы, но и давали конкретные советы, за кого голосовать.

Но несмотря на упорные попытки коллективного Запада дестабилизировать обстановку перед выборами и возросшие террористические атаки ВСУ на приграничные регионы, наши граждане показали, что выступают за развитие страны и курс на Победу. Об этом говорит их готовность участвовать в выборах и явка.

Слаженная работа Центризбиркома и всех ветвей власти позволила обеспечить проведение выборов в полном соответствии с законами России. И с полным доверием избирателей.

Впереди у нас важная электоральная кампания 2026 года — выборы в Государственную Думу. Очевидно, что будут новые вызовы и новые попытки вмешательства. Будем реагировать, в том числе в законодательной плоскости. Для успешного противодействия подрывной деятельности против нашей страны важно изучить методы и технологии, которые используют недружественные страны для вмешательства в наши внутренние дела.

ИСПОЛЬЗОВАНИЕ ДИПФЕЙКОВ

Одной из особенностей минувших выборов стало не просто использование противником фейков для того, чтобы повлиять на наших избирателей (это уже стало обыденным приёмом), но, пожалуй, впервые в нашей стране зафиксировано применение на выборах так называемых дипфейков (deepfake), иными словами видеофрагментов, измененных с помощью искусственного интеллекта.

Искусственный интеллект (ИИ) всё активнее внедряется в нашу повседневную жизнь и уже приносит много пользы. В частности, помогая медикам распознавать симптомы заболевания по результатам УЗИ и рентгеновским снимкам, или облегчая труд криминалистов в поиске преступников и создании фотороботов, а студентам упрощая написание дипломных работ. В Москве и Санкт-Петербурге уже тестируют беспилотный трамвай, а роботы-курьеры известной компании развозят заказы. И сфер применения ИИ в обиходе будет становиться всё больше.

Что же касается выборов, то, к примеру, один из индийских парламентариев использовал метод дипфейка для привлечения симпатий избирателей вполне благовидным способом — записал обращение на языках народов Индии, которыми он не владеет. Одним словом, человечество успешно учится использовать возможности ИИ во благо развития. Однако такой прогресс в обучении и расширении сфер применения ИИ не исключает его попадания в нечистоплотные руки. И всё чаще дипфейки используются в мошеннических целях, а технологии так быстро развиваются, что распознать подмену становится всё труднее.

Сегодня дипфейк открывает широкие возможности в области кино, позволяя оживить в современных фильмах давно ушедших от нас актеров. Оставляя за рамками этическую сторону дела, замечу, что подобные манипуляции с их видеоизображениями и голосом уже причиняют проблемы и ныне здравствующим артистам. Фейковые видео и голосовые сообщения от их имени распространяют мошенники, пытаясь выманить деньги у их знакомых.

Василий Пискарев. Пресс-конференция в Инфоцентре ЦИК РФ по итогам Единого дня голосования 8 сентября 2024 г.

ОТСУТСТВИЕ ТВЕРДОЙ ПОЧВЫ

Появление такого вида правонарушений в отсутствие внятного этического и правового регулирования представляет серьезную опасность для современного общества. Использование дипфейков открывает преступникам широкие возможности для шантажа, для подрыва репутации неугодных политиков и обычных граждан, для манипулирования общественным сознанием. Дипфейки оскорбляющие общественную мораль, религиозные чувства верующих, экстремистского содержания могут быть использованы для дестабилизации обстановки, как в отдельных населенных пунктах, так и в государстве в целом. А совершенство технологий с каждым днем все более повышает достоверность восприятия подобного контента.

РЕГУЛИРУЮЩИЕ МЕРЫ

Во многих странах уже задумались над этим и стали вводить регулирующие меры. В частности, уголовное наказание за распространение дипфейков порнографического содержания уже применяется в Японии, Австралии и других странах. В ряде государств необходимо делать обязательную пометку, что фото были подвергнуты компьютерной обработке, а также запрещено создание и распространение дипфейковых видео для влияния на выборы. А в Китае теперь требуется маркировать любой контент, измененный с помощью ИИ, чтобы не вводить людей в заблуждение.

* * *

В Государственной Думе также ведется работа над законопроектами по правовому регулированию использования искусственного интеллекта. Поспешая по пути цифровизации и научного прогресса, очень важно сохранить наш цифровой суверенитет, не допустить использование ИИ в целях умышленного причинения вреда гражданам и юридическим лицам и защитить безопасность нашей страны в киберпространстве.

КВАРТАЛЬНЫЙ ОТЧЁТ

О НОРМАТИВНОМ РЕГУЛИРОВАНИИ В СФЕРЕ ИБ В III КВАРТАЛЕ

Екатерина РАЧКОВА
обозреватель BIS Journal

ПОДВЕДЕНИЕ ПРОМЕЖУТОЧНЫХ ИТОГОВ

В рамках подведения промежуточных итогов в III квартале 2024 года были опубликованы:

- 17.07.2024 сведения о принятых национальных и международных стандартах за II квартал 2024 года (на сайте ФСТЭК России);
- 20.08.2024 обзор отчётности об инцидентах информационной безопасности при переводе денежных средств за II квартал 2024 года (на сайте Банка России);
- 03.09.2024 справка-доклад о ходе работ по плану ТК 362 «Защита информации» на 2024 год (по состоянию на 30.08.2024);
- 05.09.2024 (до этого — 19.08.2024) перечень организаций, осуществляющих образовательную деятельность, имеющих дополнительные профессиональные программы в области информационной безопасности, согласованные с ФСТЭК России;
- 13.09.2024 обновлённые по состоянию на 13.09.2024: перечень органов по аттестации, реестр аккредитованных ФСТЭК России органов по сертификации и испытательных лабораторий и государственный реестр сертифицированных средств защиты информации (доступно на сайте реестров ФСТЭК России).

О новых разрабатываемых и утверждённых документах расскажем далее.

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА (КИИ)

10.07.2024 ФСТЭК России был представлен проект Постановления Правительства Российской Федерации «О внесении изменений в Правила категорирования объектов критической информационной инфраструктуры Российской Федерации».

Если изменения будут приняты, с субъектов КИИ будет снята обязанность разработки перечней объектов КИИ, подлежащих категорированию.

05.08.2024 был опубликован проект постановления Правительства Российской Федерации «О внесении изменений в постановление Правительства Российской Федерации от 14.11.2023 № 1912». Проектом предлагается внести изменения в Правила перехода субъектов КИИ на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах КИИ.

20.08.2024 Минтруда Российской Федерации опубликовало проект ведомственного акта об утверждении профессионального стандарта «Специалист по обеспечению безопасности значимых объектов критической информационной инфраструктуры».

ПЕРСОНАЛЬНЫЕ ДАННЫЕ (ПДН)

Вступил в силу (частично с 08.08.2024) Федеральный закон от 08.08.2024 № 233-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных».

Настоящим законом разрешено использование средств защиты информации с функцией уничтожения данных, определены особенности обработки обезличенных ПДн при формировании составов данных и предоставления доступа к ним, урегулирована передача обезличенных ПДн в ГИС Минцифры.

Изменения вступили в силу со дня опубликования, за исключением некоторых положений, для которых был установлен иной срок (п.п. 1–3, 5 статьи 1, статья 2 Федерального закона вступят в силу с 01.09.2025).

ПРЕЗИДЕНТ И ПРАВИТЕЛЬСТВО РФ

11.07.2024 было опубликовано постановление Правительства Российской Федерации от 10.07.2024 № 929 «Об утверждении Положения о государственной единой облачной платформе» (в части требований к обеспечению информационной безопасности в рамках предоставления облачных услуг)».

В Положении определены цели, задачи и основные принципы функционирования единой облачной платформы, основные группы предоставляемых облачных услуг, состав участников и их функции. Постановление вступит в силу с 01.01.2025, с этой же даты Единая облачная платформа будет функционировать в полном объёме.

08.08.2024 опубликован и вступил в силу Федеральный закон от 08.08.2024 № 216-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации».

В числе прочего настоящим законом:

- на владельца социальной сети возлагается обязанность выявления в том числе информации, оскорбляющей человеческое достоинство и общественную нравственность, выражающей явное неуважение к обществу, содержащей изображение действий с признаками противоправных, в том числе насильственных, и распространяемой из хулиганских, корыстных или иных низменных побуждений;
- на оператора связи возлагается обязанность по установке в своей сети предоставляемых Роскомнадзором технических средств контроля, предусматривающих ограничение доступа к информации, а также обязанность предоставлять в Роскомнадзор информацию, позволяющую идентифицировать средства связи и пользовательское оборудование (оконечное оборудование) в сети Интернет на территории Российской Федерации, территории субъекта Российской Федерации или части территории субъекта Российской Федерации;
- Роскомнадзор наделяется полномочиями по управлению сетью связи общего пользования путём управления техническими средствами противодействия угрозам или путём передачи обязательных к выполнению указаний операторам связи, собственникам или иным владельцам технологических сетей связи, собственникам или иным владельцам точек обмена трафиком, собственникам или иным владельцам линий связи, пересекающих Государственную границу Российской Федерации, иным лицам;
- скорректирован порядок лицензирования деятельности в области оказания услуг связи.

22.08.2024 было опубликовано «Соглашение между Правительством Российской Федерации и Правительством Исламской Республики Иран о сотрудничестве в области обеспечения информационной безопасности» от 26.01.2021. Документ вступил в силу 15.08.2024.

01.09.2024 вступило в силу Постановление Правительства Российской Федерации от 26.08.2024 № 1151 «Об образовании регионального сегмента единой биометрической системы в г. Москве». В соответствии с Постановлением в Москве будет образован региональный сегмент единой биометрической системы (ЕБС) и определены случаи использования сегмента, предоставления векторов ЕБС, использования ЕБС с применением биометрических ПДн, размещённых через региональное мобильное приложение системы, актуальные до 01.01.2027.

МИНЦИФРЫ РФ

19.08.2024 был опубликован приказ Минцифры Российской Федерации от 01.08.2024 № 682 «О внесении изменения в перечень индикаторов риска нарушения обязательных требований при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных, утверждённый приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 15.11.2021 № 1187».

Документ определяет новый индикатор риска нарушения обязательных требований для госконтроля за обработкой персональных данных, связанный с выявлением в предоставленных владельцем сайта данных или в ходе проверки в течение календарного года двух и более фактов несоответствия установленным правилам информации, связанной с применением рекомендательных технологий в рамках предоставленного контролируемым лицом доступа к программно-техническим средствам этих технологий.

30.08.2024 вышел приказ Минцифры Российской Федерации от 31.07.2024 № 677 «Об утверждении требований о защите информации при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно подключённой к информационно-телекоммуникационной сети «Интернет», операторам государственных информационных систем, муниципальных информационных систем, информационных систем государственных и муниципальных унитарных предприятий, государственных и муниципальных учреждений».

Приказ устанавливает для провайдеров хостинга требования к защите информации (в том числе с использованием криптографических средств) при предоставлении вычислительной мощности для размещения сведений в информационной системе, постоянно подключённой к сети Интернет.

ФСТЭК РОССИИ, ТК №26 «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

17.07.2024 были опубликованы проекты документов ТК № 26 «Криптографическая защита информации»:

- Рекомендации по стандартизации «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе получения актуальных статусов сертификатов (OCSP)»;
- Рекомендации по стандартизации «Информационная технология. Криптографическая защита информации. Ключевая система сети шифрованной связи с использованием ККСВ ВРК с сетевой топологией „звезда“»;
- Рекомендации по стандартизации «Информационная технология. Криптографическая защита информа-

ции. Ключевая система полносвязной многоарендаторной сети шифрованной связи на базе ККС ВРК с ДПУ».

Также был выпущен проект документа ТК № 058 «Функциональная безопасность»: ГОСТ Р/IEC TS 63074:2023 «Безопасность машин. Вопросы защиты информации в системах управления, связанных с обеспечением функциональной безопасности».

18.07.2024 ФСТЭК России опубликовал проект приказа «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утверждённые приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17, и Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утверждённые приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239».

Проект приказа конкретизирует требования по защите информации, содержащейся в государственных информационных системах (ГИС) и информационных системах значимых объектов КИИ от угроз атак типа «отказ в обслуживании».

01.08.2024 ФСТЭК России также был выпущен Приказ от 27.06.2024 № 127 «Об утверждении форм документов, используемых ФСТЭК России и её территориальными органами при осуществлении и по результатам федерального государственного контроля за обеспечением защиты государственной тайны в пределах компетенции ФСТЭК России», зарегистрированный 01.08.2024 за № 78984.

Приказом были утверждены формы:

- приказа о проведении плановой (внеплановой) выездной проверки;
- акта проверки;
- предписания о приостановлении работ, связанных с использованием государственной тайны;
- предписания об устранении выявленных нарушений.

08.08.2024 ФСТЭК России был опубликован Проект приказа «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

БАНК РОССИИ

12.08.2024 Банком России был опубликован проект Указания «О внесении изменений в Положение Банка России от 17 августа 2023 года № 821-П».

Было предложено внести изменения в части требований к обеспечению защиты информации при осуществлении переводов денежных средств, а также о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств. Изменения касаются:

- определения обязанности реализации наиболее высокого из требуемых нормативными актами Банка России уровней защиты информации при определённых условиях;
- установления сроков предоставления сведений об инцидентах операторами по переводу денежных средств, операторами услуг платёжной инфраструктуры в Банк России (в том числе по запросу Банка России);
- установления требований к расчёту значений показателей оценки выполнения требований к мерам защиты информации в отношении технологии безопасной обработки защищаемой информации и оценки выполнения требований к мерам защиты информации в отношении прикладного программного обеспечения автоматизированных систем и приложений;
- установления требования об осуществлении деятельности по планированию, реализации, контролю и совершенствованию мер и мероприятий, направленных на реализацию требований, применяемых в отношении прикладного программного обеспечения автоматизированных систем и приложений и в отношении технологии обработки защищаемой информации;
- определения права субъекта Национальной платёжной системы по реализации процессов разработки программного обеспечения и приложений, включающих меры обеспечения безопасного жизненного цикла разработки программного обеспечения и приложений;
- расширения перечня сведений о действиях клиентов участников национальной платёжной системы, осуществляемых в рамках переводов денежных средств, подлежащих регистрации и хранению.

В то же время был выпущен и проект указания «О внесении изменений в Положение Банка России от 20.04.2021 № 757-П».

Предполагались изменения в части установления обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций, касающиеся:

- распространения требований по реализации минимального уровня защиты информации, установленного национальным стандартом Российской Федерации ГОСТ Р 57580.1–2017 на микрофинансовые организации, операторов инвестиционной платформы (с некоторыми оговорками);
- определения обязанности реализации наиболее высокого из требуемых нормативными актами Банка России уровней защиты информации при определённых условиях;
- установления сроков предоставления сведений об инцидентах некредитными финансовыми организациями в Банк России (в том числе по запросу Банка России);
- установления требований к расчёту значений показателей оценки выполнения требований к мерам защиты информации в отношении технологии безопасной обработки защищаемой информации и оценки выпол-

нения требований к мерам защиты информации в отношении прикладного программного обеспечения автоматизированных систем и приложений;

- корректировки значения термина «получатель финансовых услуг»;
- установления требования об осуществлении деятельности по планированию, реализации, контролю и совершенствованию мер и мероприятий, направленных на реализацию требований, применяемых в отношении прикладного программного обеспечения автоматизированных систем и приложений и в отношении технологии обработки защищаемой информации;
- определения права некредитных финансовых организаций по реализации процессов разработки программного обеспечения и приложений, включающих меры обеспечения безопасного жизненного цикла разработки программного обеспечения и приложений;
- распространения требований по использованию электронной подписи для некредитных финансовых организаций, реализующих минимальный уровень ГОСТ Р 57580.1;
- установления требований по регистрации информации о действиях клиентов при приёме электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети Интернет.

20.08.2024 Банк России опубликовал «Методические рекомендации по установлению целевых значений и расчёту фактических значений количественных контрольных показателей уровня риска информационной безопасности, связанных с осуществлением перевода денежных средств без добровольного согласия клиента и связанных с заключением кредитных договоров (договоров займа) без добровольного согласия клиента, а также установлению пороговых значений и расчёту фактических значений ключевых индикаторов риска информационной безопасности» № 13-МР.

Документ содержит новые методические рекомендации по установлению пороговых значений индикаторов и целевых значений показателей, а также по расчёту фактических значений индикаторов и показателей.

ОТРАСЛЕВЫЕ ДОКУМЕНТЫ

30.07.2024 появился проект постановления Правительства Российской Федерации «О внесении изменений в Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности».

Напоминаем, что такие документы полезно рассмотреть как примеры проработки вопросов аналогичного содержания в других организациях и ведомствах.

— Видишь суслика?
— Нет.
— И я не вижу. А он есть.
К/ф «ДМБ»

НА КОЛУ МОЧАЛО, НАЧИНАЙ СНАЧАЛА

ЭССЕ НА ТЕМУ ОБЕЗЛИЧИВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПОЗИЦИИ РОСКОМНАДЗОРА ПО ЭТОМУ ВОПРОСУ

Сергей ВИХОРЕВ
советник генерального директора
ООО «Умные решения»

Сейчас скажут: «Ну, опять жвачку будут жевать!» И да, и нет. Тема, конечно, не новая, но с принятием в августе этого года закона[1], вносящего изменения в закон «О персональных данных», она получила новый импульс развития, направленный на создание механизма формирования обезличенных составов персональных данных (дата-сетов).

Я позволю себе вступить в дискуссию с заместителем руководителя Роскомнадзора господином Милошем Эдуардовичем Вагнером, который при подготовке этого закона неоднократно публично заявлял[2], что персональные данные, которые получены в результате обезличивания, всё равно «остаются персональными» и формально, и юридически, потому что всё ещё характеризуют человека, а с дополнительной информацией и прямо на него указывают. И далее: «В обезличенных персональных данных убраны прямые идентификаторы, которые не позволяют человеку сопоставить их с собой. Но это нетрудно машине, тем, у кого есть вычислительные мощности или доступ к нейронным сетям»[3]. Что-то здесь не так, в одном предложении уже заложены противоречия. Давайте разберёмся.

ПО БУКВЕ ЗАКОНА...

Будем опираться на основное определение[4] персональных данных из ФЗ-152. По заявлению господина Вагнера, в обезличенных персональных данных убраны прямые идентификаторы, которые не позволяют человеку сопоставить их с собой. То есть, говоря обычным языком, обезличенные данные нельзя однозначно соотнести с конкретным субъектом и уж тем более определить этого человека, так как нет «прямых идентификаторов». Но это значит, что такие данные не соответствуют ключевому определению, так как их нельзя привязать к определённому субъекту или определить по ним конкретного субъекта. Они есть и принадлежат некоему Имяреку, которого никто не знает. Поэтому заявление господина Вагнера о том, что данные, которые получены в результате обезличивания, всё равно «остаются персональными», мягко говоря, противоречат букве закона.

Я, конечно, уважаю такую организацию, как Роскомнадзор в целом, и лично господина Милоша Вагнера как одного из руководителей этой организации, но в российской юриспруденции право трактовать положения законов является прерогативой Верховных судов, а Положением о Роскомнадзоре[5] ему такого права не предоставлено. Так что при всём уважении, пока нет нормативно-правового акта, изменяющего ключевое понятие «персональные данные», мнение господина Вагнера может быть расценено исключительно как частное мнение (впрочем, как и моё). Кстати, новый ФЗ-233 также не даёт оснований считать, что понятие персональных данных изменено, он регулирует совсем другую сферу. Ну и как вы думаете, на чьей стороне будет суд, если он объективный?

[1] Федеральный закон от 08.08.2024 № 233-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона „О персональных данных“».

[2] https://tass.ru/obschestvo/19484395.

[3] https://iz.ru/1533308/2023-06-23/v-roskomnadzore-otcenili-ispolzovanie-obezlichennykh-personalnykh-dannykh.

[4] Персональные данные — любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных), Федеральный закон № 152-ФЗ, ст. 3 п. 1.

[5] Постановление Правительство РФ от 16.03.2006 № 228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций».

ПО ДУХУ ЗАКОНА...

Конечно, закон «О персональных данных» прежде всего направлен на защиту интересов субъектов персональных данных — это императив! Теперь о том, что «обезличенные данные всё равно и формально, и юридически всё ещё характеризуют человека, а с дополнительной информацией и прямо на него указывают». Господа, у вас всё в порядке с формальной логикой? Да, действительно, даже обезличенные данные могут характеризовать человека, но КОГО? Homo sapiens, Имярек — точно. Но сказать более конкретно — нельзя. Правда, есть продолжение фразы «но это нетрудно машине, тем, у кого есть вычислительные мощности или доступ к нейронным сетям». Видимо, речь идёт о том, что с помощью нейросети можно легко обработать именно ДОПОЛНИТЕЛЬНУЮ информацию и принести вред субъекту. Что ж, это возможно, но тогда мы опять выходим за рамки буквы закона, это нарушает определение процедуры обезличивания, установленное законом[6]. Ключевое слово здесь ДОПОЛНИТЕЛЬНАЯ информация.

Говоря простым языком, использование вычислительных мощностей или нейронных сетей для получения дополнительной информации — это нарушение закона, так как используются не только обезличенные данные, но и дополнительная информация. И идентификация субъекта происходит именно по дополнительной информации, и только потом к нему привязываются обезличенные данные. Да, это может причинить вред субъекту. Но регулировать в этом случае надо не оборот персональных данных, прошедших процедуру обезличивания, а оборот дополнительной информации или использование нейросетей, которые позволяют «деобезличить» эти персональные данные. А то получается действие по принципу «у меня нет бритвы, но есть топор, поэтому брить не будем, отрубим голову».

ЧТО ДЕЛАТЬ?

Ну, это извечный российский вопрос, но и на него есть ответ.

Во-первых, надо отделить мух от котлет и не путать понятия «персональные данные» и «обезличенные данные». Кстати, бытует мнение (я с этим сталкивался), что так как процедура обезличивания по закону относится к обработке персональных данных[7], то и обезличенные данные будут персональными (опять нарушение формальной логики). Результат процедуры обезличивания не должен содержать исходную информацию. По аналогии: есть секретный текст, который проходит криптопреобразование. Что будет на выходе? Тоже секретный текст? Конечно нет! И его можно передавать по открытым каналам связи. Так и здесь: результат процедуры обезличивания — это не персональные данные, а набор неких отвлечённых данных.

Во-вторых, надо чётко определить те самые «прямые идентификаторы» (я бы назвал их «идентификационные персональные данные»), которые позволяют однозначно идентифицировать субъекта. К сожалению, в законе «О персональных данных» такого определения нет, а жалко, это сняло бы много вопросов и казусов. Но, с другой стороны, статья 6 ГК РФ позволяет, когда какой-то вопрос не определён, использовать аналогию права и аналогию закона. У нас есть несколько нормативно-правовых актов, которые регулируют процедуру идентификации (установление личности) субъекта[8]. Это позволяет сказать, что набор данных из фамилии, имени, отчества, пола, даты рождения и места рождения субъекта позволяет однозначно его идентифицировать. Вот и надо законодательно закрепить этот набор как идентификационные персональные данные.

В-третьих, необходимо законодательно закрепить необходимость применения самых жёстких требований по защите (например, первый усиленный уровень защищённости) баз данных, содержащих идентификационные персональные данные (полные или неполные — это вопрос к обсуждению экспертами), в том числе при размещении таких баз данных в сети Интернет или массивах big data, а также определить порядок оборота таких баз данных.

В-четвёртых, надо ввести очень жёсткий репрессивный механизм за нарушения требований по защите информации или правил обработки баз данных, содержащих идентификационные персональные данные, вплоть до «десяти лет расстрела».

Ну а что делать с теми данными, что уже «утекли»? Здесь вопрос сложнее, и, думаю, на сегодня мало кто может предложить радикальное решение этой проблемы. Хотя, как всегда, есть «два путя»: «оптимистический» и «пессимистический». Оптимистический предполагает, что если будут реализованы выше озвученные пункты и они будут неукоснительно выполняться, то лет через пять, скорее всего, эти «утёкшие» данные устареют и потеряют свою актуальность. Пессимистический же предполагает разработку специального программного продукта (поисковая машина?), который сможет отслеживать несанкционированное появление баз данных с идентификационными персональными данными в публичной сети и их блокирование. И этим как раз и может заняться Роскомнадзор.

Таково сугубо моё мнение.

---

[6] Обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных, Федеральный закон № 152-ФЗ, ст. 3 п. 9.

[7] Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, Федеральный закон № 152-ФЗ, ст. 3 п. 3.

[8] Постановление Правительства РФ № 828 «Положение о паспорте гражданина РФ»; Уголовно-процессуальный Кодекс РФ, ст. 265.

PAM, NGFW И SOC

СТРАТЕГИЧЕСКАЯ ТРИАДА ДЛЯ УСПЕШНОГО ИМПОРТОЗАМЕЩЕНИЯ

Импортозамещение в условиях санкций и ограничений в доступе к иностранным технологиям заставляет менять отношение к подходам в обеспечении информационной безопасности. Защитить базовые критические системы и применить возможности ИБ-решений по максимуму — вот первоочередные вопросы большинства российских компаний сегодня. Работоспособные центры управления безопасностью (SOC) и функциональные межсетевые экраны нового поколения (NGFW) стали самыми востребованными системами, на основе которых организации выстраивают свою защиту.

Вместе с экспертами российской компании «АйТи Бастион» обсудим значимость защиты привилегированных доступов в контексте NGFW и SOC.

ПРО SOC

Финансовый сектор и финтех-компании активно включились в процесс импортозамещения. С одной стороны, они особенно уязвимы перед киберугрозами, с другой — находятся под строгим контролем в части соблюдения законодательных норм, с третьей — всегда должны сохранять операционную устойчивость. Важно, чтобы новые решения могли интегрироваться в существующую инфраструктуру, поддерживая высокий уровень защиты данных и минимизируя риски, связанные с санкциями и повышенным вниманием со стороны киберпреступников.

SOC как центр мониторинга ИБ по определению занимает центральное место в защите всей области ИТ-инфраструктуры компании, включая, помимо прочего, сети, программное обеспечение и существующие данные.

Владимир АЛТУХОВ
руководитель технического центра «АйТи Бастион»

Когда мы говорим о доступе к объектам в рамках серьёзной инфраструктуры, важно учитывать, что он может быть как удалённым, так и внутренним. На этапе подключения, который часто называют «последней милей», эти виды доступа практически неразличимы с точки зрения рисков и уязвимостей. Именно поэтому контроль корректной конфигурации систем, отвечающих за сбор, анализ и реагирование на потенциальные инциденты, становится критически важным. Малейшая ошибка на этом уровне может привести к недопустимым событиям, способным поставить под сомнение целесообразность существования SOC и оправданность вложенных в него ресурсов.

Особую роль в этом процессе играет управление доступом к критически важным системам, таким как SIEM, например, которые являются ядром SOC. Использование PAM-решений помогает контролировать пользователей на пути к этим системам, предотвращая несанкционированный доступ. Однако нельзя забывать и о собственных системах безопасности: изменения их конфигураций могут стать одним из возможных векторов атаки. Игнорирование этого аспекта может привести к серьёзным последствиям, включая компрометацию всей инфраструктуры. Таким образом, комплексный подход к защите и управлению конфигурацией, включая мониторинг и контроль всех этапов доступа, должен быть в приоритете для поддержания надёжной и устойчивой к атакам сети.

Но SOC, собранный даже из изученных группой безопасности систем, сам нуждается в защите.

Ввиду критичности систем, содержащихся в SOC, доступ к нему должен быть организован с учётом всех необходимых мер безопасности. Даже если основная часть сотрудников располагается непосредственно в инфраструктуре, удалённый доступ в современных реалиях полностью исключать нельзя. А соответственно, он должен быть под контролем. Кроме того, невозможно исключать и необходимость контроля доступа к критически важным объектам инфраструктуры внутри контура.

Применение российской PAM-платформы СКДПУ НТ позволяет обеспечить контролируемый доступ, управление парольной политикой и её жизненным циклом. Также её можно активно использовать в системах автоматизации процессов и расследовании инцидентов. К примеру, контроль конфигурации системы сбора данных, контроль доступа к данным объектов и т.п.

Любой внешний пользователь, получающий доступ к инфраструктуре, проходит дополнительный контроль и аутентификацию с помощью СКДПУ НТ и автоматически получает собственный профиль в подсистеме мониторинга и аналитики. Тем самым любое отклонение в стандартном поведении пользователя, начиная с его геолокации и заканчивая пулом команд, подлежит анализу и детектированию. Факт действий пользователей, работающих с объектами системы, логируется и проверяется. В случае возникновения подозрений на нелегитимный доступ платформа позволяет оперативно локализовать источник проблемы в разрезе «внешний пользователь / внутренний пользователь / объект инфраструктуры».

Помимо стандартных функций записи действий и видеозаписи работы в инфраструктуре, СКДПУ НТ позволяет реагировать на определяемые инциденты в автоматическом режиме. Так пресекаются возможности по развитию и закреплению атаки. Несмотря на то что современные SOC обладают полнофункциональными инструментами классов IRP/SOAR, применение реагирования на стороне профильной системы контроля удалённого доступа оправдано с точки зрения эшелонированной защиты контура.

ПРО NGFW

Межсетевые экраны предоставляют расширенные возможности фильтрации трафика, обнаружения и предотвращения вторжений, глубокий анализ данных. Они эффективно обеспечивают защиту корпоративных сетей от внешних угроз (атак «нулевого дня», фишинга и других видов вредоносного воздействия). Многие отечественные разработки способны заменить зарубежные аналоги, при этом надо быть готовым к тому, что их интеграция потребует тщательного планирования и настройки.

Совместное использование NGFW и PAM-систем представляет собой мощный инструмент для оптимизации кибербезопасности — так пользователь не только получает внешнюю фильтрацию, но и минимизирует риски внутренних угроз благодаря контролю привилегий администраторов.

ПРО СОВЕТЫ

Финансовым компаниям, чтобы успеть завершить процесс импортозамещения к 1 января 2025 года, необходимо действовать по чётко структурированному плану. По мнению экспертов «АйТи Бастион», важно провести аудит текущей ИТ-инфраструктуры, выявить все критически важные компоненты, которые зависят от зарубежных технологий. На основе этого анализа нужно разработать дорожную карту по замене этих решений на отечественные аналоги или на те, которые уже адаптированы к российским условиям.

Далее необходимо ускорить процессы закупки и внедрения новых решений, уделяя особое внимание критическим системам, таким как управление доступом, защита периметра и мониторинг безопасности. Важно также заранее обеспечить квалифицированную поддержку и обучение персонала для работы с новыми системами, чтобы минимизировать риски, связанные с переходом на новые технологии.

Кроме того, взаимодействие с регуляторами и соблюдение всех требований законодательства, включая стандарты безопасности, должно стать приоритетом на всех этапах импортозамещения. В условиях сжатых сроков критически важно поддерживать гибкость в планировании и готовность к быстрым корректировкам стратегии в ответ на возможные изменения в технологической и экономической среде.

Алексей ШИРИКАЛОВ
руководитель группы поддержки продаж «АйТи Бастион»

Интеграция систем двух классов позволяет бизнесу создать многослойную защиту, где NGFW обеспечивает контроль на уровне сети, а PAM-платформы — на уровне привилегированных пользователей и их прав. Такое сочетание позволяет не только улучшить общую безопасность, но и оптимизировать процессы реагирования на инциденты за счёт единого мониторинга и управления.

Преимущества внедрения отечественных PAM-систем сегодня:

- Технологическая независимость и гарантия работоспособности продуктов вне контекста внешних условий или новых санкций.
- Соблюдение требований законодательства и стандартов регуляторов в области защиты информации.
- Гибкость и кастомизация под задачи заказчика благодаря плотному взаимодействию с разработчиками.

ВОПРОС ВРЕМЕНИ

ПОЧЕМУ УСТРОЙСТВА КЛАССА «ДИОД» ВСЁ БОЛЬШЕ ВОСТРЕБОВАНЫ ДЛЯ ОРГАНИЗАЦИИ ЭШЕЛОНИРОВАННОЙ ЗАЩИТЫ

Вячеслав ПОЛОВИНКО
руководитель направления собственных продуктов АМТ-ГРУП

Задача обеспечения информационной безопасности банковского и финансового секторов — одна из приоритетных для государства. Безопасность в этой сфере является фактором, обеспечивающим устойчивость экономики отдельных отраслей и страны в целом.

ФИЗИЧЕСКАЯ ИЗОЛЯЦИЯ

С точки зрения типовой модели угроз для банковского и финансового сектора наиболее разрушительными оказываются последствия реализации угрозы несанкционированного доступа со стороны стороннего или внутреннего злоумышленника в защищённые («доверенные», закрытые) сегменты сети периметра финансовой организации.

Один из наиболее действенных способов защитить сетевой периметр «доверенного» сегмента от любого несанкционированного воздействия извне — его физическая изоляция от внешних («менее доверенных») сетей.

Среди СЗИ, обеспечивающих сетевую сегментацию, управление и маршрутизацию сетевыми потоками, только устройства класса «диод» способны именно физически изолировать сетевой сегмент от внешней сети, сохраняя возможность передачи требуемых (и часто обезличенных) данных внешним потребителям. Решение этой задачи достигается за счёт наличия в устройствах класса «диод» одностороннего канала — а именно функционирования передатчика света, направленного в одну сторону — во внешнюю сеть, — и отсутствие приёмника света на передающей стороне, что фактически формирует аналог «воздушного зазора». Данный принцип работы исключает ключевой вектор удалённой атаки на защищаемую (изолируемую) сеть, делая поверхность атаки минимальной, а организацию самой атаки по этому каналу связи полностью невозможной.

ПРИЧИНЫ «ЗАПАЗДЫВАНИЯ»

Однако, несмотря на это значимое преимущество, устройства класса «диод» в настоящий момент не так распространены в банковском и финансовом секторе в сравнении с другими СЗИ, устанавливаемыми на границе защищаемого периметра и в сравнении с использованием «диодов» в других секторах экономики. Их применение только набирает обороты.

Причина 1:
непрозрачные требования

Причин такого «запаздывания» несколько. Первой и наиболее весомой из них является тот факт, что требования профильных регуляторов, предъявляемые конкретно к применению устройств класса «диод» в банковском и финансовом секторе, прописаны недостаточно прозрачно. Это, в свою очередь, позволяет предприятиям ссылаться на «необязательность» использования такого класса СЗИ.

Причина 2:
неосведомлённость заказчика

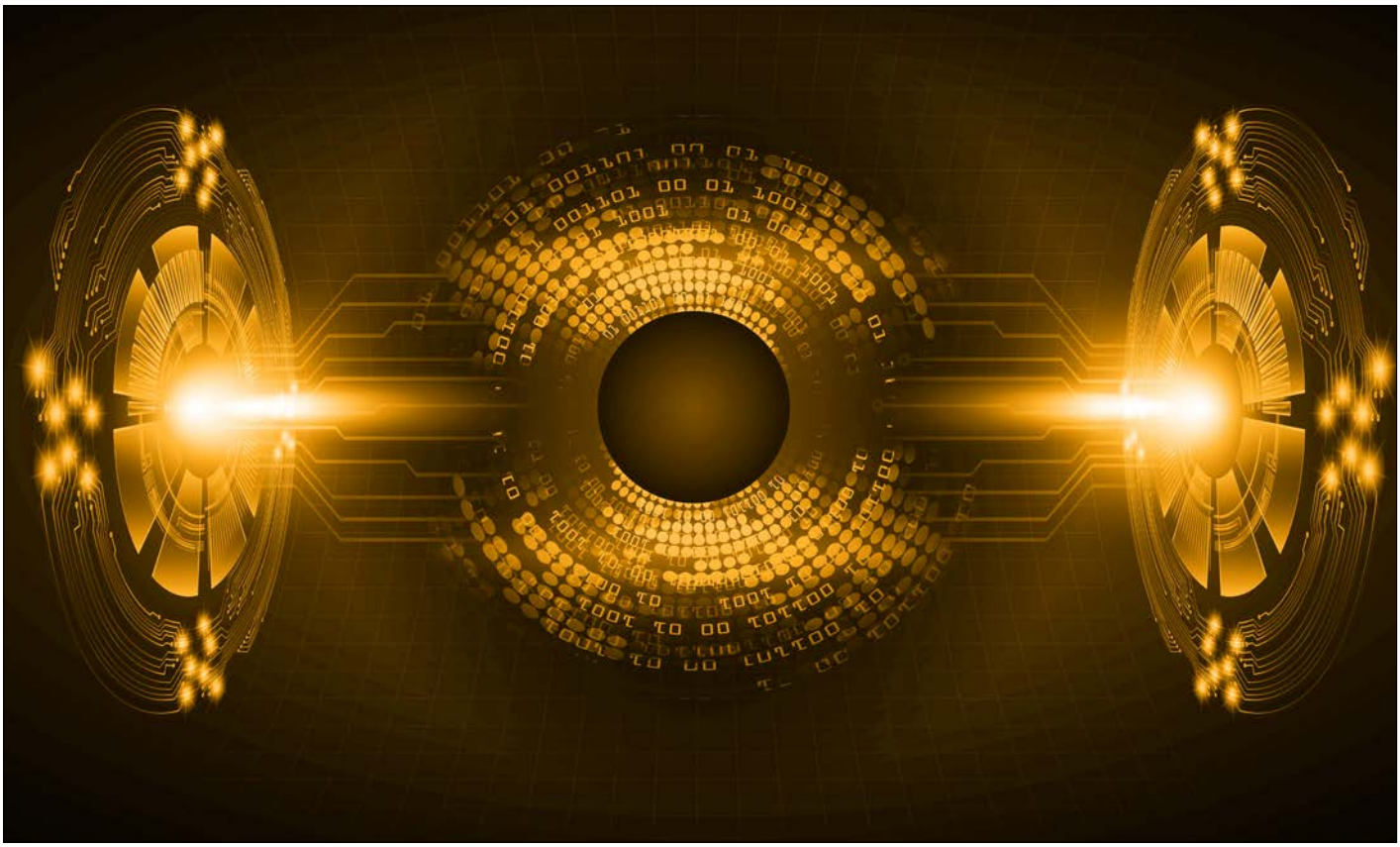
Другая причина — недостаточная осведомлённость руководителей банковских и финансовых организаций о возможностях и преимуществах данного класса устройств ввиду их относительно недавнего появления на рынке, в сравнении с другими СЗИ, призванными обеспечивать защиту периметра. Следствием этого являются часто необоснованные предположения о том, что внедрение СЗИ класса «диод» связано с необходимостью серьёзных инвестиций и реорганизации всей существующей сетевой инфраструктуры предприятия. Отчасти указанные задачи действительно возникают перед блоками ИБ и ИТ в процессе внедрения, но совсем не в том объёме, который пытаются представить в качестве обоснования отказа от применения «диодов».

Причина 3:
неосведомлённость на местах

Наконец, ещё одна причина отказа от применения устройств класса «диод» — отсутствие на местах чёткого описания процесса обмена данными между сегментами сетей с разными уровнями доверия. То есть, когда обмен данными организуется по принципу открытия (разрешения) соединений и протоколов на уровне L3-L7 модели OSI, с одновременным обоснованием, что «по-другому это работать не будет, требуется постоянный двусторонний обмен информацией с внешней сетью и устройства класса „диод“ в такой схеме применяться не могут». Как и в предыдущем случае, для части интеграционных обменов такие заключения справедливы, но в значительном количестве сценариев сам факт наличия закрытой сети означает минимизацию обращений к ней по какому-то внешнему каналу связи и прямо указывает на возможность применения «диодов».

СИТУАЦИЯ ПО ОТРАСЛЯМ

Указанные выше причины приводят к тому, что на сегодняшний день устройства класса «диод» недооценены в банковском и финансовом секторах. Однако их широкое при-



менение в данной сфере — это лишь вопрос времени. Схожая ситуация ранее наблюдалась в области обеспечения безопасности объектов в сфере промышленности, энергетики, добычи. Однако сейчас устройства класса «диод» — один из ключевых факторов обеспечения безопасности значимых объектов КИИ в различных регионах страны и в различных отраслях.

При этом направлений применения устройств класса «диод» в банковском и финансовом секторе может быть даже больше, чем в других сферах, так как здесь объединяются сразу несколько ключевых областей, среди которых может быть защита КИИ, защита персональных данных, защищённое взаимодействие с центрами SOC и др.

СЦЕНАРИИ ПРИМЕНЕНИЯ

Для обеспечения безопасности предприятий финансового сектора возможно множество сценариев применения устройств класса «диод». В качестве основных (но не ограничиваясь ими) можно выделить следующие:

1. Обеспечение регулярного резервного копирования ключевой информации, ВМ, ресурсов из сети банка в защищённое хранилище;
2. Обеспечение обезличенных выгрузок данных для использования внешними подразделениями банка и другими организациями (разработчики, аналитики), без возможности получения доступа к защищённой сети банка;
3. Обеспечение передачи образов виртуальных машин и ПО, подозрительных файлов из сети организации в лабораторию информационной безопасности SOC или стороннего подрядчика;
4. Обеспечение передачи оповещений о киберугрозах из защищаемого сетевого сегмента организации в иные сетевые сегменты для решения задач обнаружения вторжений.

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

Для нормального функционирования бизнес-процессов банковский и финансовый сектор, в свою очередь, предъявляет ряд технических требований, которым устройства класса «диод» должны соответствовать. К таким требованиям относятся высокая пропускная способность канала передачи, продвинутая функциональность в части настройки схем передачи данных, а также совместимость устройств с соответствующей ИТ-инфраструктурой прикладного уровня организации, например, такой как АБС (автоматизированная банковская система), интеграционные шины, контакт-центры.

* * *

Несмотря на все перечисленные выше причины пока ещё ограниченного применения устройств класса «диод», крупные банковские и финансовые организации уже обратили внимание на данную технологию сетевой защиты периметра. В частности, решения InfoDiode уже не первый год используются в наиболее крупных финансовых организациях страны. Текущие тенденции организации защиты ключевой инфраструктуры и сетей банков говорят о том, что рост спроса на устройства класса «диод» в этом секторе остаётся лишь вопросом времени.

ЗАЧЕМ МФО ЗАЩИЩЁННЫЙ САЙТ

И С КАКИМИ АКТУАЛЬНЫМИ РИСКАМИ ПРЕДСТОИТ СПРАВЛЯТЬСЯ

Артём СЕМЁНОВ
менеджер по развитию бизнеса, NGENIX

По данным Центробанка, в 2023 году микрофинансовые организации (МФО) выдали заёмщикам более 1 триллиона рублей. Согласно статистике, дистанционные каналы обслуживания — самый предпочтительный метод получения займов. В 2023 году доля онлайн-займов выросла до 75%. В 60% случаев всё взаимодействие клиента и МФО осуществляется через сайт или приложение.

Это означает, что веб-сайт — ключевой инструмент для успешного функционирования микрофинансовой организации и её конкурентоспособности.

КАКИМ ДОЛЖЕН БЫТЬ ЭФФЕКТИВНЫЙ И КОНКУРЕНТОСПОСОБНЫЙ ВЕБ-РЕСУРС МФО?

Во-первых, веб-ресурс должен быть быстрым. Потребители микрофинансовых продуктов нередко оказываются в обстоятельствах, которые требуют быстрого решения. Если приложение работает медленно, МФО столкнётся с повышенным оттоком пользователей: потенциальные клиенты уйдут к конкурентам. Медленная загрузка веб-страниц вкупе с ростом трафика отказов негативно влияет на позиции в поисковой выдаче и значительно снижает видимость МФО в публичном инфопространстве.

Во-вторых, веб-ресурс должен быть устойчив к высоким нагрузкам легитимного и/или нелегитимного трафика. Сезонные события могут повлечь наплыв заёмщиков и рост легитимной нагрузки. Если приложение не выдержит её, клиенты уйдут к конкурентам. Высокий уровень нелегитимной нагрузки генерируют мощные DDoS-атаки, и потеря доступности сайта или приложения из-за DDoS-атаки также может мотивировать пользователей выбрать конкурента.

В-третьих, веб-ресурс должен быть надёжно защищён от взлома извне. Последствия взлома, дефейса сайта или утечки персональных данных могут спровоцировать реальные денежные убытки и потерю потенциальной выручки.

КАКОВЫ РИСКИ КИБЕРБЕЗОПАСНОСТИ ДЛЯ МФО?

Финансовые веб-ресурсы и приложения постоянно находятся под угрозой: киберинциденты в кредитно-финансовом секторе, по данным Solar JSOC, в 2023 году составили 20% от общего выявленного числа инцидентов.

Риски ИБ для МФО разнообразны.

- Репутационные риски: негативные отзывы приводят к оттоку, а публичное освещение инцидентов создаёт негативный образ и МФО, и всей отрасли.
- Юридические риски: проверки по итогам инцидентов приводят к штрафам и судебным издержкам.
- Операционные риски: потеря критической информации может привести к частичной или полной остановке бизнес-процессов, а остановка деятельности — к убыткам.
- Стратегические риски: при выявлении серьёзных нарушений Банк России может приостановить деятельность микрофинансового института. При рецидивах — исключить организацию из государственного реестра.

То есть от того, насколько веб-ресурсы МФО способны выдержать растущий уровень угроз, может напрямую зависеть её прибыльность и в целом сама возможность организации вести коммерческую деятельность.

С КАКИМИ УГРОЗАМИ БЕЗОПАСНОСТИ СТАЛКИВАЮТСЯ СОВРЕМЕННЫЕ ВЕБ-РЕСУРСЫ?

Одна из наиболее серьёзных угроз — DDoS-атаки. По нашим оценкам, организации сегмента МФО зачастую ограничиваются встроенными средствами защиты от DDoS на уровне канала связи от регистратора доменных имён или оператора связи. Это не спасает от сложных атак на уровень приложений.

Всё больше неприятностей доставляют нежелательные боты — автоматизированный низкочастотный трафик, проходящий ниже традиционных радаров средств защиты. Их цель — это веб-ресурсы, которые имеют сложную логику, например, предполагают механизм аутентификации. Управляющая сложным ботом команда способна быстро адаптироваться и избегать обнаружения. Ущерб может быть ощутимым: из-за роста паразитной нагрузки (до 50% от общего трафика) растут расходы на инфраструктуру. Такое явление, как SMS-бомбинг, при котором запрашиваются коды подтверждения на несуществующие номера, может приводить к миллионным тратам ежемесячно. Также боты могут использоваться для поиска уязвимостей, подбора паролей к учётным записям.

С эксплуатацией уязвимостей, взломов и последующей утечки данных связано более трети всех киберинцидентов в финсекторе, они имеют серьёзные последствия для всей организации в части регуляторных рисков, а с принятием «закона об оборотных штрафах» возрастут и прямые убытки. Для отражения таких атак требуются специализированные решения, а настройка и управление ими осуществляются высококвалифицированными ИБ-специалистами.

КАК РЕШИТЬ ПРОБЛЕМУ ЗАЩИТЫ ВЕБ-РЕСУРСА, НЕ НАНИМАЯ ИБ-СПЕЦИАЛИСТОВ?

Команды веб-ресурсов МФО сталкиваются практически с теми же угрозами, что и популярные ecommerce-игроки, и онлайн-присутствие в такой же мере влияет на прибыльность и жизнеспособность бизнеса. Если сравнить спектр вызовов МФО с банками, то первые намного более чувствительны к оттоку клиентов, чем банки, но при этом несут сопоставимые регуляторные риски.

При этом команды микрофинансовых организаций особенно остро ощущают дефицит кадров ИБ и имеют меньше ресурсов для привлечения и удержания специалистов по ИБ, зачастую ограничиваясь только специалистами по оценке рисков для выполнения регуляторных требований, которые не могут иметь настолько всеобъемлющего экспертного опыта в ИБ, чтобы выбирать, внедрять, настраивать и поддерживать сложные СЗИ.

Облачные сервисы защиты могут решить насущную для команд МФО проблему без необходимости иметь ИБ-специалиста в штате. На то есть несколько причин.

Высокая ёмкость

Облачный провайдер способен предоставить эластичную веб-инфраструктуру, способную принять любую легитимную и нелегитимную нагрузку. Это защитит веб-ресурс как от мощных DDoS-атак более 1 Тбит/с, так и от непрогнозируемых наплывов легитимных пользователей.

Если сравнить спектр вызовов МФО с банками, то первые намного более чувствительны к оттоку клиентов, чем банки, но при этом несут сопоставимые регуляторные риски

Встроенные комплексы защиты от кибератак

Внутри облачной платформы уже интегрированы необходимые сервисы защиты, например антибот- и AntiDDoS-системы, ПО для защиты от взлома. Отсекая нелегитимный трафик на различных эшелонах защиты, они снижают нагрузку на инфраструктуру заказчика. Работу разных СЗИ можно контролировать в режиме единого окна, не нанимая отдельные специализированные команды.

Управляемость и прозрачность

Чтобы всегда иметь полное представление о том, как чувствует себя веб-ресурс, доступна наглядная аналитика в режиме реального времени, что позволяет быстро принимать правильные решения.

Компетенции

В команде провайдера накапливается обширный экспертный опыт на основе множества кейсов с различными клиентами. Его крайне трудно и дорого собрать в рамках собственной ИТ-команды. Настроив эффективное и открытое взаимодействие с командой провайдера, можно профессионально решать задачи защиты, не имея ИБ-компетенций в штате.

ЧТО НУЖНО СДЕЛАТЬ, ЧТОБЫ НАЧАТЬ ПОЛЬЗОВАТЬСЯ ОБЛАКОМ ДЛЯ ЗАЩИТЫ ВЕБ-РЕСУРСОВ?

Итак, вы решились выбрать облачного провайдера для защиты своего веб-приложения. Что необходимо сделать, чтобы наиболее эффективно использовать облачные СЗИ?

1. Знайте свой трафик

Несмотря на то что облачные СЗИ работают в автоматическом режиме, нужно понимать свой реальный трафик. Чтобы СЗИ правильно обучились отражать атаки или блокировать нелегитимные запросы без ложнопозитивных срабатываний, провайдер должен знать, что является аномалией, а что нет, — а это может подсказать только заказчик.

2. Обсудите сферу ответственности провайдера «на берегу»

Немногие заказчики, по нашему опыту, перед подписанием договора внимательно изучают положения SLA и понимают уровень ответственности провайдера, а это очень важно. Нужно оценить уровень технических компетенций команды, которая будет взаимодействовать с провайдером. Из этого станет понятно, стоит ли дополнительно привлекать экспертов контрагента для решения дополнительных задач (например, настройки WAF).

3. Архитектурно разделите приложение

Необходимо найти баланс между требованиями регуляторов в части хранения персональных данных и обширными возможностями публичного облака. Лучшая практика — архитектурно разделить приложение таким образом, чтобы его публичная часть, которая зачастую является высоконагруженной, защищалась облачным провайдером, а критичные данные хранились и защищались внутри собственной on-premise-инфраструктуры. Монолитный легаси-код — это основная проблема при интеграции с облаком.

ЗАЧЕМ ТРАТИТЬ НА ЧТО-ТО ПОЛЧАСА?

ЕСЛИ МОЖНО АВТОМАТИЗИРОВАТЬ ЗА НЕДЕЛЮ...

Артём МЕДВЕДЕВ
генеральный директор ООО «ИНТЕЛПРО»

Владимир БОНДАРЕВ
технический директор ООО «ИНТЕЛПРО»

Валерий ГОРБАЧЁВ
руководитель группы внедрения систем мониторинга АО «ДиалогНаука»

ПРИНЦИП ДРУКЕРА

Намного легче управлять тем, что можно измерить. Количественные показатели играют важную роль в управлении и улучшении бизнес-процессов или любой организационной функции. Если не измерять результаты, может быть сложно эффективно оценивать стратегии и действия. Например, невозможно снизить вес, не измеряя его.

Эту идею упоминал Питер Друкер, известный как изобретатель теории современного управления бизнесом. По мнению Питера Друкера, без чётко установленных метрик успеха невозможно определить, насколько успешно идёт бизнес. Нельзя количественно оценить прогресс и скорректировать процесс для достижения желаемого результата.

Генеральный директор ООО «Интел Про» Артём Медведев считает, что, измеряя результаты, можно эффективно оценивать стратегии и действия. Это помогает выявить области для улучшения и принять правильные решения, основываясь на реальных данных, а не только на догадках. Постоянный мониторинг эффективности процессов помогает менеджерам и руководителям принимать более точные управленческие решения. Без анализа данных решения принимаются интуитивно или экспертно и могут привести к ошибкам, иногда к существенным.

О ВАЖНОСТИ МЕТРИК И ПОКАЗАТЕЛЕЙ

Мониторинг метрик и показателей эффективности бизнеса важен по следующим причинам.

- Получение информации. Метрики дают возможность уверенно судить об эффективности и сделать выводы о том, правильно ли организована текущая работа компании, а также в каких направлениях могут понадобиться корректировки.
- Выявление областей совершенствования. Отслеживая и изучая метрики эффективности бизнеса, компании могут определить, на каких участках возникают наибольшие трудности в процессе работы или существует необходимость в увеличении ресурсов.
- Постановка реалистичных целей. Путём исследования метрик за прошлые периоды можно прийти к заключению, какие целевые значения показателей являются оптимальными, а также на какую эффективность стоит рассчитывать.
- Более эффективное распределение ресурсов. Контролируя с использованием метрик эффективность работы подразделений или проектов, компании могут выяснить, куда следует в первую очередь направлять трудовые и денежные ресурсы, чтобы обеспечить наилучший результат.
- Мониторинг хода реализации стратегий и инициатив. Бизнес-метрики проекта позволяют получить наглядную картину реализации намеченных планов и соответствия достигнутых показателей контрольным значениям.
- Оптимизация производительности. Использование метрик предоставляет убедительные аргументы при принятии решений, за счёт чего наблюдается рост производительности.

Для визуализации метрик и показателей эффективности удобно использовать дашборды (рис. 1) — интерактивные аналитические панели, где на одном экране расположены все ключевые метрики, показатели цели или

Без чётко установленных метрик успеха невозможно определить, насколько успешно идёт бизнес. Нельзя количественно оценить прогресс и скорректировать процесс для достижения желаемого результата

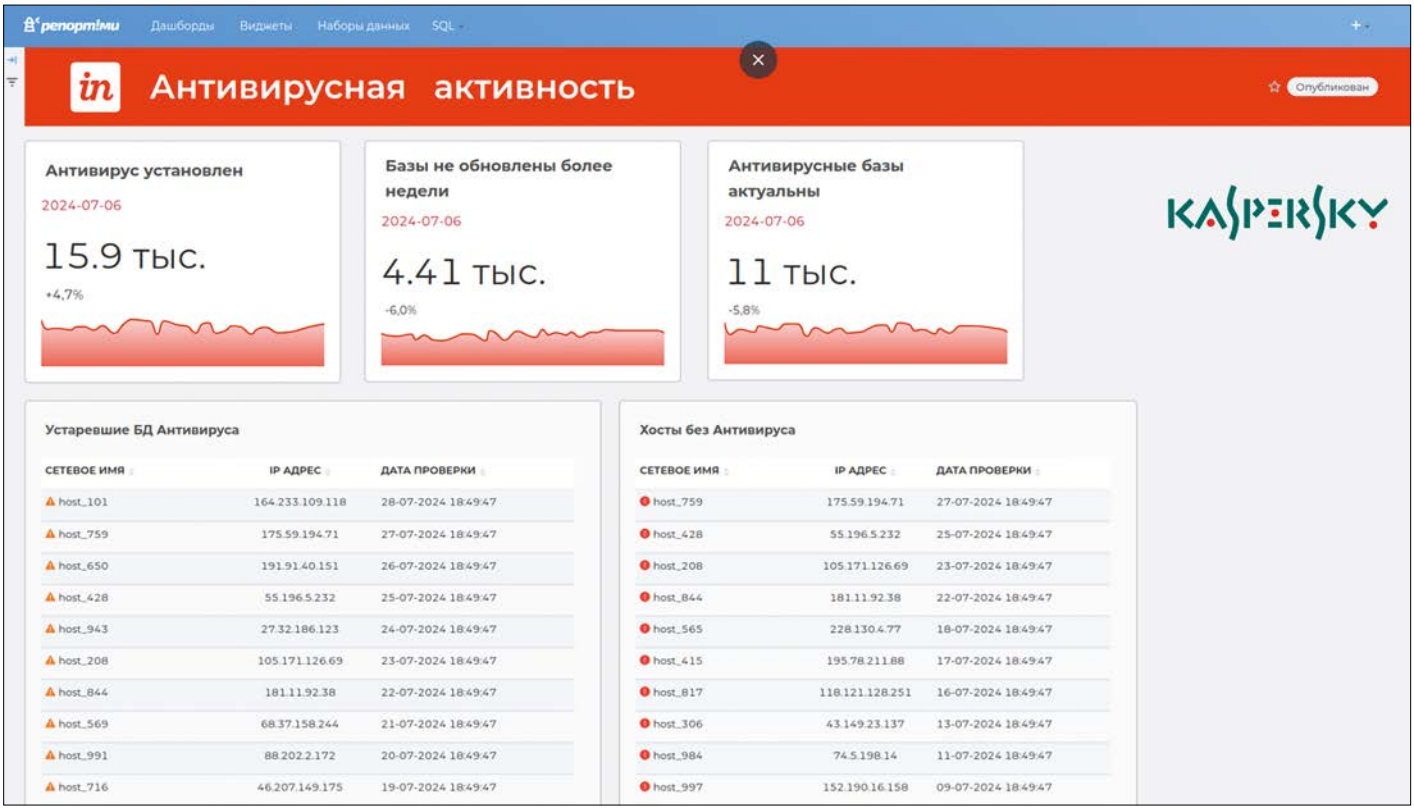


Рисунок 1. Дашборд антивирусной активности от «Репорт! Ми»

процессов. Оптимальным будет сочетание объективных и субъективных метрик и параметров. Первые основаны на конкретных числовых измерениях, вторые — на личной оценке руководителя.

Основные виды дашбордов:

1) операционный: отображает текущие операционные изменения данных в бизнесе;

2) аналитический: помогает исследовать тенденции и делать выводы. Обычно их используют для конкретного бизнес-подразделения;

3) стратегический: нужен, чтобы составить представление о ситуации в целом или об отдельных показателях, выявляет проблемы и помогает их исправлять.

НАСТРОЙКА И СИНЕРГИЯ

Задачи формирования дашбордов и отчётов в крупных компаниях тесно пересекаются, данные из дашбордов перетекают в отчёты и наоборот. При этом по-прежнему подготовка отчётов зачастую выполняется вручную и может быть автоматизирована.

Одним из вариантов решения для визуализации метрик и показателей эффективности бизнеса является использование платформы «Репорт! Ми» и «Коллект! Ми».

Технический директор ООО «Интел-Про» Владимир Бондарев отмечает ряд полезных и уникальных функций платформы для автоматизации микропроцессов:

◆ Сбор разнородных данных и хранение с помощью «Коллект! Ми» (рис. 2):

- штатные коннекторы ко всем наиболее используемым источникам и возможность подключения нетиповых источников данных;
- возможность инкрементного сбора данных и данных реального времени;
- гибкие настройки сбора данных по расписанию и условиям;
- первичная обработка данных, фильтрация, нормализация и агрегация, возможности обогащения, использование регулярных выражений;
- уникальный механизм схем сбора данных для формирования заданий без привлечения высококвалифицированных специалистов;
- хранение метрик в отдельной СУБД в контуре пользователя.

◆ Аналитика и визуализация метрик с помощью «Репорт! Ми»:

- поддержка всех типов дашбордов, в том числе статических отчётов и онлайн-дашбордов для отображения данных реального времени;
- уникальный визуальный конструктор виджетов с интуитивно понятными настройками позволяет пользователю самостоятельно формировать дизайнерское отображение данных;
- возможность построения многопараметрических виджетов;
- полный контроль над формированием дашборда за счёт визуального конструктора дашбордов. Множество настроек: параметры холста, фон, стили, вспомогательные линии и т.д.;
- поддержка концепции Pixel Perfect для наилучших результатов;
- гибкие механизмы для решения нестандартных задач: механизм вычисляемых колонок, механизм шаблонирования, механизм виртуальных данных;
- и др.

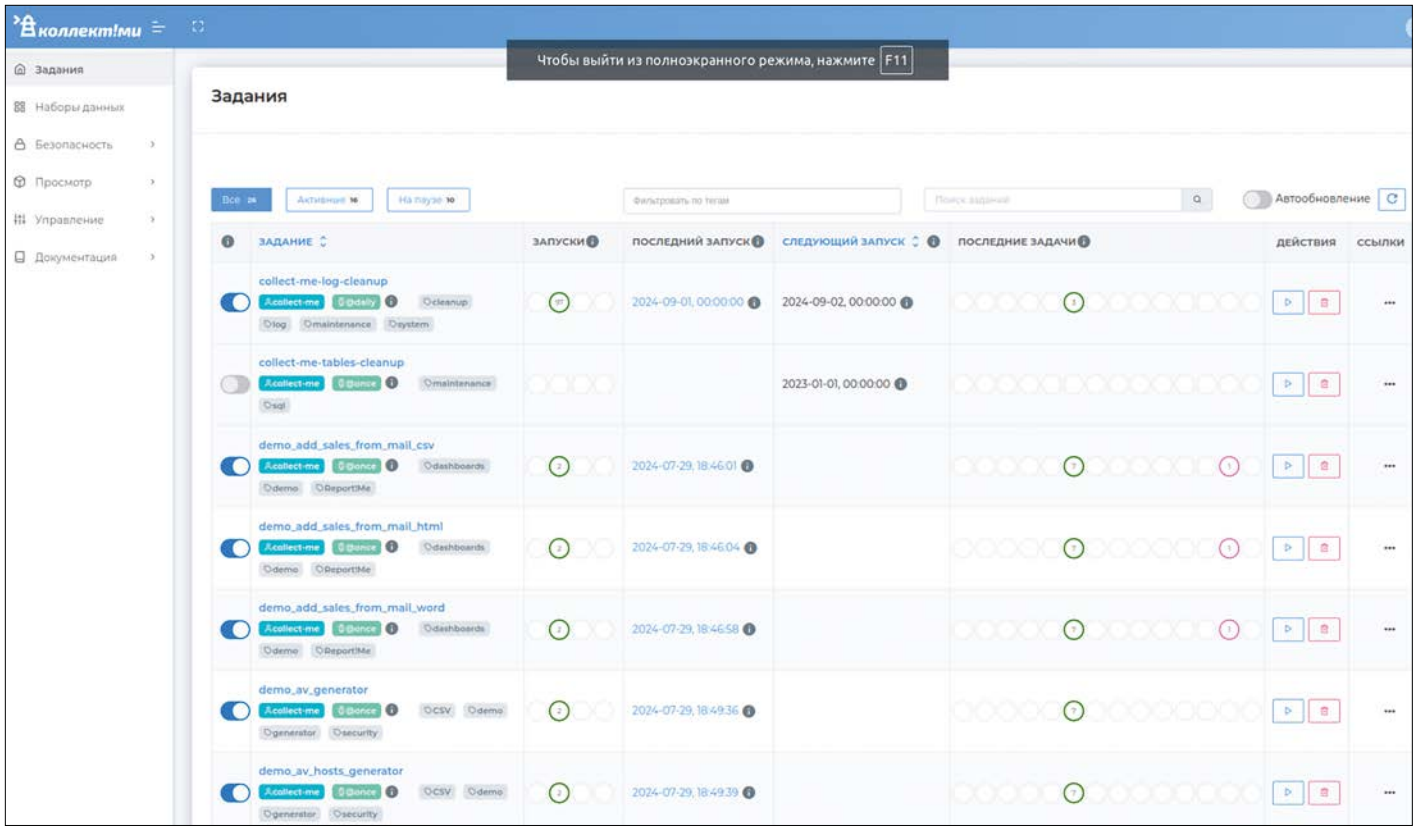


Рисунок 2. Примеры заданий «Коллект! Ми»

Платформа обладает широким рядом возможностей, таких как интеграция с 1С, аналитика финансовых данных, мониторинг транзакций и платежей, использование дополненной реальности (AR), повышенный уровень безопасности за счёт применения QR-меток и т.п.

КАК ПОМОЧЬ БИЗНЕСУ С ПРОЦЕССОМ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Задачи бизнес-аналитики и автоматизации микропроцессов, помимо инструмента (платформы) автоматизации, предусматривают комплекс работ по цифровой трансформации компании для анализа и подготовки процессов к автоматизации. Конечная цель этих работ — получение оперативной достоверной информации для принятия управленческих решений.

С этими задачами своим клиентам помогает справиться компания «ДиалогНаука», используя комплексный подход и выполняя оптимизацию процессов в компании при цифровой трансформации.

В рамках проекта по цифровой трансформации проводится аудит процессов, определяются ключевые метрики эффективности, целевые процессы разбиваются на атомарные сегменты деятельности и автоматизируются частные случаи деятельности сотрудников, максимально исключая ручной сбор и обработку данных.

Следующим шагом формируется и настраивается система, которая позволяет собирать данные из разнородных источников, таких как файлы, таблицы, базы данных и электронная почта. Из собранных данных целевые значения метрик забираются и хранятся во внутренней базе, позволяя оперативно создавать отчёты и панели визуализации с максимальной скоростью и надёжностью.

Автоматизируется процесс регулярной отчётности деятельности департамента. Настраивается автоматическая сборка данных для генерации еженедельных отчётных презентаций на оперативных планёрках у руководства департамента, ежегодные отчёты для правления. Также формируются и настраиваются панели визуализации для Центра мониторинга. Скорость подготовки еженедельных отчётов сокращается с дней до часов.

Также у компании «ИНТЕЛПРО» есть хорошая команда специалистов по инфографике, которые могут помочь с построением эффективного и понятного дашборда, основываясь на лучших практиках. Панели визуализаций созданы и оптимизированы в едином цифровом стиле заказчика, с учётом средств вывода информации, а также персоналий потребителя данных, с использованием самых эффективных методов создания инфографики.

ПОСЛЕСЛОВИЕ

Объединяя вместе вышеописанные шаги, в итоге вы получите автоматизированный достоверный источник информации, работающий в реальном времени и позволяющий принимать грамотные управленческие решения на основе данных аналитики и метрик по деятельности компании, что позволит снизить риски и повысить эффективность ведения бизнеса.

БЕЛГОРОДСКИЙ ОПЫТ ЦЕНТРА ГОССОПКА

Сергей ЩЕКИН
генеральный директор, компания БелИнфоНалог

Компания «БелИнфоНалог» является корпоративным центром ГосСОПКА класса «А» и оказывает субъектам критической информационной инфраструктуры услуги по выполнению требований Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

— Сергей Васильевич, как давно компания «БелИнфоНалог» стала корпоративным центром ГосСОПКА?

— Мы завершили все процедуры по согласованию и получили лицензию в 2023 году.

— Были ли сложности с регистрацией компании как центра ГосСОПКА? Ведь для получения статуса требуются лицензии ФСБ и ФСТЭК России, необходима разработка документации и согласование её с регуляторами, а ваша организация сравнительно небольшая?

— Да. Компания действительно небольшая, около 50 человек. Но при этом у нас в штате порядка 20 специалистов, имеющих образование в области информационной безопасности. Мы были готовы, что процесс получения лицензии займёт не один месяц. Но в целом процедура регламентирована, все требования изложены достаточно точно и однозначно.

— Откуда к вам приходят компании? Часто организации не знают, что относятся к субъектам КИИ. Что вы делаете в этом случае?

— Основной пул заказчиков приходит к нам из госсектора: сказывается работа профильных федеральных и региональных органов власти, регуляторов. Некоторые компании обращаются к нам самостоятельно. Они трезво оценивают свои возможности и хотят воспользоваться услугами профессионалов для категорирования объектов КИИ и обеспечения их безопасности, подключения к ГосСОПКА.

Также мы работаем со старыми клиентами и проводим разъяснительную работу о необходимости соблюдения требований законодательства в области обеспечения безопасности объектов КИИ и подключения к ГосСОПКА. Порой ведём длительный диалог с компаниями и в итоге находим правильное решение.

— Как построена работа вашего центра ГосСОПКА?

— Компания «БелИнфоНалог» оказывает услуги по выполнению требований 187-ФЗ в полном объёме. Мы берём на себя подготовку организационной документации для создания комиссии по категорированию, определяем объекты КИИ (ИС, ИТКС, АСУ), проводим категорирование, которое включает определение перечня процессов на предприятии и выявление критических для дальнейшего рассмотрения комиссии. Также мы проводим анализ угроз безопасности и принятых мер по обеспечению кибербезопасности объекта, оцениваем возможные последствия инцидентов. По итогам процесса наша компания готовит пакет документов для определения категории значимости или отсутствия КИИ и отчёт о результатах категорирования для отправки во ФСТЭК России.

Но самым трудозатратным этапом является создание комплексной системы защиты, начиная от моделирования угроз безопасности, проектирования подсистемы безопасности до устранения всех уязвимостей и ввода в эксплуатацию системы защиты информации.

Мы предлагаем своим клиентам полный спектр услуг по мониторингу и реагированию на компьютерные инциденты, в том числе на объектах КИИ.

— Хватает ли вам специалистов и как вы решаете кадровые проблемы с учётом требований регуляторов к штатному расписанию и квалификации сотрудников?

— В УЦ «Белинфоналог» работают высококвалифицированные специалисты, которые регулярно проходят переобучение и готовы противостоять кибератакам. Конечно, найти людей с опытом сложно, и мы всегда готовы взять в команду новых толковых сотрудников, которые хотят расти и развиваться вместе с компанией.

— Изменилось ли что-то в работе компании после того, как она стала корпоративным центром ГосСОПКА?

— Как и любая компания, работающая в сфере кибербезопасности, мы постоянно подвергаемся атакам на нашу инфраструктуру. Однако и в рамках текущей работы, и при получении статуса центра ГосСОПКА класса «А» мы проводим работу по укреплению внутренней инфраструктуры компании — без этого невозможно лицензирование деятельности у регуляторов — и систем заказчиков, поэтому готовы к любым неожиданностям.

БелИнфоНалог

ООО «УЦ «Белинфоналог» создано в 2012 году. Компания предлагает заказчикам широкий спектр услуг в области ИТ, защиты информации и обеспечения защиты КИИ, юридическое сопровождение. Офисы компании открыты в Белгороде и Белгородской области, Москве, Брянске и Симферополе.

Компания «БелИнфоНалог»
belinfonalog.ru
8-800-511-82-81

PKI-ФОРУМ РОССИЯ 2024

ПЕРВАЯ ПЯТИЛЕТКА ПРОЙДЕНА

Марина БРОДСКАЯ
Оксана ДЯЧЕНКО
специальные корреспонденты
BIS Journal

В Санкт-Петербурге прошла XXII Международная конференция по проблематике инфраструктуры открытых ключей и электронной подписи «PKI-Форум Россия — 2024». Её участники обсудили актуальные вопросы в области PKI и электронной подписи, электронного документооборота, криптографии и информационной безопасности.

ИТОГИ ПЯТИЛЕТКИ

Эксперты Стратегической сессии «Итоги 5 лет реализации самой масштабной реформы 63-ФЗ», которую провёл И. Качалин (АНО НТЦ ЦК), подвели итоги реформы закона «Об электронной подписи», стартовавшей в декабре 2019 г. с принятия поправок в 63-ФЗ.

За пять лет сфера электронной подписи претерпела значительные изменения и динамично развивается, подчеркнул Ю. Шабанов (Минцифры). Он отметил активное развитие сферы электронных цифровых подписей (ЭП), динамику роста архитектуры отрасли и рост числа удостоверяющих центров (УЦ). Помимо органов, аккредитованных по закону (Банк России, Казначейство, ФНС), 43 организации получили аккредитацию как удостоверяющие центры (АУЦ). Ю. Шабанов отметил ключевые элементы реформы, в том числе запреты на выдачу сертификатов юрлиц в коммерческих АУЦ и получение сертификатов по доверенности, возможность использования облачной ЭП только при выполнении ряда требований, разработанных регуляторами, а также выдачу усиленной ЭП в дистанционном формате.

Основные элементы реформы подтвердили её значимость и необходимость развивать ЭП, машиночитаемые доверенности (МЧД) и пр., считает К. Дробаденко (ФСБ России). Однако существует люфт между нормативным регулированием и практической реализацией требований, и задача регуляторов — уменьшить его.

Ф. Новиков (ФНС России) полагает, что реформа не имеет обратного хода, она дала толчок для других изменений, в том числе в рамках трансграничного взаимодействия. Но есть области, в которых необходимо дальнейшее развитие.

Главным показателем реформы стало количество госуслуг, оказываемых населению, и снижение числа мошенничеств в этой сфере, считает В. Бражко (Федеральное казначейство). Он отметил рост числа сервисов и применений PKI, ЭП и МЧД и предложил подвести итоги через пять лет, если новые технологии, включая ИИ, не привнесут что-то своё.

С. Смышляев («КриптоПро») считает реформу логичной с точки зрения нормативной базы и технологий.

Появились новые задачи в области создания технических решений и стандартизации. Многие из них становятся работающими инструментами и технологиями. Люфт между нормами и их реализацией позволяет отладить процессы. «Логика в реформе приземляется на реальные средства и процессы», — отметил С. Смышляев.

Участники сессии выделили вопросы, которые находятся вне правового поля и требуют отдельного решения регуляторов. Найдены промежуточные решения по срокам действия сертификатов и служб времени, учитывающие специфику PKI-технологий и функционирование сервисов в легальном поле. В целом вопрос находится в стадии обсуждения.

МОБИЛЬНАЯ ПОДПИСЬ

Одна из сложных тем в области применения ЭП — мобильная подпись (МП). Найдены пути решения легитимного распространения мобильных приложений для работы с ЭП, методы аутентификации с обеспечением криптографической защиты посредством российских алгоритмов, удобные способы интеграции с информационными системами (ИС), отметили участники профильной сессии.

По мнению С. Смышляева, «мобильная подпись — это всегда про систему, а не про отдельные средства». Он отметил, что средства ЭП мобильных устройств давно сертифицированы, а технологии МП развиваются достаточно быстро, но предстоит решить ещё много задач.

А. Мелузов («РТЛабс») предложил посмотреть на проблему в целом: сама по себе ЭП чаще всего не нужна людям — им нужен результат бизнес-процесса или услуги. Он призвал перейти на электронный документооборот, который даёт экономию ресурсов и ускорение бизнес-процессов, обеспечивает безопасность, скорость и удобство для граждан. 80% пользователей заходят на Госуслуги с мобильных устройств — реализуется концепция mobile first, подчеркнул А. Мелузов. С появлением сертифицированного решения МП ситуация улучшилась. Однако отрасль остаётся сильно кластеризованной, есть замкнутые отраслевые сегменты, где технологии внедряются фрагментарно. Это неудобно пользователям и мешает цифровизации.

МЧД

Вопросы машиночитаемых доверенностей и подтверждения полномочий обсуждались на разных площадках Форума. Не все организации готовы использовать универсальный формат МЧД, и задача регуляторов — вынудить всех перейти на единую форму МЧД, для чего необходимо внести изменения в 63-ФЗ и установить сроки перехода, составить классификатор полномочий, полагают эксперты. Ужесточение требований по использованию МЧД для тех сегментов, которые готовы перейти на новые технологии, позволит активнее развивать инструмент. В итоге он будет принят бизнесом и гражданами, считает В. Бражко, но доработка ИС по правилам, которые сильно размыты, — тяжёлая и инвестиционно непривлекательная задача.

Ю. Шабанов считает, что для поиска общего решения необходим диалог ведомств и бизнеса. Минцифры не готов вводить нормативное регулирование, поскольку последствия могут быть непредсказуемыми.

СЕРТИФИКАТЫ ФИЗИЧЕСКИХ ЛИЦ

Массовый переход на сертификаты физических лиц дал положительный эффект, но и создал новые риски. По мнению экспертов, сертификат физлица означает, что человек должен его беречь в паре с МЧД и ЭП. При этом возникают новые задачи, связанные с повышением осведомлённости граждан и технической подстраховкой пользователя. Переход на регулярное использование сертификатов и ЭП требует обновления части инструментария, усиления защиты и повышения грамотности граждан.

ЗАКОНОТВОРЧЕСТВО

Вопросы законотворчества широко обсуждались на PKI-Форуме. В частности, в закон 63-ФЗ «Об электронной подписи» будет внесена норма, касающаяся сертификатов органов власти, не являющихся налоговыми агентами. Появится новый тип сертификатов для госструктур, взаимодействующих друг с другом. Сегодня такие организации получают сертификаты в УЦ Казначейства, который и ведёт реестр.

В завершающей стадии готовности находится законопроект о национальном удостоверяющем центре, который призван легализовать сертификаты безопасности, подписей кода на основе ГОСТ. Этот законопроект станет продолжением PKI-реформы.

Продолжается работа над законопроектом по архивному хранению электронных документов с ЭП, он был принят в первом чтении в апреле 2022 г. На сегодня почти все спорные вопросы сняты, отметил

В. Волошин (Минэкономразвития), и есть надежда, что документ будет принят во втором чтении до конца текущего года.

КРИПТОГРАФИЯ

Широкое применение сертифицированных средств криптозащиты информации (СКЗИ) — задел для массовой криптографии в рамках использования ЭП физлицами, считает С. Смышляев. Рассматриваются подходы, которые позволят мобильным приложениям с СКЗИ существовать и развиваться, не противореча требованиям регуляторов. К. Дробаденко подчеркнул, что массовое применение СКЗИ — задача государственного суверенитета РФ. Ведётся работа с лицензиатами ФСБ, продукты востребованы, отметил он. Массовое проникновение СКЗИ должно происходить в составе предустановленных на устройства отечественных ОС и браузеров с российской криптографией, что облегчит массовому пользователю взаимодействие с органами власти и между собой. Этот вопрос требует нормативного регулирования.

СИСТЕМНЫЙ ПОДХОД

Тема криптографии была продолжена на сессии «Системный подход в отрасли PKI: регулирование, комплексное использование, перспективные разработки». Об изменениях нормативной базы в области разработки и эксплуатации СКЗИ рассказала А. Толстолуцкая (ФСБ России). Она отметила нововведения Приказа ФСБ России № 50, вступившего в силу 1 сентября 2024 г., призванные повысить уровень защищённости и унифицировать использование ЭП, уточнить требования к форме квалифицированного сертификата ключа проверки ЭП и требования к МЧД.

Спикер остановилась на доверенных микросхемах, которые прошли экспертизу на соответствие требованиям к СКЗИ для регистрации информации, не содержащей гостайну. Такие устройства обеспечивают дополнительную защиту при извлечении ключа, их взлом достаточно дорог, а себестоимость относительно низка, что позволяет широко применять микросхемы. В будущем планируется увеличить срок действия ключей от 5 до 7 лет или до истечения срока службы изделия, в зависимости от итогов экспертизы, назначения и конкретного исполнения.

НОВЫЕ ТРЕБОВАНИЯ ФСТЭК

С. Груздев («Аладдин Р.Д.») посвятил доклад новым требованиям ФСТЭК России к защите государственных информационных систем (ГИС), обеспечению доверия в ИС и ИТ-инфраструктуре, которые придут на смену Приказу № 17 ведомства. Эти меры обязательны для исполнения, отметил докладчик. Проект документа находится в стадии обсуждения, рабочей группой ведётся подготовка методических рекомендаций по реализации требований приказа. Планируется, что документ вступит в силу через год после принятия, а требования, касающиеся вопросов PKI в ГИС, начнут действовать через два года.

Важный вопрос — доверие к ИС, которое строится от оборудования, подчеркнул спикер. ГИС рассматривает комплексную инфраструктуру, учитывающую всех участников процесса: ИТ-инфраструктуру, ПО, пользователей всех рангов. Для обеспечения высокого уровня доверия необходима строгая аутентификация с использованием аппаратных СКЗИ и отказ от паролей. Докладчик также пояснил нюансы работы PKI в открытых и закрытых ИС, затронул вопросы подписи кода.

Подходы к обеспечению дополнительных свойств ЭП описал И. Герасимов («НПК «Криптонит»). Он пояснил, что требования к свойствам ЭП по ГОСТ 34.10 «Процессы формирования и проверки электронной цифровой подписи» могут не выполняться по ряду причин при использовании ЭП в рамках ИС. При этом появляются дополнительные атрибуты, которые требуют дальнейших исследований, а также проработки нормативной базы и стандартов.

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Вопросы обеспечения идентификации и сертификатов безопасности в рамках деятельности НТЦ ЦК поднял Андрей Пьянченко (АНО «НТЦ ЦК»). Спикер выделил области, требующие идентификации, и подробно рассказал о проектах, которые ведёт НТЦ ЦК по каждому направлению.

В части идентификации «Волеизъявление» работают положения 63-ФЗ и ЭП, подтверждающие юридическую значимость решения. Для аутентификации граждан АНО «НТЦ ЦК» ведёт работы по проекту «Адаптер-инфраструктура», в рамках которого разрабатываются сертификаты безопасности и порядок сертификации пользователей, а также сертификаты безопасности для ИС. Итогами реализации проекта станет модернизированный криптографический протокол OpenID Connect 1.0

и создание библиотек для встраивания в различные системы.

В части аутентификации веб-пространства традиционно используются разные подходы, которые не исключают реализацию атаки типа «человек посередине». В рамках проекта «Домен-Протокол» создаются сертификаты безопасности для веб-ресурсов, что включает создание инфраструктуры для выдачи сертификатов безопасности, реализацию криптографического протокола ACME ГОСТ, клиент-серверной архитектуры и сертификатов. Спикер подчеркнул, что отрасли необходим вывод темы сертификатов безопасности в правовое поле РФ, однако пока такого законопроекта нет. НТЦ ЦК создаёт УЦ, который будет выдавать сертификаты на основе протокола ACME.

В рамках проектов «Домен-Протокол» и «Репозиторий-Сертификат» ведётся аутентификация ПО на основе меток доверенного кода (CodeSign, МДК). Итогом работ стало создание инфраструктуры для выдачи МДК и управления жизненным циклом и библиотеки создания и проверки МДК. Это портальные решения, которые позволяют взаимодействовать с пользователями и УЦ для формирования меток.

В части сертификации оборудования на 2025 г. запланированы исследовательские работы по изучению криптопротоколов идентификации устройств.

О ПРОТОКОЛЕ TLS

Об одном подходе к внедрению постквантовых криптографических алгоритмов в протокол TLS рассказал Е. Алексеев (Академия криптографии РФ). Он обосновал необходимость разработки квантовоустойчивой защиты, в частности алгоритмической защиты в постквантовом протоколе TLS. Один из путей защиты — KEM (Key Encapsulation Mechanism), постквантовый защищённый алгоритм шифрования с открытым ключом. Разработка алгоритма ведётся в рамках рабочих групп ТК26 «Криптографическая защита информации». Это долгий процесс, отметил спикер, и чем раньше заработают постквантовые протоколы, тем больше данных удастся защитить. Идут работы и по созданию постквантового протокола TLS. Он должен предъявлять чёткие требования к KEM и обосновать то, что KEM, который будет разработан в будущем, им удовлетворяет.

Докладчик рассказал о разработке KEM в мире и России, поделился опытом внедрения KEM в TLS, рассказал о возможностях новых решений и о проблемах создания отечественного постквантового TLS. В частности, в ходе НИР «Квант-2», проводимых АНО «НТЦ ЦК», ведутся исследования по созданию механизма доказательства знания закрытого ключа для кодового KEM. Механизм долговременного ключа слишком мало исследован, чтобы встраивать его в другие решения. Разработчики протокола выбрали промежуточный вариант кратковременного ключа с ограниченным сроком жизни.

Докладчик подчеркнул, что исследователи впервые разрабатывают протокол, базирующийся на механизме, который разрабатывается другой группой на базе ТК-26. По итогам проведённых работ потребуется полноценный криптографический анализ протокола и формирование требований к механизму KEM, а также прохождение экспертизы ТК26.

* * *

Подробные отчёты обо всех мероприятиях конференции размещены на сайте *https://ib-bank.ru/bisjournal/*

OFFZONE 2024

БЫЛО ИНТЕРЕСНО, ОСОБЕННО ПРО BUG BOUNTY

Марина БРОДСКАЯ
обозреватель BIS Journal

В этом году на пятую международную встречу безопасников, разработчиков, инженеров, исследователей, преподавателей и студентов пришли 4 тыс. человек. Прозвучали 98 докладов в исполнении 124 спикеров. В центре внимания был только технический контент, посвящённый актуальной проблематике кибербеза. Впрочем, всё было далеко не так скучно и сухо. У стен древнего Симонова монастыря, на территории современного Культурного центра ЗиЛ, состоялся большой праздник кибербеза.

ВОСЕМЬ ТРЕКОВ

Летняя жара и дружеский формат общения не располагали к встречам при галстуках и нудным деловым отчётам. Евгений Волошин, директор департамента анализа защищённости и противодействия мошенничеству BI.ZONE и директор OFFZONE2024, в приветственном слове отметил рекордное число участников, спикеров и партнёров. Он выделил восемь тематических треков OFFZONE2024, которые шли параллельно и охватили технические аспекты по всем направлениям кибербезопасности.

На Main track эксперты искали уязвимости в операционных системах и мобильных приложениях, проводили пентесты, обходили системы защиты, обсуждали ключевые тренды и опыт расследования инцидентов в различных средах. Авторы коротких докладов Fast track раскрывали ключевые тренды ИБ, рассказывали об исследовании устройств и делились опытом расследований.

В AppSec.Zone обсуждали безопасность приложений. В новой для OFFZONE Threat.Zone делились практической информацией об актуальных атаках, методах и инструментах злоумышленников. Вопросы социальной инженерии, мошенничества и методы противостояния им прояснялись на AntiFraud.Zone.

Впервые в рамках OFFZONE был выделен трек, посвящённый ИИ. На AI.Zone эксперты говорили о передовых методах прикладного применения ИИ в корпоративной среде и за её пределами, работе с большими языковыми моделями и их совместном использовании в Threat Intelligence или SIEM. Также обсуждались реальные кейсы и проблемы, с которыми приходится сталкиваться при внедрении этих технологий.

CTF track был посвящён формату Capture The Flag. Участники соревнований делились опытом с комьюнити, представители которого могли попробовать силы в решении сложных задач от авторов соревнований CTFZone.

Community track объединил участников сообщества кибербеза. Первый день был посвящён докладам, а второй — рассказам организаторов Community.Zone о решении задач на тематических стендах.

В ходе докладов все участники треков могли задать вопросы спикерам, принять участие в соревнованиях и викторинах и заработать внутреннюю валюту — офкоины. Их активно обменивали на стильный мерч OFFZONE. Заработать валюту можно было и в зоне активностей, где проходили соревнования и квесты на любой вкус и квалификацию.

ДЕЛОВАЯ ПРОГРАММА

Серию докладов открыл Сергей Голованов. В непривычном для него формате главный эксперт «Лаборатории Касперского» рассказал о причинах и эволюции инцидентов кибербезопасности за последние 20 лет, поискал волшебников и йети, обсудил семь смертных грехов и гороскоп безопасника. Так спикер пытался ответить на вопросы об истинных причинах инцидентов, человеческом факторе, злом умысле и мотивах атакующих, а также способах минимизации рисков.

В рамках единственной и не свойственной OFFZONE панельной дискуссии представители различных компаний — F.A.C.C.T., «Лаборатория Касперского», Solar 4RAYS, PT ESC и BI.ZONE — обсудили тренды и изменения локального ландшафта угроз в 2024 г.

БАГБАУНТИ

На традиционной пресс-конференции подвели итоги двух лет работы программы BI.ZONE Bug Bounty. Кратко об итогах:

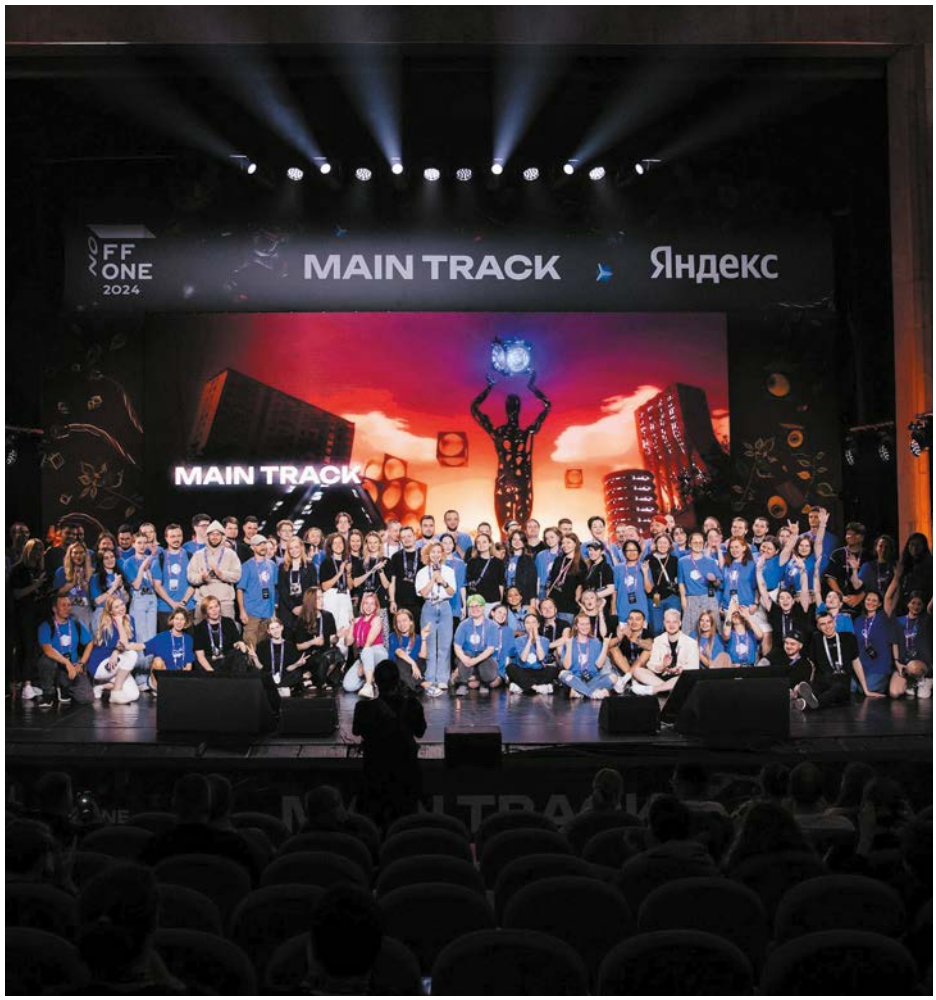
- в 2024 г. в России работают три платформы по поиску уязвимостей за деньги (BugBounty.ru, Standoff 365 Bug Bounty от Positive Technologies и Bi.Zone Bug Bounty), в которых участвуют 29 публичных компаний, запущены 74 публичных программы;
- на платформе BI.ZONE Bug Bounty представлены 34 компании (рост в 2 раза по сравнению с 2023 г.), из них 29 — публичные. Запущены 78 программ по поиску уязвимостей (51 программа в 2023 г.);
- общая сумма выплат багхантерам за два года работы платформы BI.ZONE составила более 60 млн рублей, из них 15 млн выплачено в 2023 г. За минувший год стоимость уязвимостей значительно выросла, поэтому сумма выплат превысила прогнозируемый двукратный рост и составила 45 млн рублей;
- максимальный размер единовременной выплаты — 2,4 млн рублей (за найденную уязвимость на одном из сервисов ВК);
- средний размер выплат на платформе BI.ZONE Bug Bounty составляет порядка 35 тыс. рублей;
- за последний год лидерами российского рынка поиска уязвимостей стали финансовый и государственные секторы, более чем в три раза увеличилось количество компаний из финтеха;

- пять банков из рейтинга топ-10 по версии «Банки.ру» разместили программы на платформе;
- благодаря усилиям Минцифры в шесть раз выросло число программ от госсектора;
- первую в стране программу по поиску уязвимостей в инфраструктуре субъекта РФ — Ленинградской области — запустили в рамках OFFZONE;
- на платформе увеличивается число компаний из ретейла и ИТ-сектора, а также растёт число онлайнсервисов, что связано с высокой скоростью цифровизации и темпами разработки новых решений в этих отраслях, трендом на безопасную разработку, а также оценкой финансовых и репутационных рисков для компаний в случае успешной кибератаки.

Комментируя итоги работы программы, Е. Волошин отметил, что за прошедший год более чем в полтора раза возросло количество отчётов от независимых исследователей. При этом каждая шестая обнаруженная уязвимость относилась к уровню high и critical. За них заплатили в общей сложности 28 млн рублей.

В рамках конференции было объявлено о запуске сразу трёх публичных программ от Сбера, который ранее работал в приватном режиме. Багхантерам предлагается протестировать три сервиса банка: официальный сайт Сбера, «СберИнвестиции» и «СберБанк Онлайн», сообщил С. Крайнов, начальник управления экспертизы киберзащищённости Сбера. Исследователи смогут искать уязвимости мобильных приложений в версиях для iOS и Android, мессенджере онлайн-банка и Сбер ID — сервисе для входа на сайты и приложения Сбера. Багхантеры могут получить вознаграждение до 500 тыс. рублей в зависимости от уровня критичности.

Также к программам Bug Bounty присоединилась «Группа Астра», предоставившая для исследования ОС Astra Linux Special Edition и платформу VMmanager. Это особенно актуально на фоне повышенного интереса к Astra Linux со стороны иностранных государств, отметили участники пресс-конференции.



Отвечая на вопросы журналистов, участники отметили, что:

- вендоры — компании-участники на платформе Bug Bounty — рады широкому участию отечественных и иностранных исследователей уязвимостей и интересу к их продуктам;
- в приватных программах участвует в полтора раза больше вендоров, чем работают в паблике; такая схема является для компаний отработкой всех механизмов работы с программами Bug Bounty перед выходом в публичную сферу;
- отечественные багхантеры не боятся конкуренции со стороны иностранных участников, те часто не понимают специфики российских онлайн-сервисов, есть и языковой барьер; с точки зрения комьюнити это отличный обмен опытом;
- платформа BI.ZONE Bug Bounty работает в официальном формате и не рассматривает иностранных участников через «серые схемы» с использованием криптовалют, но при изменении действующего законодательства платформа будет использовать все возможные способы выплаты вознаграждений;
- для многих иностранных исследователей привлекательны не столько призовые суммы, сколько участие в программах и мерч от российских вендоров.

* * *

Отвечая на вопрос корреспондента BIS Journal об инициативе Минцифры и регуляторов об изменении законодательства и создании реестра «белых» хакеров, Евгений Волошин подчеркнул, что эта информация несанкционированно вышла за пределы профессионального ИБ-сообщества, но интересантом решения является государство. В настоящий момент вопрос находится в стадии обсуждения и о подробностях говорить рано.

АРМИЯ-2024

ТЕХНОЛОГИЧЕСКИЙ СУВЕРЕНИТЕТ РОССИИ: ОТ БПА И ВИДЕОКАМЕР ДО ИИ

Анна КАТАНКИНА
корреспондент BIS Journal

Круглый стол «Обеспечение технологического суверенитета России в сфере безопасности с использованием производственного потенциала российских разработчиков и производителей» прошёл в рамках Международного форума «Армия 2024». Организатором круглого стола выступила компания «Цикада», соорганизаторами — АО «Инфотекс» и НИЦ «Технологии». Участники мероприятия обсудили вопросы физической и информационной безопасности объектов и систем в условиях реализации атак.

ЗАЩИТА ОТ БЕСПИЛОТНЫХ АППАРАТОВ

Первая секция — «Обеспечение защиты и безопасности объектов от БПА» — была посвящена нормативно-правовым аспектам и вопросам противодействия беспилотным аппаратам (воздушным, наземным, подводным и надводным). Главный радиочастотный центр (ГРЧЦ) при Минцифры разработал детальный алгоритм процедуры согласования эксплуатантов и разработчиков таких средств, в том числе устройств электромагнитного подавления. Принята методика подтверждения технических требований к техническим средствам, включая определение недопустимых событий на объекте эксплуатации, средств для атаки и защиты, сообщил О. Пелипас (ТПП России).

Применение любых средств радиоэлектронного подавления требует получения разрешения на использование радиочастотного спектра и регламентируется федеральными законами и иными нормативными актами, уточнил представитель ГРЧЦ Д. Лобанов. Он представил алгоритм подачи заявки на выделение полос радиочастот, регистрации и использования радиочастотного спектра, предназначенного для противодействия БПА, и отметил, что регистрацию устройств в ГРЧЦ рекомендуется проводить силами разработчика. Требования приняты недавно, и регулятор не накопил практического опыта регистрации средств радиоэлектронной борьбы (РЭБ).

Закупку оборудования для РЭБ надо начинать с комплексного подхода — построения модели угроз конкретного объекта, указания взрывоопасных зон и расчёта потенциальных потерь — напомнила Н. Котляр (ГК «Ростех»). На основе модели угроз просчитываются сценарии недопустимых событий, создаётся схема безопасности объекта с учётом требований НПА, строительных возможностей и радиоэлектронной обстановки на предприятии. Поэтапный план внедрения средств радиоэлектронной защиты должен учитывать финансовые возможности и изменения на рынке новых технологий и угроз. Это грамотный подход к вопросам безопасности предприятия без дополнительных затрат, подчеркнула эксперт.

В ОБЛАСТИ ВИДЕОНАБЛЮДЕНИЯ

О проблемах и задачах в области видеонаблюдения говорили на секции «Отечественные разработки в области видеонаблюдения: проблемы и возможности». В. Присяжнюк (НИЦ «Технологии») отметил, что в процессе импортозамещения на рынке систем видеонаблюдения происходит замещение оборудования одних азиатских производителей продукцией из Китая. При этом на Западе идёт массовый отказ от китайского оборудования, в том числе из-за недокументированных возможностей.

Дать оценку систем видеонаблюдения должен 8-й центр ФСБ России, считает спикер. Он отметил устаревшие, но действующие нормативные требования к видеосистемам, которые писались для аналоговых устройств и не учитывают современных требований по ИБ для смарт-устройств. Устаревшие видеосистемы дают доступ злоумышленникам к любым системам организаций.

Важный вопрос — вклад технологий ИИ в системы наблюдения. В ближайшие 5–10 лет принимать решение в вопросах безопасности, в том числе на объектах КИИ, будет всегда живой оператор, а ИИ-системы наблюдения или аналитики будут вспомогательным инструментом, считает В. Присяжнюк.

А. Новиков (АО «Цикада») затронул волнующие интеграторов вопросы использования мультибрендовых решений в рамках одной системы, устаревания оборудования и его обновления в условиях ограниченного финансирования. Докладчик предложил мотивировать бизнес и разработчиков к созданию собственной программно-аппаратной базы, модернизации систем видеонаблюдения и масштабированию современных решений.

Об оценке качества систем ИИ применительно к задачам видеонаблюдения говорил Ю. Силаев (АО «Цикада»). Он выделил классический подход использования систем ИИ для распознавания объектов, дыма и пожаров, а также задачи повышенной сложности, требующие исследований и обучения нейронных сетей. Спикер отметил важность тестирования сложных систем не только на датасетах и стендах разработчика, но и на стороне регуляторов и потребителей. Необходимы проработки понятий модели качества и оценки ка-

чества на каждом этапе жизненного цикла и при разработке таких систем.

Докладчик обратил внимание на работы, которые ведутся в рамках ТК 164 «Искусственный интеллект», и выделил группы характеристик, связанные с функциональными возможностями, надёжностью и защищённостью систем и их метриками для решения прикладных задач. Он предложил разработать подходы по комплексному тестированию систем видеонаблюдений с использованием ИИ и их сертификации в будущем. Важный аспект — кибербезопасность подобных систем, защита каналов связи и самих камер. Многие вопросы необходимо рассматривать в рамках ТК 164 и ТК 362 «Защита информации», считает Ю. Силаев.

В ходе дискуссии участники уточнили, что часть из затронутых вопросов уже находится в работе подкомитетов ТК 164, а системы видеонаблюдения относятся к объектам категорирования КИИ и уже подпадают под регуляторные требования ФСТЭК России.

Завершая сессию, модератор С. Соболев (НИЦ «Технологии») предложил также организовать взаимодействие отрасли с Консорциумом для исследования ИБ искусственного интеллекта в части безопасного применения технологий ИИ к задачам видеонаблюдения.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

Завершила круглый стол секция «Обеспечение кибербезопасности в условиях реализации атак, основанных, в том числе, на использовании ИИ».

Модератор сессии А. Тихонов (Ассоциация «Доверенная платформа») напомнил, что, согласно прогнозам, сделанным Ассоциацией и «Росатомом» в 2021 г., искусственный интеллект, квантовые вычисления и недокументированные возможности были определены как главные потенциальные угрозы кибербезопасности на 2025 г. Этот прогноз уже оправдывается в части ИИ. Проведена большая работа в части доверенного ИИ, и сформировался некий «портрет» ИИ как оружия. В первую очередь это связано с генеративным ИИ и дипфейками. Уровень «специализации» экспертизы ИИ растёт во всех областях, этим пользуются и злоумышленники. ИБ-специалисты уже столкнулись со способностью ИИ масштабировать атаки с огромной скоростью.

Ю. Силаев отметил появление новых типов атак и систем защиты на базе ИИ. Однако возникают проблемы с сертификацией и разработкой доверенных фреймворков — этим занимаются специалисты ИСП РАН и регуляторы. Спикер отметил необходимость создания новых требований на всех этапах жизненного цикла датасетов и моделей, подходов к обучению и переобучению моделей, а также интерпретации результатов. Самые жёсткие требования должны быть прописаны к этапу эксплуатации, спикер привёл аналогию с требованиями к СКЗИ и их аккредитации.

Е. Генгринович (АО «Инфотекс») уточнил, что технологии ИИ уже сертифицированы как инструменты в ряде продуктов и используются для помощи и ускорения при принятии решений. Устойчивостью таких решений могут заниматься только производители, а задачи компаний, работающих в области ИБ, — помочь им с инструментами для внедрения решений и их сертификации.

Хакеры успешно используют технологии ИИ для исследования инфраструктуры предприятий, поиска уязвимых мест для максимального ущерба. ИИ значительно сокращает время подготовки атак, отметил докладчик. Наметилась тенденция и к пересмотру старой модели построения бизнес-процессов и стиранию границ между подразделениями в условиях новой цифровой реальности, считает Е. Генгринович. Эти же подходы приходят и в образование, где все специалисты должны получать знания в сфере ИТ и ИБ.

Дискуссию о роли и месте кибербеза в бизнес-процессах предприятий, нейросетях и СЗИ, а также оценки зрелости организаций и подходов к ИБ завершил модератор. Он отметил:

- готовность участников работать по теме технологий ИИ и их применения;
- необходимость взаимодействия с Консорциумом для исследования ИБ ИИ для определения системных предложений и подходов по применению технологии ИИ в целях оценки уровня киберустойчивости; необходимость взаимодействия с ТК 167 «Программно-аппаратные комплексы для КИИ» в части разработки требования по контролю устойчивости на жизненном цикле доверенных ПАК и систем с информационной составляющей, в т.ч. с использованием ИИ.

ПОСАДЯТ ВСЕХ И КАЖДОГО

НОВЫЙ ЗАКОН О КИБЕРБЕЗОПАСНОСТИ МАЛАЙЗИИ РАСПРОСТРАНЯЕТ УГОЛОВНУЮ ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ ИБ НА СОТРУДНИКОВ ОБЪЕКТОВ КИИ

Марина БРОДСКАЯ
обозреватель
BIS Journal

НА УРОВНЕ ГОСУДАРСТВА

Швейцария. Швейцария присоединится к Европейской организации по кибербезопасности (ECSO), сообщило правительство конфедерации. Эти меры направлены на укрепление защиты нейтральной страны от хакеров и кибератак. Благодаря членству в ECSO правительство Швейцарии получит информацию о текущих технологических решениях и разработках, а также доступ к сетям экспертов, говорится в заявлении Берна.

В ECSO входят 300 участников, в том числе корпорации и малые компании, университеты и исследовательские центры, правительства европейских стран.

В 2024 г. Швейцария зафиксировала рост кибератак и фейков, число которых увеличилось в преддверии саммита по Украине.

Малайзия. Малайзии приняли «Закон о кибербезопасности». Он разработан в рамках национальной стратегии кибербезопасности и вступил в силу 26 августа, после принятия нормативных актов, подготовленных профильным национальным агентством.

Новый закон направлен на повышение кибербезопасности национальной КИИ, к ней относятся любые компьютеры или системы, выход из строя которых может повлиять на национальную безопасность, экономику, общественное здравоохранение или работу правительства. Документ вводит требования по управлению киберугрозами и режиму лицензирования поставщиков услуг кибербезопасности и имеет экстерриториальное применение.

Документ определяет как КИИ правительство, финансовый сектор, транспорт, оборону и национальную безопасность, информационно-телекоммуникационные и цифровые технологии, энергетику и медицину, водоснабжение, канализацию и утилизацию отходов, сельское хозяйство, торговлю и промышленность, сферу науки, технологий и инноваций.

Согласно закону, каждый из секторов КИИ получит своего руководителя, ответственного за ИБ. В его обязанности войдёт разработка отраслевых кодексов и стандартов, касающихся управления кибербезопасностью, и категорирование объектов КИИ. Организацией КИИ может стать госструктура или физическое лицо, владеющие или управляющие объектом КИИ. В обязанности такого субъекта входит информирование руководителя сектора обо всех изменениях в структуре по запросу или самостоятельно в течение 30 дней; реализация отраслевых требований к объектам КИИ и оперативное извещение об инцидентах. Закон не распространяет требования к отчётности на киберинциденты с участием цепочки поставок, куда вошли объекты КИИ.

Документ вводит режим лицензирования для поставщиков услуг кибербезопасности. Работа без лицензии является уголовным преступлением, карается крупным штрафом и/или тюремным заключением на срок до десяти лет.

Наказания за несоблюдение Закона о кибербезопасности варьируются в зависимости от типа и серьёзности нарушения. Ответственность распространяется также на сотрудников и агентов организации-нарушителя.

Венесуэла. Кибербезопасность стала политической проблемой Венесуэлы. 12 августа ми-

нистр науки и технологий Венесуэлы Габриэла Хименес на заседании Госсовета и Совета национальной обороны страны представила доклад, в котором отмечена уязвимость национальной технологической системы.

Согласно заявлению, с 28 июля атакам подверглись практически все институты Венесуэлы, включая системы Президента республики, Национальный избирательный совет (CNE) и Национальный телекоммуникационный провайдер (CANTV). Пострадали 25 учреждений, расследование инцидентов в 40 организациях продолжается.

Венесуэльские эксперты считают, что эта кибератака стала беспрецедентной для страны и является частью стратегии государственного переворота: на целевые DDoS-атаки пришлось 65% всех атак, были затронуты серверы госучреждений и международные каналы связи; 17% атак — фишинговые, проведена массовая рассылка заражённых электронных писем. В 6,9% случаев происходила подмена DNS, в 3,45% инцидентов был перехват BGP-маршрутов, а в 3,44% инцидентов — дефейс веб-сайтов. Также злоумышленники перехватывали IP-адреса CANTV.

Пик кибератак пришёлся на 29 июля, когда венесуэльские специалисты зафиксировали 30 млн атак в минуту, что совпадает с данными OpenStack Security Advisories (Ossa). 98% DDoS-атак, пиковые нагрузки которых достигали 700 Гб/сек, шли через сервисы бот-ферм с настольных компьютеров, менее 2% пришлось на мобильные технологические платформы. Объём трафика через системы CANTV в пять раз превышал возможности этой ИТ-структуры Венесуэлы. Кибератаки не прекратились и после президентских выборов.

Источник кибератаки, по данным венесуэльских властей, находился в Северной Македонии, где размещаются киберкоманды Пентагона и НАТО. «За кибервойной против Венесуэлы стоит огромная экономическая и технологическая держава», — считает Г. Хименес. Для обеспечения ИБ страны необходима поддержка правительства.

Поэтому президент Николас Мадуро создал Национальный совет кибербезопасности. Министерство науки и технологий и новая структура как будут решать текущие задачи по отражению атак и смягчению их последствий, так и начнут разрабатывать новые стратегии безопасности, учитывая, что киберпространство стало полем для новых гибридных войн.

ИБ В ОТРАСЛИ

Судостроение. Норвежская компания Kongsberg Maritime завершила тестирование систем автоматизации, навигации и динамического позиционирования на соответствие стандарту IACS UR E27 «Киберустойчивость бортовых систем и оборудования», который основан на серии стандартов кибербезопасности в системах автоматизации и управления. Тестирование включает сертификацию по 1-му классу кибербезопасности DNV Cyber Security, который устанавливает требования к судам и морским установкам.

Международная ассоциация классификационных обществ (IACS) ввела два унифицированных требования (UR E26 и E27) для снижения киберрисков. Они стали обязательными для всех судов, построенных после 1 июля 2024 г. UR E26 регулирует проектирование и эксплуатацию судов, а UR E27 применяется к основным бортовым системам и потребует от верфей, проекцтировщиков и владельцев встраивать решения по кибербезопасности в системы и суда.

В прошлом году компания Kongsberg Maritime решила ускорить сертификацию своей продукции. Она разработала программу, включающую оценку каждого продукта и внедрение необходимых функций и документации для обеспечения соответствия стандартам безопасности, качества, охраны здоровья и окружающей среды. Компания ожидает, что большинство её цифровых продуктов получат одобрение типа DNV на соответствие требованиям к концу августа. Следующим шагом станет расширение сферы применения интеграционных и энергетических систем, силовых установок и оборудования для обработки грузов.

Сертификация об утверждении типа также принесёт пользу верфям при новом проектировании, интеграции, монтаже и испытаниях морской техники Kongsberg, строительстве и модернизации судов. Поскольку продукты уже проходят предварительную проверку на соответствие требованиям ИБ, это значительно сэкономит время на этапах проектирования и тестирования.

Тесное сотрудничество между Kongsberg Maritime и DNV повысило эффективность процедур за счёт создания единого подхода к интерпретации и документированию сертификационных требований. Упрощённый порядок работы позволит ускорить получение разрешений и уделит повышенное внимание тестированию продукции.

Автомобильная промышленность. Мировые автопроизводители готовят стандарты для автомобильного ПО. К отраслевой инициативе по улучшению кибербезопасности автомобилей присоединились японские компании, включая Toyota Motor и Hitachi.

116 компаний, входящих в Японский центр обмена и анализа информации в автомобильной промышленности (Japan Automotive Information Sharing and Analysis Center, J-Auto-ISAC), хотят сформулировать общеотраслевые правила, касающиеся спецификаций ПО (software bills of materials, SBOM), или перечней компонентов автомобильного ПО.

Центр J-Auto-ISAC планирует завершить разработку стандартов к марту 2025 г., чтобы помочь компаниям быстро определять, используют ли они ПО, уязвимое для кибератак.

Требования по безопасности автомобилей, основанные на стандартах ООН, становятся обязательными в Японии и Европе. Многие крупные автопроизводители сотрудничают с поставщиками для разработки собственных программных продуктов. Это привело к тому, что SBOMs компаний различаются, при этом одна и та же программа может быть классифицирована или названа по-разному в разных спецификациях. Это затрудняет поиск компонента, который использует уязвимую программу.

Широкое распространение подключённых к интернету автомобилей, необходимость управления сведениями о транспортных средствах и оказания помощи при вождении приводят к необходимости стандартизации данных. Tesla и автопроизводители из КНР лидируют в производстве подключённых к сети транспортных средств благодаря бизнес-модели, основанной на подписке и частых обновлениях ПО.

Обновления могут улучшить функциональные свойства автомобиля. Но неконтролируемые уязвимости ПО позволяют реализовать кибератаки, которые могут завести двигатель или остановить автомобиль, дать доступ угонщикам, открыв салон удалённо. Нарушение безопасности также может привести к краже данных о поездках и ПДн. Злоумышленники смогут угонять транспортные средства, как только автономное вождение станет распространённым явлением.

Ожидается, что объём кодирования в автомобильном ПО будет расти по мере усложнения функций помощи водителю. Стандартизация узлов для устранения уязвимостей ПО также поможет контролировать затраты на разработку.

В мае этого года технический комитет J-Auto-ISAC, куда входят автопроизводители Toyota и Mazda Motor, производители запчастей Aisin и Denso, промышленная группа Hitachi, подготовил предложение по единым правилам SBOM. Ведётся совместная работа с Ассоциацией производителей автомобилей Японии и другими структурами по оценке применения предлагаемых норм на практике. Ожидается, что после окончательного согласования новые стандарты будут приняты в 2025 году.

В альянс автопроизводителей Auto-ISAC, помимо японских и американских компаний, также входят европейские концерны, например Mercedes-Benz. J-Auto-ISAC уже начал координировать свою деятельность с Automotive ISAC из США, который взял на себя ведущую роль в разработке единых отраслевых правил для инвентаризации ПО.

ОБРАЗОВАНИЕ И КАРЬЕРА

Университет Нового Южного Уэльса провёл Australian Cybersecurity Games. Конкурс, организованный Австралийской сетью педагогов и специалистов по кибербезопасности SECedu, прошёл со 2 по 30 сентября 2024 г. и привлёк внимание студентов всей страны.

SECedu возникла как результат партнёрства университета из Сиднея и Commonwealth Bank, организация объединила усилия австралийских педагогов и крупнейших команд по кибербезопасности Австралии для подготовки нового поколения ИБ-специалистов.

Australian Cybersecurity Games направлены на сотрудничество, инновации и развитие навыков среди студентов, выбирающих карьеру в области кибербезопасности. Цель игр — предоставить студентам площадку для получения новых навыков у экспертов отрасли, демонстрации полученных навыков, общения с коллегами и профессионалами. Студенты приняли участие в практических занятиях и состязаниях, в т.ч. имитирующих реальные сценарии кибератак и защиты, изучили методы криптографии, сетевой безопасности и работы с веб-уязвимостями.

«Australian Cybersecurity Games подчёркивают важность образования в области кибербезопасности и побуждают студентов расширять границы своих знаний и креативности, — заявил директор SECedu и профессор университета Ричард Бакленд. — Игры ставят студентам реальные задачи, чтобы помочь развить практические навыки и образ мышления, столь необходимые будущим специалистам по кибербезопасности».

По оценке экспертов, подобные соревнования способствуют не только индивидуальному росту и успешной карьере их участников, но и защите цифровых активов страны и национальной безопасности в целом.

СПОРТ, СПОРТ, СПОРТ!

Олимпиада и чемпионат Европы по футболу. Главные спортивные события 2024 года принесли не только радость любителям спорта, но и головную боль специалистам по кибербезопасности. Чемпионат Европы по футболу и Олимпийские игры в Париже стали центром притяжения для киберпреступников. Согласно обзору Human Risk Review 2024 от SoSafe, любой ажиотаж способствует манипулированию людьми. Атаки с использованием социальной инженерии были успешно реализованы и масштабированы с помощью ИИ. 79% опрошенных сотрудников службы безопасности с тревогой оценивают растущее влияние генеративного ИИ. Киберпреступники рассылают фишинговые email, обещая бесплатные билеты или ставки на игры с привлекательными призами. Эти эмоционально насыщенные предложения используют чувства и азарт спортивных болельщиков и легко заманивают их в ловушку.

ИТ-инфраструктуры, необходимые для организации крупных мероприятий, часто особенно уязвимы из-за их сложности и большого объёма обрабатываемых данных. Инфраструктуры включают не только системы, используемые для управления мероприятиями, но и сети для связи, продажи билетов и трансляции мероприятий. Личная и финансовая информация миллионов посетителей, участников и организаторов чрезвычайно ценна для киберпреступников и может быть использована для различных видов кибератак, включая фишинг, программы-вымогатели и кражу данных.

Перед чемпионатом Европы по футболу МВД Германии и УЕФА предупредили об атаках на систему продажи билетов, поскольку в этом году впервые использовались исключительно электронные билеты. Ещё до начала первого этапа продаж от компьютерных ботов были получены миллионы недействительных запросов, которые парализовали работу системы или вводили в систему фальшивые билеты.

Не спортом единым. Во время Олимпийских игр хакеры предприняли атаку с использованием программ-вымогателей на музеи Парижа. Хакеры атаковали систему, которая централизует финансовые данные магазинов и бутиков музеев по всей Франции. Они заблокировали доступ и пригрозили обнародовать данные, если учреждения не заплатят требуемый выкуп в криптовалюте.

По оценкам исследователей, за атаками стоят как отдельные киберпреступники, стремящиеся к финансовой выгоде, так и субъекты, поддерживаемые иностранными государствами и движимые политическими или экономическими мотивами. Поэтому внедрение комплексной стратегии безопасности сложных мероприятий должно быть приоритетом у организаторов. Эта стратегия должна охватывать не только технологические меры, но и весь персонал. В 74% случаев киберпреступники нацеливаются на сотрудников, чтобы получить доступ к системам.

Устойчивая защита в цифровой среде возможна только в случае, если кибербезопасность станет частью повседневной жизни, напоминают ИБ-эксперты.

Футбольные клубы. Итальянский «Ювентус» и компания Fortinet, мировой лидер в области кибербезопасности, подписали соглашение о том, что Fortinet является новым официальным ИБ-партнёром футбольного клуба на ближайшие два сезона. «Ювентус» будет использовать платформу Fortinet Security Fabric для идентификации и решения сетевых проблем и проблем безопасности на объектах клуба до 2026 года.

Домашний стадион клуба Allianz является примером устойчивого развития и одним из развлекательных центров и туристических достопримечательностей Турина. «Ювентус» внедрит решения Fortinet в районе Continassa, включая штаб-квартиру клуба, дата-центр стадиона, отель, медицинский и тренировочный центры первой команды Италии.

Платформа Fortinet Security Fabric позволяет объединять сетевые технологии и безопасность, повысит прозрачность, производительность и сократит среднее время реагирования на инциденты.

Представители клуба уверены, что сотрудничество с Fortinet станет ключевой вехой для «Ювентуса», позволит создать устойчивую сеть, даст возможность добиваться успехов на поле и за его пределами. А партнёр «Ювентуса» по кибербезопасности видит новые горизонты сотрудничества в области киберзащиты одного из самых технологически продвинутых объектов в мире.

ОДКБ. РЕСПУБЛИКА АРМЕНИЯ

ОБЗОР ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Александр ВИНОГРАДОВ
ФГУП «ЦНИИХМ»

Сергей МЕНЬШИКОВ
основатель Belarusian InfoSecurity Community

Андрей СИТНОВ
независимый эксперт

Валерий СОКОЛЕНКО
заместитель начальника службы информационной безопасности ICBC в г. Алматы

Продолжаем публикацию материалов по анализу законодательств в области ИБ стран — членов ОДКБ. В этом номере рассматриваем законодательство Республики Армении.

БАЗОВЫЕ АКТЫ

Базовыми актами, закрепляющими общие положения о доступе к информации, конфиденциальности и защите информации, являются следующие законы:

Закон РА от 18 мая 2015 г. № ЗР-49-Н «О защите личных данных»

Закон регулирует порядок и условия обработки личных данных органами государственного управления или местного самоуправления, государственными или муниципальными учреждениями, организациями, юридическими или физическими лицами и осуществления за ними государственного надзора.

В целом закон «О защите личных данных» похож на российский закон «О персональных данных». В то же время закон РА имеет ряд специфичных положений.

В частности, кроме понятия «обработка личных данных», вводится понятие «использование личных данных — действие, совершаемое с личными данными, прямой или косвенной целью которого может быть принятие решений или формирование мнения, или приобретение прав, или предоставление прав либо льгот, или ограничение либо лишение прав, или реализация иной цели, которые влекут или могут повлечь для субъекта данных или третьих лиц правовые последствия или иным образом соотноситься с их правами и свободами».

Одним из принципов обработки личных данных является «принцип минимального вовлечения субъектов». Непосредственно от субъекта личные данные стараются не получать. Основным источником личных данных для обработки должна являться единая информационная система.

Сохранено понятие «общедоступных личных данных». Общедоступными считаются имя, фамилия, день, месяц и год, место рождения лица; место, день, месяц и год смерти лица, а также личные данные, которые при совершении субъектом данных сознательных действий, направленных на их общедоступность, становятся доступными для определённого или неопределённого круга лиц.

При взаимодействии с организациями РА, предполагающем обмен персональными данными, следует также учитывать, что в соответствии с законом «О защите личных данных» оператор при обработке личных данных обязан использовать шифровальные средства для обеспечения защиты информационных систем, содержащих личные данные, от случайной потери, незаконного проникновения в информационные системы, незаконных использования, записи, уничтожения, преобразования, блокирования, копирования, распространения личных данных и другого вмешательства. Данное положение требует согласования взаимного применения сторонами средств криптографической защиты информации, в том числе с учётом особенностей российского регулирования в области применения криптографических средств защиты информации.

Закон РА № ЗР-40-Н «Об электронном документе и электронной цифровой подписи»

Закон регулирует отношения, возникающие при применении электронных документов и электронных цифровых подписей, порядок применения электронного документа и электронной цифровой подписи и услуги по сертификации электронной цифровой подписи.

ТАЙНЫ

Конституционно-правовые нормы о защите персональных данных закреплены как в предыдущей, так и в нынешней редакции Конституции Республики Армении, принятой по итогам референдума от 6 декабря 2015 г. Данная норма, имеющая высшую юридическую силу (статья 34), устанавливает право каждого субъекта на защиту персональных данных.

Пункт 1 статьи 141 Гражданского кодекса РА в качестве общей нормы служебной, коммерческой или банковской тайной признаёт ту информацию:

- которая имеет действительную или потенциально коммерческую ценность в силу неизвестности её третьим лицам,
- получение которой невозможно свободным путём на законном основании и
- обладатель которой принимает меры по сохранению её секретности.

Статья 925 Кодекса относительно **банковской тайны** устанавливает общую норму, в соответствии с которой:

1. Банк гарантирует тайну банковского вклада на банковском счету, операций по счёту и сведений о клиенте.

2. Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренных законом.

3. В случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причинённых убытков.

Закон РА от 14 октября 1996 года № ЗР-80 «О банковской тайне»

Статья 4.

Банковской тайной считаются сведения о счетах клиента, ставших известными данному банку в связи с обслуживанием клиента банка, сведения об операциях, совершённых по поручению клиента или в его пользу,

ОБЩИЕ СВЕДЕНИЯ

Республика Армения (далее — РА). Государство в Закавказье, не имеет выхода к морю. Граничит с Азербайджаном на востоке; на юго-западе — с Нахичеванской АР, входящей в состав Азербайджана; с Ираном на юге, с Турцией на западе и с Грузией на севере. Столица — город Ереван. Государственный язык — армянский.

Армения является членом ООН, ОДКБ, СНГ, ЕврАзЭС, МВФ, ОБСЕ, ВТО.

Органы, утверждающие и согласовывающие законы и подзаконные акты в области ИБ: Президент РА, Правительство РА.

Все рассмотренные в публикации документы имеют общереспубликанское значение и применяются для организации и обеспечения информационной и кибербезопасности. Государственная политика РА в сфере ИБ регулируется следующими нормативными актами и развивается по представленным направлениям.

а также его коммерческая тайна, сведения о любой программе его деятельности или о разработке, изобретении, промышленном образце и любое другое сведение о нём, которое клиент был намерен сохранить в тайне, и банк знал или мог знать об этом намерении.

Закон РА от 24 марта 2023 года за № ЗР-49 «О государственной тайне»

Статья 3.

Государственная тайна (сведения, содержащие государственную тайну) — сведения, продукция или материалы в военной области или области внешних отношений, либо в экономической, научно-технической, либо разведывательной, внешнеразведывательной, контрразведывательной, оперативно-разведывательной областях деятельности Республики Армении, которые согласно настоящему Закону охраняются и защищаются государством и распространение которых может нанести ущерб национальной безопасности или интересам Республики Армении;

Служебная информация ограниченного распространения — сведения, продукция или материалы, относящиеся к деятельности государственных органов и органов местного самоуправления, юридических лиц, должностных лиц Республики Армении, согласно настоящему Закону не относимые к содержащим государственную тайну сведениям, которые содержат элементы государственной тайны, однако сами по себе не раскрывают государственную тайну и распространение которых может иметь негативное воздействие на оборону, национальную безопасность, внешние отношения, политические и экономические интересы Республики Армении, охрану правопорядка.

РЕГУЛИРОВАНИЕ В СФЕРЕ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Уголовный кодекс Республики Армении (статья 144) предусматривает уголовную ответственность за незаконный сбор, хранение, использование и распространение информации о частной (личной и семейной) жизни лиц.

Кодексом РА об Административных правонарушениях (статья 189.17) предусмотрена административная ответственность за нарушение закона «О защите персональных данных»:

1. Нарушение установленного законом порядка сбора или звукозаписи, или ввода, или координирования, или организации, или корректировки, или хранения, или использования, или преобразования, или восстановления, или передачи личных данных, если данное деяние не содержит признаков преступления (влечёт назначение штрафа от двухсоткратного до пятисоткратного размера установленной минимальной заработной платы).
2. Нарушение установленного законом порядка уничтожения или блокирования личных данных, если данное деяние не содержит признаков преступления (влечёт назначение штрафа от трёхсоткратного до пятисоткратного размера установленной минимальной заработной платы).
3. Непредоставление обрабатывающим лицом установленной законодательством информации по требованию субъекта личных данных в ходе сбора личных данных, или нарушение порядка предоставления, или неразъяснение причин и следствий непредоставления (влечёт назначение штрафа в размере от стократного до двухсоткратного размера установленной минимальной заработной платы).
4. Неуведомление обрабатывающим личные данные лицом в уполномоченный орган по защите личных данных или нарушение порядка уведомления (влечёт назначение штрафа от пятидесятикратного до стократного размера установленной минимальной заработной платы).
5. Неиспользование криптографических средств в ходе обработки личных данных, если данное деяние не содержит признаков преступления (влечёт назначение штрафа в стократном размере установленной минимальной заработной платы).
6. Нарушение требований к обеспечению безопасности обработки личных данных в информационных системах, требований к материальным носителям биометрических данных и технологиям хранения этих личных данных вне информационных систем, если данное деяние не содержит признаков преступления (влечёт назначение штрафа в размере от стократного до двухсоткратного размера установленной минимальной заработной платы).
7. Несоблюдение конфиденциальности лицами, обрабатывающими личные данные, или иными лицами, предусмотренными законом, во время или после исполнения служебных или трудовых обязанностей, связанных с обработкой личных данных (влечёт назначение штрафа от двухсоткратного до трёхсоткратного размера установленной минимальной заработной платы).

НАЦИОНАЛЬНЫЕ СТАНДАРТЫ

ISO/IEC27001 — Information Technology — Security techniques — information security management systems — requirements Standard

На этот стандарт ссылается «Порядок об установлении минимальных требований по обеспечению информационной безопасности» от 9 июля 2013 г. № 173Н, где прописано, что финансовые организации должны построить свою систему управления информационной безопасности, соответствующей требованиям международных стандартов, применяемых в области обеспечения информационной безопасности, и получить сертификат о соответствии требованиям соответствующих стандартов.

Надеемся, что данная статья поможет вам не заблудиться в Законодательстве РА. Мы постарались облегчить путь изучения и применения на практике нормативных документов в области ИБ одного из наших соседей, члена ОДКБ — Республики Армении.

СКОВАННЫЕ ОДНОЙ ЦЕПЬЮ

ОТ ОТДЕЛЬНЫХ УЯЗВИМОСТЕЙ К БЛОКИРОВАНИЮ МАРШРУТОВ АТАК

Алексей ЛУКАЦКИЙ
бизнес-консультант по безопасности Positive Technologies

В мире кибербезопасности есть ряд основополагающих принципов, неменяющихся годами и десятилетиями, а есть ряд достаточно спорных правил, которые превратились в нечто монументальное, незыблемое, что никто не хочет свергнуть с пьедестала. Например, классическое уравнение риска ИБ, которое представляет собой произведение уязвимости, угрозы и ущерба. Даже если в принципе не брать некорректность этой формулы (все-таки риск — это не про изначально плохое, это про возможности, которые могут дать как положительный, так и отрицательный эффект), то многие специалисты фокусируются на первом показателе, тратя на него все силы.

При этом многие компании продолжают делать одну и ту же ошибку: фокусируются на отдельных уязвимостях, упуская из виду способы их эксплуатации. А ведь здравый смысл подсказывает нам, что не все из них опасны, а если и опасны, то не в конкретно вашей организации. Эффективность защиты часто зависит не от того, как много уязвимостей мы можем обнаружить и устранить, а от того, как хорошо мы понимаем пути, по которым атакующие могут добраться до ключевых активов организации, то есть как может быть реализована угроза и какой ущерб может быть нам нанесен (вот и оставшиеся две переменные уравнения риска проявились). Именно поэтому важно отойти от анализа атомарных событий, которые нам дают отдельные средства защиты и сосредоточиться на управлении цепочками атак.

Вместо того чтобы рассматривать уязвимости как изолированные события, стоит анализировать их как элементы более широкого пути атаки, по которому идет злоумышленник, чтобы достигнуть своей цели. Вы обращали внимание на одну странность — в Даркнете, на форумах по продаже доступов в различные компании, их стоимость измеряется сотнями или, в крайнем случае, тысячами долларов. И это при том, что сами компании, в периметре которых нашли уязвимость и

продают ее, ворочают десятками и сотнями миллиардов долларов. Почему такой разрыв? А все потому, что использование всего одной уязвимости не дает злоумышленнику почти никакого преимущества и не приводит к реализации ущерба для уязвимой компании. Нужно найти несколько уязвимостей на всем маршруте движения от периметра до конечной цели (АБС, АСУ ТП, биллинг, сервер бухгалтерии, Active Directory, сервер сборки ПО и т.п.), простроить этот маршрут по нужным узлам, не зайти в тупик и успеть реализовать недоброе, пока тебя не заметила служба ИБ. Поняв это, мы сможем лучше разобраться, какие уязвимости могут действительно привести к недопустимым для организации событиям, влекущим катастрофические последствия.

Исследования показывают, что в среднем у компании существует около 11 000 уязвимостей, которые могут быть использованы злоумышленниками. У крупных предприятий этот показатель может превышать 220 000. Однако далеко не каждая из этих уязвимостей представляет реальную угрозу. На самом деле, около 75% всех обнаруженных уязвимостей, в случае их эксплуатации, ведут в так называемые «тупики», то есть они не представляют реальной опасности для критических активов компании.

Ключевая проблема заключается в том, что команды кибербезопасности тратят слишком много времени на обработку этих незначительных уязвимостей. И это негативно влияет на их результативность. Вместо того чтобы сосредоточиться на действительно важных угрозах, они тратят время на задачи, которые не приносят ощутимого снижения риска. Даже попытка применить один из пары десятков стандартов и подходов по приоритезации уязвимостей не дает эффекта — они либо слишком сложны для ежедневной работы, либо заставляют нас быть привязанными к продуктам конкретного вендора, который придумал очередное «ноу-хау» и только благодаря его секретному соусу все уязвимости будут побеждены. Но те, кто в ИБ работает давно, понимает, что это не так, серебряной пули не существует.

Как же решить эту проблему? Во-первых, важно понимать, какие активы в компании являются критическими с точки зрения бизнеса. Это могут быть данные клиентов, финансовые системы или ключевые производственные процессы. Важно классифицировать эти активы и определить, какие из них имеют наибольшее значение для достижение бизнес-целей. Этот процесс позволяет лучше понять, какие уязвимости представляют наибольшую угрозу, и сфокусировать усилия именно на них. Да, выстраивание процесса управления активами само по себе не является простой задачей, но без ее решения (даже в первом приближении) мы будем походи на героя русских сказок, которого регулярно посылают «туда, не зная куда, принести то, не зная что». Но и тут есть лайфхак — не надо пытаться идентифицировать все активы и одинаково управлять ими всеми. Достаточно обратиться к бизнесу и спросить, что важно именно ему. Затем, с помощью владельцев бизнес-процессов и систем, а также при непосредственном участии ИТ и АСУ ТП служб, определяются ключевые системы, которые и будут интересны хакерам, а также рассматриваться как первоочередные объекты защиты, а также мониторинга.

Во-вторых, необходимо начать работать с цепочками атак. Это означает, что вместо того, чтобы просто фиксировать наличие уязвимости, нужно оценивать, как эта уязвимость может быть использована злоумышленниками для достижения их целей. Например, простая уязвимость в системе не всегда является проблемой, если она не связана с критически важным активом. Но если она может быть использована для доступа к важным данным, то ее нужно устранять в первую очередь.

Исследования показали, что только 2% всех уязвимостей находятся на «узловых» точках, которые могут привести к компрометации критических для бизнеса активов. Именно эти уязвимости и должны стать фокусом для команд безопасности. Получается, что из 11000 уязвимостей только около 220 действительно требуют немедленного внимания. А компании могут справиться только с 10% из них, что означает, что в реальности может быть исправлено лишь 22 уязвимости. Это вроде небольшая часть от общего числа, но именно они могут оказать наиболее значимое влияние на безопасность компании, так как именно они интересны хакерам, стремящимся добраться до целевых систем организации. Помочь в ответе на вопрос «А какие 10% надо устранить в первую очередь» могут не только качественные сервисы Threat Intelligence, данные по трендовым уязвимостям, используемым именно сейчас в «дикой природе», но и специалисты по проведению тестов на проникновение, которые сами используют понятие «цепочки» и знают, какие уязвимости чаще всего используются в пентестах.

Важно отметить, что фиксация на ненужных уязвимостях приводит к тому, что команды не достигают своей цели — повышения результативности. Вместо этого они теряют время на «тупиковые» задачи, которые не влияют на снижение риска и недопущение катастрофических для бизнеса последствий. В результате эффективность работы падает, а ключевые угрозы остаются без внимания.

Анализ путей атак как раз и помогает решить эту проблему и минимизировать количество ненужных действий, сосредоточившись на главном. Он помогает понять, какие уязвимости действительно могут быть использованы злоумышленниками для достижения их целей. А это, в свою очередь, позволяет значительно сократить вре-

	Активов	Путей атак	Критических путей атак
Здравоохранение	72 000	55 000	0,04%
Финансовый сектор	59 000	46 000	0,5%
Ретейл	41 000	38 000	0,07%
Бизнес-услуги	29 000	30 000	0,1%
Производство и технологии	48 000	26 000	0,1%
Агросектор и пищевая промышленность	19 000	25 000	0,2%
Образование и государство	18 000	15 000	0,6%
Транспорт	14 000	12 000	7%
Энергетика и ЖКХ	11 000	11 000	11%
Телеком и СМИ	16 000	9 200	0,2%

Таблица 1.

мя и усилия, затрачиваемые на устранение второстепенных угроз.

По данным аналитики в среднем в организации существует 15000 путей атак (100 тысяч у крупных предприятий), но 74% из них ведут «в тупик», то есть малоинтересны и для хакеров и, соответственно, для специалистов по ИБ. Эта цифра нам вновь говорит о том, что не надо защищать абсолютно все и инвестировать туда, где мы не увидим отдачи. Критических же путей, которые ведут сразу к целевым системам и того меньше — доли процентов, а значит, сфокусировавшись на них в первую очередь, мы получим максимум результата (см. таблицу).

Таким образом, эффективная кибербезопасность — это не просто обнаружение всех уязвимостей и устранение большей их части. Это умение правильно расставлять приоритеты и работать с теми уязвимостями, которые могут действительно привести к нанесению ущерба за счет анализа цепочек атак.

Но... если у нас есть список ключевых и целевых систем, приоритизированный список уязвимостей, а также понимание цепочек их использования, то может быть мы способны автоматизировать задачу и обнаружения передвижения хакера по его маршруту? А раз мы можем обнаружить это движение, то нам не составляет большого труда и заблокировать хакера, не дав ему достигнуть целевых систем? А может быть пойти еще дальше и, зная цепочку атаки, разорвать ее путем включения тех или иных защитных мер — многофакторной аутентификации, сегментации сети, установки виртуальных или реальных патчей, добавления новых правил контроля доступа на NGFW?..

И тут мы вплотную подходим к тому, что можно было бы назвать автопилотом ИБ, когда средства защиты, а они уже появляются на мировом рынке, начинают самостоятельно, без участия и так все время нехватающих кадров, автоматически защищать нас от 80–90% всех возможных угроз, что не просто хорошо, а в разы лучше, чем обеспечивается в современных организациях.

* * *

Подводя итог, стоит сказать, что основная задача команд безопасности — это не просто закрывать все уязвимости, а делать это результативно. Для этого нужно правильно классифицировать активы, определять цепочки атак и выделять наиболее важные из них, после чего либо вручную, либо в перспективе в автоматическом режиме эффективно управлять ими, предотвращая нанесение ущерба для организации. В конечном счете, это поможет командам добиться большей эффективности и снизить вероятность реализации недопустимых событий, которые могут угрожать бизнесу.

ОТ КАРИЕСА ДО ПУЛЬПИТА

ЗАМЕТКИ БЕЗОПАСНИКА

Александр ИГОНИН
эксперт BIS Journal,
ведущий рубрики

В конце прошлой заметки я упомянул о теневой инфраструктуре. Сегодня поговорим о не совсем очевидной её части — учётных записях (УЗ). Они очень важны, так как фактически являются ключом для входа, в ряде случаев — напрямую из интернета. Рассмотрим несколько типичных проблем.

АКТУАЛЬНЫЙ ВЛАДЕЛЕЦ

Прежде всего, это банальное обеспечение того, чтобы у каждого аккаунта был указан актуальный владелец. «Ничейные» УЗ могут стать лёгкой добычей злоумышленников. Вот пример: в SOC поступил алерт из Azure о подозрительном входе в систему. Соответствующий аккаунт временно заблокировали, а в ходе расследования установили, что:

- попытка входа была успешной (то есть УЗ действительно была скомпрометирована);
- аккаунт был неиспользуемым (так как спустя несколько месяцев никто так и не попросил его разблокировать).

ACTIVE DIRECTORY

Второй аспект касается Active Directory: неплохо бы периодически проводить аудиты состояния учётных записей в ней. Пример: произошёл инцидент, в ходе которого была скомпрометирована УЗ администратора домена. Затем при очередном аудите AD было обнаружено, что у этой УЗ были изменены определённые параметры, что позволяло злоумышленнику подобрать пароль доменного администратора значительно быстрей обычного. Выявлено это было так: команда Get-Aduser сгенерировала дамп всех учётных записей AD, после чего было проанализировано поле UserAccountControl. Несмотря на большое количество пользователей, упомянутое поле имело всего порядка 5–6 уникальных значений, а подозрительный флаг присутствовал лишь у скомпрометированной УЗ.

Ещё пример: в ходе пентеста «белые шляпки» обнаружили, что пароли у нескольких сервисных учётных записей были указаны прямо в поле «комментарий» в Active Directory. Надо ли говорить, что после обнаружения этого факта взлом сети пошёл куда веселее...

ЛОКАЛЬНЫЕ УЗ

Ну и третий момент — это локальные учётные записи. Отследить их появление и использование значительно труднее, чем в случае централизованных аккаунтов. Да, они обладают меньшим «радиусом действия», но могут доставить немало головной боли. Один из примеров здесь — это практика использования сотрудниками техподдержки аккаунта локального администратора, который имеет одинаковое имя и пароль на всех ПК и серверах. Скомпрометировав любой хост и узнав этот пароль, злоумышленник автоматически получает административный доступ на любом другом хосте сети, куда ему удалось попасть. Одним из возможных решений проблемы называют LAPS; впрочем, организаций, сумевших это внедрить, я видел немного.

Другой пример: как-то раз я запросил у администраторов СУБД список пользователей, имеющих разрешение на обращение к определённой базе данных. Мне прислали список из нескольких сотен активных локальных УЗ, в котором фигурировали имена вроде *c*, *test*, *victor* и так далее. Кому все эти аккаунты принадлежат и какие из них можно отключить, никто, конечно же, не знал.

Поддержание порядка и обеспечение необходимого документирования — дело непростое, и о нём часто забывают под гнётом более приоритетных задач. До поры до времени это можно игнорировать — однако если пустить всё на самотёк, то рано или поздно инфраструктура деградирует настолько, что единственным вариантом останется создавать с нуля новую. Это подобно кариесу, который без должного лечения с большой вероятностью перерастёт в пульпит (а то и чего похуже). На мой взгляд, специалисты и особенно менеджеры ИБ должны постоянно напоминать руководству компании о рисках недостаточного документирования изменений.

МЕЖДУ МОЛОТОМ И НАКОВАЛЬНЕЙ

ТРИ ВЗГЛЯДА: ПОЛЬЗОВАТЕЛЯ, ГОСУДАРСТВА, СОЗДАТЕЛЯ

Андрей ЖАРКЕВИЧ
эксперт StartX

Телеграм, WhatsApp, Viber и другие мессенджеры играют ключевую роль в повседневной коммуникации миллиардов людей по всему миру. Они предлагают широкий спектр функций, удобны и безопасны. Однако именно безопасность этих мессенджеров всё чаще становится предметом горячих споров. Силовые ведомства требуют от создателей мессенджеров доступа к перепискам. Некоторые страны настолько увлеклись, что перешли к более жёстким мерам. Свежее свидетельство тому — уголовное преследование и арест создателя «Телеграма» Павла Дурова во Франции.

В этой статье рассмотрим три взгляда на безопасность мессенджеров: пользовательский, государственно-силовой и взгляд создателя.

ЗАЧЕМ ЛЮДЯМ БЕЗОПАСНЫЕ МЕССЕНДЖЕРЫ

Никому не нравится, когда их личные письма читают посторонние. Даже если эти посторонние с аргументами на руках объяснят, что руководствуются благими мотивами, предотвращают преступления и защищают общество в целом, у участников переписки неизбежно остаётся ощущение, что кто-то грязными руками покопался в самом сокровенном. Это чувство настолько очевидно и понятно каждому, что во многих странах тайна переписки является неотъемлемым правом граждан, гарантированным Конституцией.

Бумажный конверт был не слишком надёжной защитой. С переездом переписок в мессенджеры обмен сообщениями стал безопаснее благодаря усовершенствованному электронному «конверту» — сквозному шифрованию.

Смысл сквозного шифрования состоит в том, что все личные сообщения, которые вы отправляете, зашифрованы, как и все личные сообщения, которые вы получаете. Расшифровать ваши послания может только получатель, а сообщения, адресованные вам, — только вы. Переписка останется тайной, даже если её кто-то перехватит. Таким образом, сквозное шифрование обеспечивает конфиденциальность переписки в мессенджерах.

Конфиденциальность позволяет свободно делиться мыслями и чувствами без страха, что их услышат посторонние. А поскольку мессенджеры используются не только для личных бесед, шифрование защищает от утечек и финансовых потерь.

Ещё одна важная для пользователей сторона безопасности мессенджеров — уверенность в том, что собеседник именно тот человек, за которого он себя выдаёт. Шифрование не поможет избежать компрометации или утечки данных, если вы беседуете с мошенником, который притворяется вашим знакомым или коллегой.

Защититься от подделки помогает аутентификация пользователей. В большинстве популярных мессенджеров («Телеграм», WhatsApp, Viber, Signal) для этого используется номер телефона. Это удобно, поскольку позволяет предотвратить создание множества фальшивых аккаунтов и снизить уровень мошенничества. Кроме того, телефонный номер можно использовать для двухфакторной аутентификации, что повышает безопасность аккаунта.

Однако в таком способе аутентификации есть недостатки. Самый серьёзный состоит в том, что телефонный номер можно связать с личностью пользователя. Данные о владельцах номеров телефонов доступны правительству или третьим лицам по запросу. Это создаёт угрозу перехвата доступа к аккаунту в мессенджере через несанкционированную замену сим-карты и практически исключает анонимность переписок.

По поводу анонимности в мессенджерах сломано немало копий. Основной аргумент противников анонимности состоит в том, что честным людям незачем скрывать свою личность. Но не всё так просто.

Стремление к анонимности не всегда связано с преступной деятельностью. Кто-то не желает «светить» личные данные перед неограниченным кругом незнакомых людей и компаний. Другие впол-

не обоснованно опасаются правительственного и корпоративного контроля. Никому не хочется пострадать из-за эмоционального комментария или поста на острую тему. А ещё анонимность позволяет избежать конфликтов с текущим работодателем при обсуждении разногласий с коллегами или поиске новой работы.

Таким образом, обычным людям безопасные мессенджеры дают уверенность в том, что их текстовые и визуальные откровения в личных переписках не смогут перехватить посторонние. Аутентификация снижает риск того, что «старый друг» окажется мошенником.

БЕЗОПАСНОСТЬ МЕССЕНДЖЕРОВ И ГОСУДАРСТВО

Преступники с удовольствием используют технологические новинки. Интернет-сервисы не стали исключением. Мгновенный обмен текстом, фото, видео или аудио позволяет оперативно решать массу задач из любой точки мира. Вполне закономерно, что мессенджеры попали в число инструментов, востребованных преступным сообществом. Благодаря сквозному шифрованию содержание переписок остаётся в секрете, а доступность анонимных мессенджеров позволяет скрывать личность.

Силовые ведомства оказались без привычных средств слежки. Прослушивать телефонные звонки бесполезно, потому что все созвоны вместе с перепиской переместились в мессенджеры. А там перехват ничего не даст, ведь расшифровать собранные данные без ключа не получится.

Ключ для шифрования трафика в мессенджерах без доступа к устройству не получить, да и смысла в этом нет, ведь в некоторых мессенджерах каждое сообщение шифруется новым сеансовым ключом. Так происходит в Signal и WhatsApp, который использует для передачи сообщений протокол Signal.

Силовики не смирились с невозможностью получить доступ к зашифрованным перепискам и начали действовать.

В марте 2024 года служба безопасности WhatsApp выпустила внутреннее предупреждение, в котором говорилось, что правительства могли следить за пользователями, не расшифровывая их разговоры.

Правительственные агентства обходили шифрование, чтобы выяснить, какие пользователи общаются друг с другом, в каких группах они состоят и где находятся. Для этого использовался анализ интернет-трафика в национальном масштабе.

Проверка и анализ сетевого трафика полностью невидимы, но они выявляют связи между пользователями. Правительство может легко определить, что человек использует WhatsApp, поскольку данные должны проходить через серверы платформы. Затем можно выявить конкретных пользователей, отслеживая их IP-адрес по учётной записи интернет-провайдера или поставщика услуг сотовой связи.

Команда внутренней безопасности WhatsApp выявила несколько примеров того, как изучение зашифрованных данных позволяло нарушить защиту конфиденциальности приложения с помощью корреляционных атак. Например, когда пользователь WhatsApp отправляет сообщение группе, пакет данных одинакового размера передаётся на устройства каждого члена этой группы. А изучая задержки между отправкой и получением сообщений WhatsApp двумя сторонами, можно определить расстояние до каждого получателя или даже его местоположение.

Подобные атаки эффективны и против других мессенджеров, поэтому отказ от WhatsApp не спасёт от слежки.

Несмотря на возможности, которые даёт анализ метаданных, содержание сообщений тоже представляет интерес. Поэтому в некоторых странах были приняты законодательные акты, цель которых — обеспечить раскрытие зашифрованной переписки и её участников по требованию властей.

Например, одно из положений законопроекта EARN IT Act в США предлагает ослабить защиту данных пользователей. Закон Investigatory Powers Act в Великобритании, который также называют «Хартия перехвата», требует от компаний предоставлять доступ к зашифрованным данным по запросу властей. Индийские «Правила информационных технологий» (IT Rules) 2021 года обязывают платформы не только раскрывать личности отправителей сообщений по запросу, но и обеспечить возможность отслеживания «первого отправителя» сообщений.

Но даже без принудительного доступа к данным существующие уязвимости в мессенджерах могут быть использованы для слежки или нарушения конфиденциальности. Например, в 2019 году была обнаружена уязвимость в WhatsApp, которая позволяла устанавливать шпионское ПО Pegasus от NSO Group через звонки в WhatsApp. Эта уязвимость предоставляла злоумышленникам доступ к сообщениям, микрофону, камере и другим данным на целевых устройствах. Ещё одна уязвимость в обработке GIF-файлов позволяла удалённо выполнять произвольный код на устройствах пользователей при открытии таких файлов.

В РФ законодательство также накладывает ряд требований к владельцам платформ для обмена сообщениями в части доступа к данным, а также правил их хранения. В случае нарушения платформа блокируется с использованием специального оборудования, установленного у провайдеров.

Когда мессенджер «Телеграм» отказался предоставлять информацию по запросам правоохранительных органов, Роскомнадзор принялся

активно блокировать доступ к платформе. Через какое-то время блокировки неожиданно прекратились. Вскоре в «Телеграме» стали появляться каналы государственных учреждений и различных ведомств. Это значит, что руководство мессенджера приняло решение выполнять требования российского законодательства в объёме, который удовлетворил надзорный орган.

В конце лета 2024 года стало известно о блокировке на территории России одного из самых защищённых и безопасных мессенджеров — Signal. Как пояснил Роскомнадзор, Signal не выполнил требования российского законодательства по хранению данных и предоставлению информации о действиях пользователей на территории России.

В итоге безопасность мессенджеров с точки зрения органов власти может существовать до тех пор, пока она не становится препятствием для действий правоохранителей и силовиков. И если платформа отказывается устранять это препятствие, последствия могут быть самыми неприятными. Для владельцев и создателей платформы.

НЕОЖИДАННАЯ ЛИЧНАЯ ОТВЕТСТВЕННОСТЬ

Некоторые страны ввели законодательные меры, которые предусматривают персональную ответственность владельцев платформ для обмена сообщениями за размещение пользователями противоправного контента. Например, Online Safety Act в Великобритании позволяет привлечь к персональной ответственности руководителей технологических компаний, если их платформы не удаляют или не блокируют противоправный контент после уведомления.

В Германии действует Закон о защите сети (Network Enforcement Act, NetzDG), который требует от социальных сетей и платформ для обмена сообщениями оперативно удалять противоправный контент. Руководители компаний могут быть привлечены к ответственности и оштрафованы, если платформа не выполнит эти требования.

В Австралии закон Sharing of Abhorrent Violent Material Act предусматривает уголовную ответственность для руководителей компаний, если их платформы не удаляют «отвратительный насильственный материал».

В Индии в 2021 году были приняты новые правила IT Intermediary Guidelines and Digital Media Ethics Code Rules, в соответствии с которыми социальные медиапосредники (SSMIs), имеющие более 5 млн пользователей, обязаны назначать лиц, которые могут быть привлечены к ответственности за несоблюдение требований по удалению противоправного контента.

В США всё ещё действует Раздел 230 Закона о приличии в коммуникациях (Section 230 of the Communications Decency Act), который предоставляет платформам иммунитет от ответственности за контент, созданный пользователями, однако уже обсуждаются поправки, которые могут ввести персональную ответственность для руководителей компаний за определённые виды противоправного контента. Одна из таких поправок содержится в упомянутом выше EARN IT Act. Авторы поправки предлагают ограничить защиту, предоставляемую онлайн-платформам в рамках Раздела 230, и разрешить привлечение их руководителей к гражданской и уголовной ответственности за размещение пользователями сервисов материалов, связанных с сексуальным насилием над детьми (CSAM).

Французский Закон о доверии в цифровой экономике (Loi pour la Confiance dans l'Économie Numérique, LCEN), принятый в 2004 году, использовался при недавнем аресте Павла Дурова в Париже. В соответствии с этим законом платформы обязаны оперативно удалять или блокировать доступ к противоправному контенту, как только они узнают о его существовании. В случае невыполнения этих обязанностей владельцы платформ могут быть привлечены к ответственности, включая уголовную.

Хотя причины, по которым страны принимают подобные законы, вполне понятны, с точки зрения здравого смысла они не выдерживают критики. Павел Дуров по этому поводу написал в своём телеграм-канале:

«Если страну не устраивает работа интернет-сервиса, принято подавать в суд именно на сам сервис. Использовать законы, принятые до появления смартфонов, чтобы попытаться возложить ответственность на руководителей платформ за действия третьих лиц, — неверный подход. Никто не будет работать над инновационными технологиями, зная, что их могут судить за то, что кто-то будет злоупотреблять их изобретениями».

В самом деле, почему руководитель BMW не несёт ответственности за нелегальные грузы, которые перевозят на выпущенных им автомобилях, а Тима Кука не сажают под арест за то, что продукцию Apple используют террористы? И почему арестовали Дурова, а не Цукерберга, у которого есть WhatsApp, а также мессенджер из заблокированной в РФ соцсети? Неужели в них нет противоправного контента? Или всё дело в том, что остальные уже «отдали ключи шифрования» и согласились на сотрудничество?

КТО ВИНОВАТ?

Если подвести итог сказанному, ситуация с безопасностью мессенджеров крайне непростая:

- сквозное шифрование есть, и оно действительно защищает переписки, но это мешает спецслужбам и правоохранителям;
- спецслужбы используют для слежки анализ интернет-трафика и метаданных, а также уязвимости в мессенджерах;
- когда требуется прочитать переписки и выяснить личности, благодаря законам о личной ответственности можно надавить на владельцев платформ и получить желаемое;
- владельцы платформ пытаются сохранить лицо, повторяя лозунги о защите данных и конфиденциальности, но вынуждены сотрудничать, поскольку под угрозой личная безопасность и благополучие.

Искать виноватых в текущих обстоятельствах вряд ли целесообразно. Мир изменился, и технологическим платформам приходится подстраиваться, чтобы выжить, сохранить и приумножить пользовательскую базу.

ЧТО С ЭТИМ ДЕЛАТЬ?

Безопасность мессенджеров — повод для горячих споров, поскольку существует несколько категорий заинтересованных лиц. Приоритет для пользователей — конфиденциальность. Они хотят быть уверенными, что их личные сообщения защищены от посторонних глаз, что они могут свободно общаться без страха за нарушение своей приватности. Важный инструмент для достижения этой цели — сквозное шифрование.

С другой стороны, правоохранительные органы сталкиваются с реальными вызовами в борьбе с преступностью и терроризмом. Они утверждают, что доступ к перепискам может быть жизненно необходим для расследования преступлений и обеспечения общественной безопасности. Для них сквозное шифрование становится препятствием, которое усложняет выполнение их обязанностей по защите граждан.

Владельцы платформ для обмена сообщениями находятся в непростой ситуации между этими двумя противоположными позициями. Они стремятся обеспечить своим пользователям высокий уровень безопасности и конфиденциальности, но в то же время подвергаются давлению со стороны государственных органов, которые требуют доступ к данным пользователей. У владельцев платформ возникает вполне логичный вопрос: почему они должны нести ответственность за противоправные действия пользователей?

Пока идут дискуссии, жизнь не стоит на месте. Баланс между потребностью в конфиденциальности и запросами органов правопорядка требует тщательного рассмотрения и сотрудничества всех вовлечённых сторон. Возможно, через какое-то время получится найти решения, которые будут учитывать интересы всех участников и обеспечат как безопасность общения пользователей, так и эффективную работу правоохранительных органов. А пока можно вспомнить проверенные временем средства защиты конфиденциальности:

1. Общайтесь только с теми, кто не станет использовать ваши сообщения вам во вред.
2. Конфиденциальные вопросы обсуждайте только с теми, кому доверяете.
3. Для обсуждения важных или чувствительных тем встречайтесь лично. Это исключает риск перехвата сообщений. Визуальный контакт помогает лучше понять намерения собеседника и избежать недоразумений.
4. Если личная встреча невозможна, используйте эзопов язык, кодовые слова и фразы, чтобы защитить содержание разговора от посторонних. Это особенно полезно при обсуждении конфиденциальных вопросов, когда велика вероятность перехвата сообщений.
5. Придерживайтесь принципа минимально необходимой передачи данных. Не делитесь лишней информацией даже с близкими. Чем меньше информации вы раскрываете, тем меньше шансов, что она будет использована против вас.
6. Регулярно проверяйте свои контакты и настройки приватности в мессенджерах. Убедитесь, что доступ к вашей информации имеет только тот круг лиц, которому вы доверяете.

ПРИКАЗАНО СЛУШАТЬ

ДОКУМЕНТЫ О ПОДСЛУШИВАНИИ ПРОТИВНИКА ВО ФРОНТОВЫХ УСЛОВИЯХ

Борис СТОЛПАКОВ
историк криптографии

Тема подслушивания телефонных переговоров неприятеля по проводной связи не отличалась новизной в годы Великой Отечественной войны. Ведь подслушивание с помощью технических средств активно и эффективно применялось ещё на фронтах Первой мировой войны. Вместе с тем ценность своевременной информации о противнике заметно выросла.

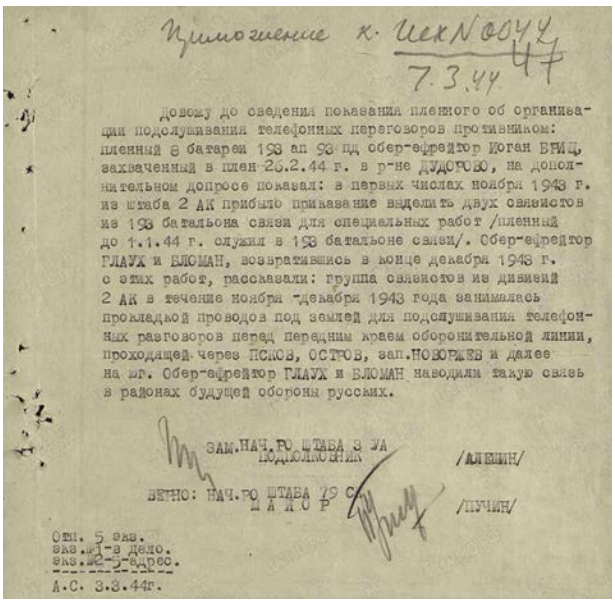
ПОКАЗАНИЯ ПЛЕННОГО

«Пленный обер-ефрейтор Иоган Брич, захваченный в плен 26.2.44 г. в р-не Дудорово, на дополнительном допросе показал: в первых числах ноября 1943 г. из штаба 2 АК прибыло приказание выделить двух связистов из 193 батальона связи для специальных работ (пленный до 1.1.44 г. служил в 193 батальоне связи). Обер-ефрейтор Глаух и Бломан, возвратившись в конце декабря 1943 г. с этих работ, рассказали: группа связистов из дивизий 2 АК в течение ноября-декабря 1943 г. занималась прокладкой проводов под землёй для подслушивания телефонных разговоров перед передним краем оборонительной линии, проходящей через Псков, Остров, зап. Новоржев и далее на юг. Обер-ефрейтор Глаух и Бломан наводили такую связь в районах будущей обороны русских.

Зам. нач. РО штаба 3 УА подполковник Алешин» (илл. 1).

В этом документе речь шла об обустройстве для подслушивания оборонительной немецкой линии «Пантера» в Псковской области. Такие сведения сообщались командному составу наступавших частей Красной армии.

В доступных ныне документах встречаются подробные и обстоятельные описания.



Приложение к Шех № 0044
7.3.44

Довожу до сведения показания пленного об организации подслушивания телефонных переговоров противником:
пленный 8 батареи 198 ап 98 пд обер-ефрейтор Иоган БРИЦ, захваченный в плен 26.2.44 г. в р-не ДУДОРОВО, на дополнительном допросе показал: в первых числах ноября 1943 г. из штаба 2 АК прибыло приказание выделить двух связистов из 198 батальона связи для специальных работ /пленный до 1.1.44 г. служил в 198 батальоне связи/. Обер-ефрейтор ГЛАУХ и БЛОМАН, возвратившись в конце декабря 1943 г. с этих работ, рассказали: группа связистов из дивизий 2 АК в течение ноября-декабря 1943 года занималась прокладкой проводов под землей для подслушивания телефонных разговоров перед передним краем оборонительной линии, проходящей через ПСКОВ, ОСТРОВ, зап.НОВОРЖЕВ и далее на юг. Обер-ефрейтор ГЛАУХ и БЛОМАН наводили такую связь в районах будущей обороны русских.

ЗАМ.НАЧ.РО ШТАБА 3 УА
ПОДПОЛКОВНИК /АЛЕШИН/

ВЕРНО: НАЧ.РО ШТАБА 29 С
МАЙОР /ПУЧИН/

Отп. 5 экз.
Экз.№1-в дело.
Экз.№2-5-адрес.
А.С. 3.3.44г.

Иллюстрация 1. Сообщение о показаниях пленного об организации подслушивания

ТРОФЕЙНЫЕ ФИНСКИЕ ДОКУМЕНТЫ

Далее приведены документы финской 5-й пехотной дивизии, дислоцированной до начала наступления Красной армии в июне 1944 г. в Карелии, на восточной стороне Ладожского озера.

«Штаб 5 дивизии 7.12.43.

Содержание: О формировании взвода подслушивания.

Основание: Приказы штаба 6 АК и Главной квартиры.

1. На основании упомянутых приказов для лучшего добывания сведений о противнике, при 1 роте 23 б-на связи создаётся взвод подслушивания.

2. Организация и численный состав взвода подслушивания даны в приложении № 1.

3. Во взвод подслушивания переводятся следующие лица...

4. Формирование взвода подслушивания возлагается на начальника связи 5 пд.

5. Подготовку личного состава начать немедленно после сформирования взвода подслушивания. Использовать для обучения имеющиеся в дивизии средства подслушивания.

6. Имеющиеся на участке дивизии станции подслушивания продолжают по-прежнему свою работу.

7. По вопросу об организации службы подслушивания приказываю: Начальник связи 5 пд. Ему в командном отношении подчиняется взвод подслушивания. Он отвечает за техническое состояние службы подслушивания. Выбирает места расположения станций подслушивания в полосе обороны дивизии и указывает их начальнику 2 отделения штаба. По указанию начальника 2 отделения штаба даёт приказания на пе-

ремену мест расположения станций подслушивания. Обрабатывает шифровки. Руководит подслушиванием телеграфных и радиопередач. Передаёт полученные им данные подслушивания начальнику 2 отделения...

Личный состав взвода подслушивания 1 роты 23 б-на связи: Командир взвода, пом. командира взвода (владеет русским языком), 1 и 2 группы подслушивания телефонной связи — по 4 чел., группа подслушивания радиопередач — 4 чел.»

Комментарий РО фронта:

«Показаниями ряда пленных, захваченных на Карельском фронте в период 1941–1944 гг., было установлено наличие в финской армии службы подслушивания. Однако данных об организационной структуре подразделений подслушивания не было. Настоящим приказом установлено создание в конце 1943 г. взвода подслушивания в 5 пд.

Взвод подслушивания в командном отношении подчиняется начальнику связи дивизии, а в оперативном отношении — начальнику 2 отделения штаба дивизии (2 отделение — оперативно-разведывательное).

Станциями подслушивания составляются ежедневные донесения, отправляемые в штаб соответствующего соединения. В штабах дивизий, бригад составляются двухнедельные обзоры подслушанных переговоров».

Обзор данных подслушивания телефонных разговоров пр-ка в период с 29.11 по 13.12.43

«В период с 29.11 по 13.12.43 пр-к не проявлял активности и вёл мало разговоров по телефону. Это вызвано, по-видимому, общим затишьем, которое наблюдается в последнее время на подслушиваемом участке. Это затишье заставило пр-ка чего-то ожидать. Так, например, 3.12 в 0.30 один из офицеров штаба 2 б-на 763 пп (по-видимому, капитан Московский) сказал, что это затишье предвещает бурю. 29.11 пр-к был обеспокоен и давал часовым указания усилить бдительность. Это могло быть вызвано проверкой, которая в это время проходила на переднем крае. В проверке участвовал некий Румянцев.

Изменений в группировке пр-ка не отмечено. Изучением данных, полученных от пленных и путём подслушивания, установлено, что находящаяся в р-не жел. дороги отд. рота (к-р роты капитан Рудковский) предположительно является 1 ротой 425 арт. — пулемётного б-на. Рота направляет снайперов и разведпартии на передний край.

Пр-к тщательно наблюдает за выпускаемыми нами ракетами и ежедневно сообщает количество и цвет выпущенных на данном участке ракет.

Пр-к также следит за нашим огнём и оборонительными работами. Он продолжает называть своих наблюдателей „глазами“ и снайперов — “охотниками“. Пока что не установлено, что он называет „ушами“, но, по-видимому, это выставленные вперёд дозоры подслушивания или аппарат подслушивания.

О пище ежедневно ведутся разговоры. Но высказывания о её качестве или количестве не было... Содержание писем также не установлено. 8.12 из тыла на передний край отправили некоторое количество лыж. В настроениях личного состава пр-ка никаких изменений не отмечено...

Позывные пр-ка менялись в 24.00 30.11 и часть из них во второй половине дня 8.12. Смена позывных продолжает вызывать путаницу...»

Обзор данных подслушивания в период с 13.12 по 29.12.43

«С 19.12 по 29.12 подслушивать разговоры пр-ка не удалось, так как аппарат для подслушивания был в неисправности.

Телефонных разговоров на переднем крае пр-ка в радиусе действия аппаратов подслушивания велось мало. Причиной, по-видимому, являлись отсутствие разведки и слабая активность арт. мин. огня. На основании подслушанных разговоров можно

ПЕРЕГОВОРЫ ПРОТИВНИКА ПО ПОВОДУ ЗАХВАТА ИМ В ПЛЕН МЛ. СЕРЖАНТА ЛЕЙНО

Откуда	Куда	Время	Кто говорит	Содержание разговоров
Лена (2 б-н)	Волга (6 рота)	6.18	Волга	...Он ранен, мы убираем всех отсюда.
Волга	Лена	6.19	Волга	Скажите, чтобы он быстро вызвал Мага (карел, который работает переводчиком, данные от военнопленных). Он тяжело ранен и может умереть.
Лена	Волга	6.21	Лена	Пошлите Артюка бегом сюда. Давайте вашего переводчика Мага. Пришлите его (раненого) на лошади и быстро доставьте сюда к Московскому (к-р 6 роты).
Лена	Огонь	6.42	Лена	Где 37 так долго задерживается? Его просят к телефону.
			37	Ваше приказание выполнено. Документы доставлены. Его (наш раненый мл. сержант) доставят к Вам сейчас. Доложил 37.
			37	Только что сообщили, что он скончался (захваченный мл. серж.)

Таблица 1. Выписка из донесения «КОУККУ» (примечание РО: станция подслушивания) №115 от 30.10.43

сделать вывод, что миномётный огонь противника очень ограничен. 13.12 из б-на не могли дать разрешения на обстрел группы наших солдат, производящих оборонительные работы. Раньше пр-к обстреливал из миномёта даже одиночных солдат».

Обзор данных подслушивания на период от 25.1 по 27.1.44

«Станция подслушивания „Матти“, расположенная на опорном пункте „Мари“(участок Карелки), начала работать 18.1.44 после выпрямления линии переднего края. До отхода на новые позиции на оставляемой территории были протянуты веерообразно 8 усов (полевой кабель) и железный шест. В частично разрушенной землянке были оставлены микрофоны, и от них были протянуты подземные провода.

В начале своей работы станция могла слушать все наши телефонные разговоры от переднего края до глубины Олонца. В 4.25 25.1 был подслушан первый разговор пр-ка, и с тех пор слышимость продолжает оставаться хорошей, не считая помех от плохой погоды.

Рано утром 25.1 пр-к выдвинулся на оставленную нами территорию; при этом он поддерживал телефонную связь со своим передним краем. Станция подслушивания отметила работу 7–8 разных телефонных точек. По подслушанным разговорам мы могли следить за продвижением пр-ка и узнали маршруты разных групп. При подходе пр-ка к нашему переднему краю мы смогли подслушать замечания пр-ка о нём. По разговорам с арт. НП пр-ка мы засекли его и обстреляли.

Из подслушанных 26 и 27.1 разговоров мы узнали, что пр-к направил небольшие разведпартии к разным пунктам нашего переднего края. Разведпартии действовали ночью и имели телефонную связь со своим передним краем. По степени слышимости и по разговорам участников разведпартии мы могли сравнительно точно определить их местонахождение и предупредить об этом свои опорные пункты.

О частях и группировке пр-ка не удалось добыть сведений, так как дисциплина связи у пр-ка очень строгая и лица, ведущие переговоры, ещё не выявлены. Все переговоры очень коротки и закодированы. Делаются предупреждения о соблюдении осторожности при переговорах».

Общий вывод РО

«Переведёнными обзорами установлено, что дисциплина телефонных переговоров в подразделениях дивизии, стоявшей в ноябре-декабре 1943 г. против 5 пд финнов, была на низком уровне.

Условные термины („глаза“, „охотники“), используемые при наших телефонных переговорах, легко расшифровывались. Новые позывные не всегда доводились до сведения тех, кому приходилось ими пользоваться. Отношение к сохранению тайны позывных было небрежным.

Противнику, благодаря службе подслушивания, удаётся выявлять группировку наших войск, офицерский состав, время и районы действий разведпартий, засекать расположение наших НП, а также получать ряд других ценных разведывательных данных.

Начальник РО Штафронта подполковник Задвинский»

1.8.44

О РАДИОПОДСЛУШИВАНИИ ПРОТИВНИКОМ

В архивных документах есть свидетельства о случаях радиоподслушивания. Удобный момент для попыток радиоподслушивания противником настал в начале 1942 г. Тогда, в ходе наступления Красной армии, её войска стали занимать оставленные немцами территории под Москвой. Об эпизоде радиоподслушивания штаб Западного фронта известил армейские штабы (илл. 2).

По проводу

«Начальникам штабов армий

Сообщаю о найденном приборе радиоподслушивания в районе действий 5 армии. 5.3.42 г. сапёрами 499 армейского инж. батальона найден на дереве радиоприбор противника. По предварительным данным, прибор служит для целей радиоподслушивания.

При разговоре бойцов, командиров около этого прибора противник открыл миномётный огонь по этому району. Специалисты-радисты при внешнем осмотре прибора подтверждают правильность его назначения.

Войскам дать указания о принятии мер по тщательному осмотру районов расположения КП, артпозиций, сосредоточения войск, танков.

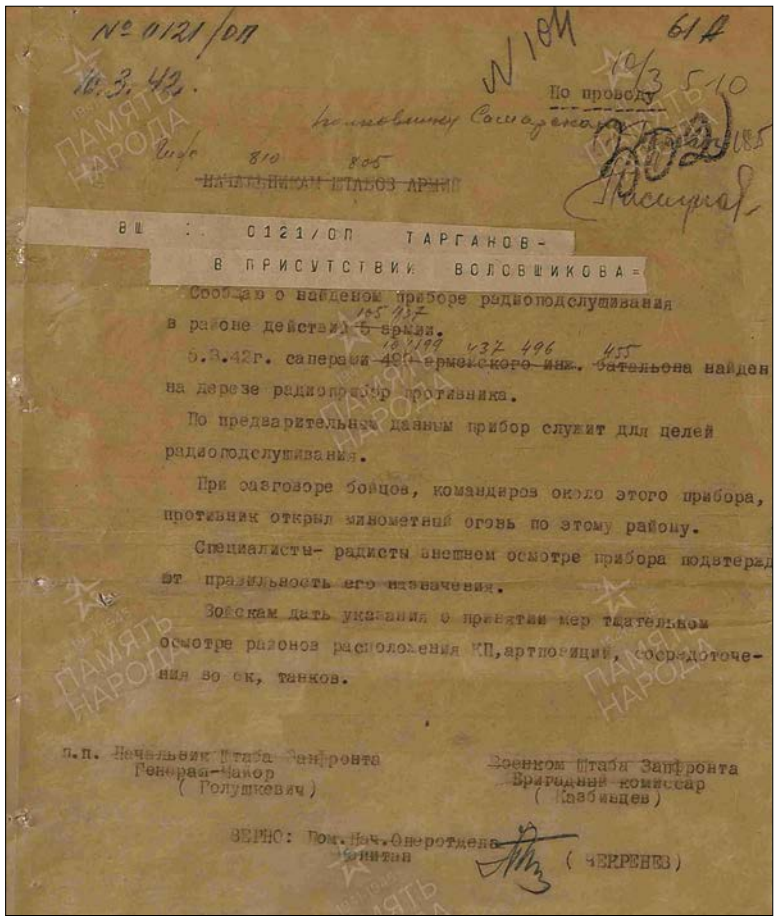
Начальник Штаба Запфронта генерал-майор Голушкевич»

ОПЕРАТИВНЫЕ ОТДЕЛЫ ИНФОРМИРОВАЛИ ПОДРАЗДЕЛЕНИЯ

Армейские оперативные отделы рассылали появляющиеся материалы о подслушивании для информирования подразделений. На илл. 3 приведён документ такой рассылки материала «по подслушиванию противником телефонных переговоров для доведения его до всего офицерского состава». Он адресован частям 200 и 219 стрелковых дивизий, которым предстояло преодолеть немецкую оборонительную линию на реке Великой в Псковской области.

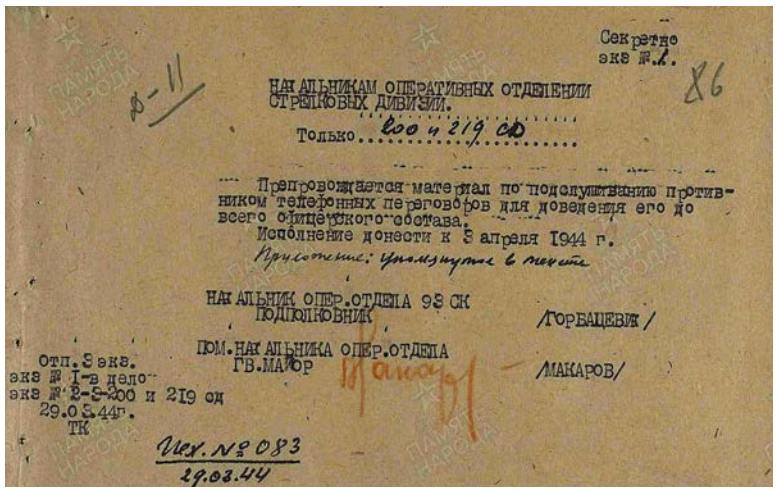
В ДОЛГУ НЕ ОСТАВАЛИСЬ

Попытки подслушивания, несомненно, были взаимными. Пример тому — документ Волховского фронта «Материал по подслушиванию телефонных переговоров противника в 265 сд 8 армии», относящийся ко времени прорыва блокады Ленинграда (18 января 1943 г.). При прорыве блокады эта стрел-



№ 0121/оп
10.3.42.
По проводу
Начальнику Разведотдела
Начальник штаба 3 АРМИИ
ВЦ : 0121/ОП ТАРГАНОВ-
В ПРИСУТСТВИИ ВОЛОВЩИКОВА-
Сообщаю о найденном приборе радиоподслушивания
в районе действий 6 армии.
5.3.42г. саперами 45-го армейского инж. батальона найден
на дереве радиоприбор противника.
По предварительным данным прибор служит для целей
радиоподслушивания.
При разговоре бойцов, командиров около этого прибора,
противник открыл минометный огонь по этому району.
Специалисты- радисты внешнем осмотре прибора подтверд
ют правильность его назначения.
Войскам дать указания о принятии мер тщательном
осмотре районов расположения КП, артпозиций, сосредоточе-
ния пех ск, танков.
п.п. Начальник Штаба Запфронта
Генерал-Майор
(Голушкевич)
Военком Штаба Запфронта
Бригадный комиссар
(Кабанцев)
ВЕРНО: Пом. Нач. Оперотдела
капитан
(ЧЕРНЕНЬ)

Иллюстрация 2. Сообщение о радиоподслушивании



Секретно
экз №1.
НАЧАЛЬНИКАМ ОПЕРАТИВНЫХ ОТДЕЛЕНИЙ
СТРЕЛКОВЫХ ДИВИЗИЙ.
Только 100 и 219 СД
Препровождается материал по подслушиванию противником телефонных переговоров для доведения его до всего офицерского состава.
Исполнение донести к 5 апреля 1944 г.
Приложение: упомянуто в тексте
НАЧАЛЬНИК ОПЕР.ОТДЕЛА 93 СК
ПОДПОЛКОВНИК /ГОРБАЦЕВИЧ/
ПОМ.НАЧАЛЬНИКА ОПЕР.ОТДЕЛА
ГВ.МАЙОР /МАКАРОВ/
Отп. 5 экз.
экз № 1-в дело
экз № 2-5-200 и 219 сд
29.03.44г.
ТК
Исх. №2083
29.03.44

Иллюстрация 3. «Препровождается материал по подслушиванию...»

ковая дивизия обеспечивала южный фланг наступления, а затем вела боевые действия, защищая возобновлённое движение железнодорожных эшелонов к Ленинграду.

«1.1.43 ...Новый год, я поздравляю спасибо. Всё хорошее, от жены имею посылочку, опять музыка не громко, да.

2.1.43 ...Аммоний, да? До 3? Наблюдали ли вы что-нибудь? Да? Огонь, огонь эти же самые четырёхугольники, огонь эти же самые квадраты, огонь немного коротко прибавить метров, огонь повторить, огонь несколько метров прибавить. Огонь, приготовиться, огонь, приготовиться. Выстрел, 2 выстрела повторить, перерыв в огне, перерыв в огне, остаться на аппарате. (Разговор совпал с обстрелом минами в районе 3 ср, около 15 часов. За каждой командой следовали действительно выстрелы, затем наступил перерыв). Новый год спасибо, чтобы был хороший год, кто у аппарата кукла, кукла да, да. Зима метров, направление Бодо, Бодо.

4.1.43 Должны находиться в дороге, куда, да. Видите ли вы ещё, я прикажу. Левая рука, именно здесь, да, здесь. Приготовить огонь, приготовить огонь, приготовиться огонь. Совсем немного же, огонь, прибавить метров. Перерыв в стрельбе до 3, что? Да, вижу 50 метров прибавить три, меньше это же самое место. Сильное движение в траншее на 50 метров, огонь. Направление три линии. Огонь это же место на 50 метров меньше, огонь да, огонь, огонь, огонь, винтовочный огонь.

(Подслушивание, проводимое во второй половине января, никакого материала, кроме команд по управлению огнём, не дало)».

«ВСЕ РЯДОВЫЕ ДОЛЖНЫ РАБОТАТЬ»

«13.2.43 12.30 „Все рядовые должны работать“. 13 ч. „Пулемёт работает“. 21.00 „Обратить внимание в случае появления самолётов на обстановку“.

15.2.43 Сегодня выверить, поняли? К вечеру должно быть закончено. Поняли? (Велась корректировка огня).

20.2.43 3.00 Вы всегда должны. 6.00 Я наблюдал, никого в траншеях. Противник ведёт огонь, один человек сгибается, поймать. 6.30 Сегодня удалить дугу. У меня 12 солдат. 13.00 Один солдат убит. 14.45 (Начало разговора было заглушено). Два с кирками. Хотите выйти. Снаружи я вижу человека. Среди белого стоит укрытый. 16.00 В укрытие идёт провод. Два заряда неправильно, дайте три заряда. 17.00 Возьмите крышку и наденьте её. Внесите аппарат в землянку. Донесение послано. 21.00 Знаете, что говорит командир полка».

«Подслушиванием 15.2 установлено: в районе 3801 обороняется рота противника, нумерация которой не установлена. Все остальные данные подслушивания не дали нужных результатов, так как перехватывались отдельные команды и отрывочные фразы. Засады результатов не имели, так как устраивались не в расположении противника, а перед его передним краем. И могли выполнить свою задачу только в случае выдвижения противника за его передний край.

Пом. нач. связи 265 сд капитан Трофимович»

* * *

Казалось бы, незамысловатые сообщения о давно прошедшем времени, а притягивают внимание и будоражат воображение.

SOLAR

SOLAR NGFW

Атакоцентричные технологии для комплексной защиты корпоративной ИТ-инфраструктуры

W: RT-SOLAR.RU

Kaspersky NGFW

- Централизованное управление и XDR-сценарии
- Актуальные глобальные данные Threat Intelligence
- Высокое качество детектирования и предотвращения угроз на ранних этапах

Лидерские технологии сетевой защиты и контроля активности приложений

Узнайте больше про бета-версию решения