В НОМЕРЕ

Константин Масленников,

директор по маркетингу компании
«Инфосистемы Джет»

«Неизведанное для ИБ» — это прежде всего Shadow IT. Тема далеко не нова, первые статьи о Shadow IT появились в JETINFO еще несколько лет назад. Свежий номер впитал в себя все наработки, теории и практики наших экспертов по информационной безопасности и вылился в 9 месяцев подготовки.

COVID-19 окрасил эту тему ИБ в яркий цвет сегодняшней децентрализованной реальности. Никто не может сказать, в какой мере вирус, представляющий угрозу для здоровья людей, повлияет на фишинг, взломы и вирусы компьютерные, а также на угрозы, связанные с BYOD, на распределенные сети предприятий с удаленной работой персонала, на данные, которые растекаются по сотням новых облачных сервисов и сред. Хаос, как известно, сложно измерить. Как следствие, им невозможно эффективно управлять. Вот вам и новый, небывалый по масштабу и спектру вызов для ИБ-специалистов.

Возможно, когда вся эта история с многоуровневым кризисом выйдет на прогнозируемый сценарий развития, мы получим новые термины в ИБ, ИТ и риск-менеджменте. Но уже сейчас понятно, что термины «непрерывность» и «угроза» обретут новый окрас. Это будет не теория от методологов Risk Management, Business Continuity Management и Cyber Security Management, а практика: значения реальных потерь от остановок деятельности вследствие того или иного ИБ-инцидента. Поэтому мне очень близок подход CI/CD: его метод непрерывной поставки можно перефразировать на язык ИБ-шников как Continuous Cybersecurity Monitoring / Continuous Secure Deployment. Только непрерывные анализ защищенности и мониторинг ИТ-активов позволяют ускорить внесение изменений в ИБ-политики компании и осуществлять адекватное ИБ-содействие в развертывании и поддержке всех ИТ-систем. Скажете, дорого? Проигрывать еще дороже, особенно когда цена вопроса сопоставима с потерей компании.

Каждый владелец бизнеса как никогда раньше должен соблюдать баланс между возможностями для развития и ИТ-рисками и ИБ-угрозами, которые они подспудно создают. Этот процесс можно представить в виде уравновешивания чаш весов: если «ставить гири» лишь на чашу возможностей, ИБ-угрозы неминуемо будут реализованы. В то же время кризис диктует свои правила игры: выживает лишь тот, кто умеет гибко и быстро подстраиваться под изменения. Поэтому любая трансформация бизнеса должна сопровождаться адекватными мерами, в том числе со стороны информационной безопасности.

Редакция журнала

Главный редактор **Константин Масленников**
+7 495 411-76-01, ext. 2751, ky.maslennikov@jet.su

Шеф-редактор **Анастасия Дискина**
+7 495 411-76-01, ext. 2397, journal@jet.su

Корректор **Ирина Карпушина**
journal@jet.su

Арт-директор **Денис Масягин**
journal@jet.su

Ведущий аналитик **Ольга Пахтанова**

Фотографы
Иван Оноприенко
Андрей Смирнов

Ментор проекта **Александр Зисман**

Директор проекта **Владимир Елисеев**

Авторы и эксперты

А. Акопян, Д. Волков, П. Волчков, А. Гаврилов, Д. Гадарь, А. Дитенкова, П. Дрейгер, О. Елисеева, М. Иванов, Д. Каросанидзе, Д. Ключников, И. Костин, М. Кусакина, И. Павлова, М. Романычева, В. Сиянов, В. Соленик, Г. Старостин, Е. Тарасова, М. Филиппов, С. Фомиченко, Л. Храмова, А. Черных, А. Янкин

Сотрудничество и реклама

Анастасия Дискина
journal@jet.su

Адрес редакции

127015, Россия, Москва,
ул. Большая Новодмитровская, 14, стр. 1,
бизнес-центр «Новодмитровский»

Отпечатано в типографии

«Ситипринт»,
129226, г. Москва, ул. Докукина, 10, стр. 41

Тираж

3000 экз.

16+

Журнал издается с 1995 г. компанией «Инфосистемы Джет»

Издание JETINFO зарегистрировано в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций *(Роскомнадзор)*. Свидетельство о регистрации средства массовой информации ПИ № ФС 77-77514 от 25 декабря 2019 г.

https://www.facebook.com/jetinfosystems.online/

https://www.youtube.com/user/JetITTube

https://t.me/jetinfo

https://vk.com/jet_integration

https://habr.com/ru/company/jetinfosystems/

JET CSIRT

КОМПЛЕКСНЫЙ СЕРВИС МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИБ

МОНИТОРИНГ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИБ

ЭКСПЛУАТАЦИЯ И ТЕХНИЧЕСКАЯ ПОДДЕРЖКА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ЭКСПЕРТНЫЕ СЕРВИСЫ ИБ ПО МОДЕЛИ SECURITY AS A SERVICE (MSSP)

Лицензия ФСТЭК России

Соглашение с НКЦКИ об организации взаимодействия с ГосСОПКА и ФинЦЕРТ

Сертификация по ГОСТ Р ИСО/МЭК 27001:2006 и ISO/IEC 27001:2013

Инфосистемы Джет
csirt@jet.su
csirt.jet.su

* Должность и место работы спикера на момент публикации.

АВТОР
Андрей Янкин,
директор Центра информационной безопасности компании «Инфосистемы Джет»

/ О ЧЕМ ЧАЩЕ ВСЕГО ЗАБЫВАЕТ БЕЗОПАСНИК / ГДЕ ИСКАТЬ SHADOW IT / ЧТО ЕСТЬ ИНТЕРЕСНОГО ВЫШЕ L7 ISO/OSI

Shadow IT

Невидимые для ИТ- и ИБ-департаментов решения, используемые в подразделениях/филиалах компаний самостоятельно, без уведомления и привлечения соответствующих специалистов

Классическая ИТ-безопасность так сосредоточена на технике, что ей порой кажется, что за пределами ее привычного скоупа ничего нет. Системы, не переданные на мониторинг, люди со своими интересами и коммуникациями, хитросплетения бизнес-процессов и новые технологии, для которых нет типовых ИБ-решений, — все это оказывается в серой зоне. В серой, а не черной, потому что обо всем этом вообще-то в общих чертах известно, но разбираться совершенно не хочется. Это тот самый «выход из зоны комфорта», который сулит ИТ-безопасникам не только непривычную работу, но и зачастую недовольство коллег и выходные в офисе.

Вообще говоря, в эту «зону дискомфорта» можно и не заходить, если в организации ограничиваются выполнением формальных ИБ-требований *(внешних регуляторов или внутренних стандартов)*. Система защищена по требованиям ФСТЭК, аттестована — и значит, в любом случае компании не придется нести ответственность. Если такой подход неприменим и нужно строить ту самую real security, то придется поднапрячься, в том числе разобраться с «неизведанным» в своей ИТ-инфраструктуре.

«Неизведанное» — это прежде всего Shadow IT (стр. 10). Системы, о которых просто неизвестно безопасникам, а порой и службе ИТ. По нашему опыту, они есть в любой мало-мальски крупной организации. Это и неконтролируемые тестовые системы, и забытые при инвентаризации ИС

ОБЪЕМ СТР.

ят на ИБ

в далеких филиалах, и подключенные системы многочисленных подрядчиков. Это зачастую самая легкая добыча для хакеров и вредоносного ПО. Зачем ломать защищенные серверы, если рядом стоит MS SQL 2003, которая не обновлялась ни разу с момента установки в прошлом десятилетии? Зачем пробираться через корпоративную сеть в АСУ ТП, если подрядчик поднял в технологическом сегменте виртуалку с удаленным доступом из Интернета? Зачем изучать уязвимости сайта за WAF, если на соседнем IP развернута его тестовая версия без всякой защиты и мониторинга? Это все невыдуманные истории. В рамках наших пентестов мы сталкиваемся с такими ситуациями постоянно.

ОБЛАЧНЫЕ СЕРВИСЫ

Отдельный крупный блок Shadow IT — всевозможные облачные сервисы. Сколько различных облачных сервисов используется в вашей организации? Три, пять, десять? На практике анализ трафика в компании обычно сходу находит их более сотни. Браузеры сливают в облака историю посещений и сохраненные пароли, приложения шлют разработчикам логи и скачивают обновления, пользователи сами сохраняют рабочие файлы на личных Google Drive и Dropbox, чтобы поработать из дома. И все это набито конфиденциальной информацией.

Был случай, когда ИТ- и ИБ-службы в одном из банков с суровыми требованиями в части Information Security лишь спустя несколько лет узнали, что департамент продаж закупил подписку и поголовно использует облачную CRM. Причем никто и не пытался скрывать этот факт.

Серебряная пуля от таких проблем существует. Это полное отключение Интернета. Но такой серебряной пулей в большинстве случаев можно только застрелиться. Анализ и частичная блокировка облачных сервисов могут быть эффективными, хотя это совсем непросто без специализированных технических средств. Но желательно сопровождать их предоставлением пользователям удобных защищенных аналогов *(почитайте, например, про Virtual Data Rooms)*.

ЖИВЫЕ ЛЮДИ

Один мой преподаватель, ветеран органов государственной безопасности, любил говорить, что плохой безопасник работает с техникой, а хороший — с людьми. Потом мне не раз приходилось убеждаться в его правоте.

Сотрудникам экономической и физической безопасности обычно эта область куда привычнее и понятнее, чем ИБ-шникам. Если удалось выстроить с ними коммуникации, то ИБ становится заметно эффективнее. Доходит до смешного. На территории обнаружен хакер. Что делать? Когда в роли хакера выступает наш пентестер, в одном случае из пяти ИБ-шники более-менее понимают, как действовать. В основном это выглядит примерно так:

ПЛОХОЙ БЕЗОПАСНИК РАБОТАЕТ С ТЕХНИКОЙ, А ХОРОШИЙ – С ЛЮДЬМИ.

— Перестаньте нас ломать! Что вы делаете? Кто вас сюда пустил?

— Я ничего не делаю. Я обновляю 1С.

— ...Уходите!

— Хорошо. [Пентестер берет ноутбук и уходит.]

Да и утечка данных из ИТ-системы может происходить вообще без использова-

УЧИТЬСЯ НА ЧУЖИХ ОШИБКАХ – СКУЧНО. ПОЭТОМУ РАЗ ЗА РАЗОМ ПОВТОРЯЕТСЯ СИТУАЦИЯ, КОГДА НОВАЯ ТЕХНОЛОГИЯ СТРЕМИТЕЛЬНО НАБИРАЕТ ПОПУЛЯРНОСТЬ, А ПОТОМ ПОСЛЕ МАССОВЫХ ВЗЛОМОВ ЕЕ СОЗДАТЕЛИ И ЭКСПЛУАТАНТЫ НАЧИНАЮТ ЛОМАТЬ ГОЛОВУ НАД ТЕМ, КУДА ТУТ ПРИКРУТИТЬ БЕЗОПАСНОСТЬ.

ния компьютерных атак и взломов. Переписывание конфиденциальной информации в блокнотик никто не отменял. Является ли это проблемой ИБ-шников? Проблемой компании является точно.

Средства защиты пытаются учитывать особенности взаимодействия и поведения живых людей. Такие концепции активно внедряются в DLP, UBA-системы. Производители часто утверждают, что системы эти самообучаемы и не требуют настройки офицером ИБ. Практика показывает, что это совершенно не так. Анализ и постоянная ручная донастройка требуются, но результат может того стоить. Тут зачастую выявляются не классические сливы информации, а различные коррупционные и мошеннические схемы.

Здесь нельзя не упомянуть и концепцию People Centric Security. Это попытка вовлечь в решение проблем ИБ информированных об ИБ-рисках сотрудников, чтобы, с одной стороны, хоть немного снизить эффективность социальной инженерии, а с другой — лучше адаптировать безопасность под требования и специфику бизнеса. Эта тема обширна, но в Интернете по ней можно найти немало практических материалов *(только избегайте вендорских интерпретаций концепции: они обычно слишком узки и ограничиваются возможностями конкретного продукта)*.

БИЗНЕС-ПРОЦЕССЫ

Выше L7 модели ISO/OSI, кроме людей, есть много другого, что может быть полезно для обеспечения информационной безопасности. В частности, это бизнес-процессы и прикладные системы, которые их реализуют. Внедрение контролей безопасности на этом уровне может стать крайне эффективной мерой защиты, когда остальные уже преодолены.

Пару лет назад на «Противостоянии» *(командная игра по взлому и защите информационных систем в рамках ежегодной конференции Positive Hack Days)* одна из наших команд защищала банк, где не использовались средства защиты и преднамеренно было внедрено большое число уязвимостей. Для блокировки несанкционированных транзакций применялась только антифрод-система. В итоге за 2 дня больше 10 команд хакеров не смогли подобрать параметры транзакций так, чтобы украсть хотя бы одну копейку со счетов «мирных граждан», переводы которых продолжали проходить.

Блокировки подозрительных с точки зрения бизнес-логики активностей кажутся очевидным и эффективным шагом, однако реализуются очень редко. Исключением, возможно, является только контроль банковских операций. Сложности очевидны: тут и риски сбоев, и необходимость вовлекать в разработку контролей людей, ничего не понимающих в вопросах ИБ, но разбирающихся в бизнес-процессах, и ограниченные возможности прикладных систем. Но игра определенно стоит свеч.

НОВЫЕ ТЕХНОЛОГИИ

Учиться на чужих ошибках — скучно. Поэтому раз за разом повторяется ситуация, когда новая технология стремительно набирает популярность, а потом после массовых взломов ее создатели и эксплуатанты начинают ломать голову над тем, куда тут прикрутить безопасность. Эта история была с компьютерными сетями, Интернетом, смартфонами, IoT, blockchain и повторится в будущем еще не раз.

Бизнес пытается как можно скорее внедрить новинки для получения конкурентных преимуществ, и у безопасника тут есть три пути: ничего не замечать, запретить или пытаться хоть как-то защищать. К сожалению, третий путь часто дает не больше безопасности, чем первый, из-за отсутствия в природе встроенных или наложенных СЗИ для новой технологии.

Хорошие примеры последних лет — DevOps (стр.68), контейнеризация и Big Data (стр.30). До недавнего времени просто не существовало эффективных средств обеспечения безопасности технологий этих классов. В итоге огромные объемы конфиденциальной информации стекались в совершенно незащищенные озера данных, а процесс разработки и эксплуатации приложений был для безопасников темным лесом.

Остается «учиться, учиться и еще раз учиться», а также стараться включить требования ИБ в процесс принятия решений о внедрении новых технологий. Практика показывает, что если безопасники при этом не пытаются всеми силами помочь «инноваторам», а просто запрещают все подряд, то очень скоро их от этого процесса оттесняют.

КАК ЖИТЬ ДАЛЬШЕ?

Вполне очевидно, что полностью устранить эту серую зону, состоящую из Shadow IT и нетехнических факторов, в крупной организации невозможно. Это не значит, что борьба безопасников со злоумышленниками обречена на провал.

Можно посоветовать, во-первых, не жить в мире иллюзий и построенных на них моделей защиты идеальной ИТ-инфраструктуры, изображенной в проектной документации пятилетней давности. Как говорится, безопасность начинается с инвентаризации (стр.26) или не начинается вовсе. Инвентаризация эта должна быть всесторонней и непрерывной.

Во-вторых, рекомендуется постоянно расширять зону контроля как в ИТ-инфраструктуре, так и на уровне логики бизнес-процессов, контроля лояльности и т.п. Мы никогда не добьемся полного покрытия, но здесь стоит вспомнить о концепции Cyber Kill Chain. Атака обычно проходит несколько стадий — начиная с разведки и заканчивая вредоносными действиями и заметанием следов.

КОНЦЕПЦИЯ CYBER KILL CHAIN

Идеальный сценарий — детектировать и пресечь атаку как можно раньше, но в целом обнаружить и сорвать ее можно на любом этапе. Если заражение прошло через не контролируемый нами хост, то мы можем отловить трафик от зараженной машины до командного центра на уровне сети. Если мы недостаточно качественно проверяем новых работников, то есть надежда на то, что антифрод-система вовремя заметит и заблокирует слив базы клиентов. Таких примеров можно привести много. При этом, расширяя зону контроля, мы должны уметь выбрать главное и чем-то пожертвовать, чтобы не захлебнуться в потоках логов и не разориться на лицензиях SIEM или оплате услуг аутсорсеров.

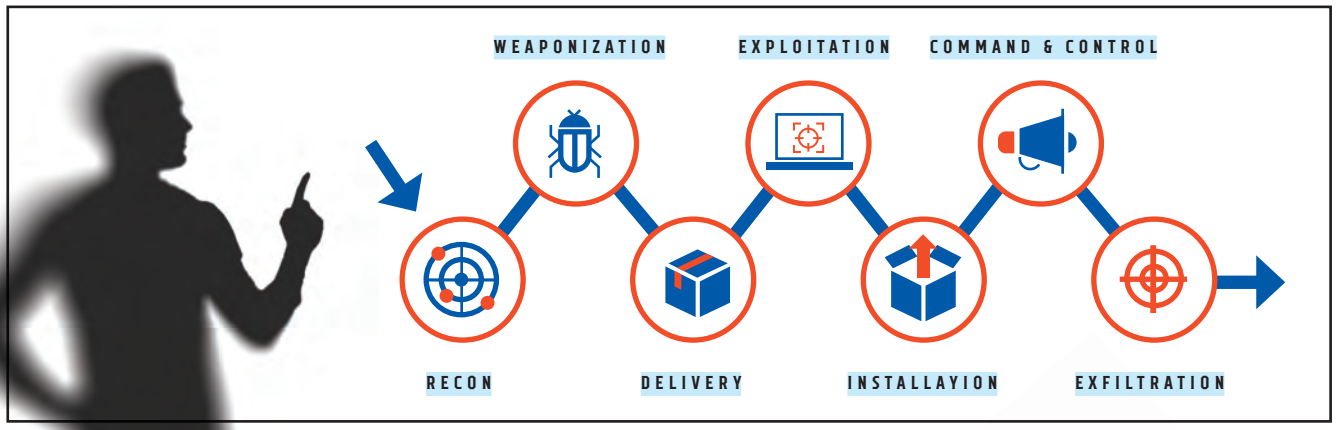
На мой взгляд, умение и желание искать, ставить на контроль и защищать «неизведанное» для безопасника чуть ли не важнее всех прочих навыков. В этом номере JETINFO мы постарались нащупать основные направления, куда стоит копать, чтобы безопасность не была похожа на сурового, но слепого и глухого сторожевого пса.

Cyber Kill Chain

Модель жизненного цикла кибератак, систематический процесс достижения ИБ-нарушителем цели для получения желаемого эффекта

АНДРЕЙ ЯНКИН

График 1 Концепция Cyber Kill Chain



АВТОР

Георгий Старостин,

эксперт лаборатории практического анализа защищенности компании «Инфосистемы Джет»

Как минимизировать угрозу Shadow IT

/ ЧТО МОЖЕТ УЗНАТЬ О КОМПАНИИ ЗЛОУМЫШЛЕННИК, ВЗЛОМАВШИЙ СКУД

/ КАКИЕ ЛИЧНЫЕ ДЕВАЙСЫ СОТРУДНИКОВ ОСОБЕННО ОПАСНЫ С ТОЧКИ ЗРЕНИЯ ИБ

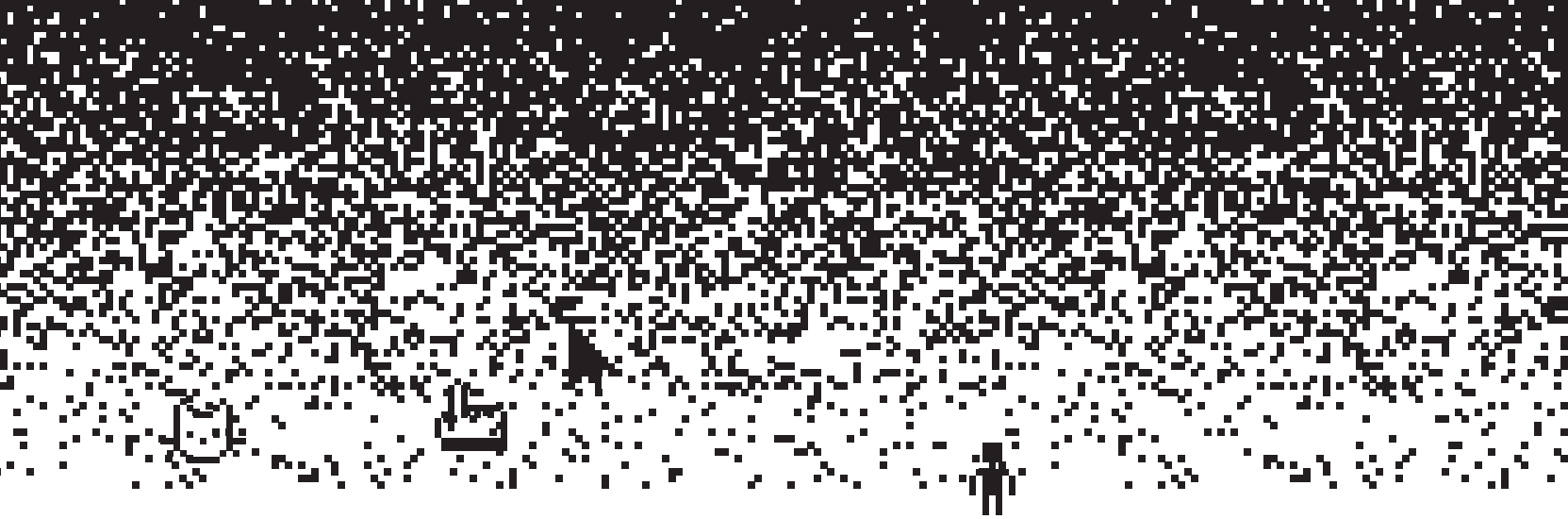
/ МОЖЕТ ЛИ SHADOW IT СТАТЬ ПРИЧИНОЙ ОСТАНОВКИ ЗАВОДА

Shadow IT — часть ИТ-инфраструктуры компании, которая находится вне поля зрения ИТ- и ИБ-служб. Во время пентестов мы регулярно находим и используем подобные системы для проведения атак, потому что они слабо защищены.

Мы легко получаем доступ к СКУД и системам видеонаблюдения заказчиков: их ОС и ПО обычно не обновляются по несколько лет, а значит, там есть критические уязвимости. Таким образом можно узнать много интересного о сотрудниках: ФИО, номера пропусков, график прихода и ухода. Если СКУД и видеонаблюдение входят в домен Active Directory, через них можно получить данные и о других системах компании. Зачастую именно они становятся плацдармом для развития атаки.

Внутренние самописные системы, развернутые без ведома ИТ- и ИБ-департаментов, тоже почти всегда имеют критические уязвимости. Они плохо задокументированы и в целом ненадежны. Их можно быстро взломать и использовать как прокси-серверы во время атаки.

Проблема бесхозных систем и устройств обычно возникает после модернизации ИТ-инфраструктуры. Старые решения выводятся из эксплуатации, но забытые серверы, коммутаторы и прочее оборудование продолжают работать. Мы находили в сетях заказчиков бесхозные устройства с аптаймом в 6,5 года! Один из самых интересных кейсов — старый сервер СКУД на Windows Server 2003 с данными администратора домена, который располагался в сегменте гостевой Wi-Fi-сети. Взломать его не составило труда, а полученный пароль подошел



SHADOW IT В КОМПАНИЯХ

Системы, в обслуживании которых не участвуют ИТ- и ИБ-подразделения. Например, СКУД и видеонаблюдение, за эксплуатацию которых обычно отвечают другие отделы. Они не допускают ИТ-шников к оборудованию, не следят за защитой и редко устанавливают обновления.

Бесхозные системы и железо. Часто появляются при модернизации ИТ-инфраструктуры и могут много лет работать «в тени», обрастая уязвимостями.

Самописные системы, о которых не знают ИТ- и ИБ-специалисты. Подразделения часто разворачивают подобное ПО для решения внутренних задач.

Личные ресурсы системных администраторов, развернутые в сети компании. Яркий пример — небольшие публичные сайты, созданные сотрудниками.

Неконтролируемые BYOD-устройства. Мобильные телефоны, флешки, ноутбуки. Особенно опасны пользовательские точки доступа к корпоративной сети (например, принесенные из дома роутеры).

Файловые хранилища, онлайн-версии офисных программ и другие облачные сервисы.

и к корпоративному Wi-Fi, и к контроллеру домена. Это был один из самых быстрых и легких наших пентестов.

Особенно опасны личные ресурсы системных администраторов, развернутые в сети компании. Самый распространенный пример — небольшие сайты. За ними плохо следят, а со временем о них вообще забывают. Мы как минимум раз в пару месяцев находим подобные сервисы в разных компаниях. Так, у одного из заказчиков обнаружили заброшенный личный сайт на IP-адресе одного из филиалов. На нескольких самописных страницах мы нашли SQL-инъекцию, которая позволила получить доступ к данным из всех БД. За несколько часов мы восстановили пароль администратора CMS Joomla, которая использовалась на сайте, и разместили шелл на сервере. С его помощью построили туннель до внутренней сети филиала, а оттуда добрались до серверов основного офиса.

Еще один тип Shadow IT — неконтролируемые BYOD-устройства *(Bring Your Own Device)*. Сегодня многие компании разрешают сотрудникам использовать собственные электронные девайсы: флешки, телефоны, ноутбуки. Но никто не может гарантировать, что они не содержат вирусов или вредоносного ПО. Особенно опасны пользовательские точки доступа к корпоративной сети. Сотрудники приносят на работу домашние роутеры, чтобы подключаться к Wi-Fi и не обременять себя проводами. Пароль для сети, как правило, ставится предельно простой, а тип шифрования выбирается произвольно. Такой роутер — отличное место для проникновения. Он приведет злоумышленника прямо в корпоративную

КАК УМЕНЬШИТЬ КОЛИЧЕСТВО SHADOW IT

01 Регулярно проводите инвентаризацию ИТ-активов, чтобы исключить появление бесхозных устройств.

02 Подключайте ИТ- и ИБ-отделы к обслуживанию всех систем.

03 Организуйте централизованный процесс публикации самописных решений, чтобы о них своевременно узнавали ИТ- и ИБ-специалисты.

04 Проводите периодическое сканирование внутренней сети, чтобы избежать появления неконтролируемых сервисов. Сканировать нужно все сегменты, а подозрительные хосты — либо отключать, либо инвентаризировать и передавать на контроль ИТ- и ИБ-подразделениям.

05 Проводите сканирование внешнего периметра сети и следите за тем, чтобы все системы, опубликованные в интернете, были инвентаризированы. Лучше использовать сканеры безопасности: это позволит параллельно контролировать уязвимости периметра.

06 Создайте отдельную изолированную сеть для личных устройств сотрудников. Нужно либо полностью отключить ее от главной сети, либо предоставлять пользователям максимально ограниченный доступ только к необходимым ресурсам. Например, для большинства веб-приложений пользователю требуются только 80-й и 443-й порты.

07 Ограничьте работу сотрудников со сторонними внешними носителями и сделайте защищенные буферные АРМ для передачи информации с таких устройств.

08 Используйте систему контроля доступа, которая будет пропускать в сеть только авторизованные устройства. Так вы предотвратите установку бесконтрольных Wi-Fi-точек и неразрешенных пользовательских девайсов.

09 Проводите мероприятия по повышению ИБ-грамотности сотрудников, чтобы они не выкладывали файлы и документы компании в публичные облачные сервисы. Конечно, только организационными методами здесь не обойтись: по возможности заблокируйте доступ к популярным облачным ресурсам обмена информацией, а для контроля новых и малоизвестных облаков используйте DLP-систему.

сеть и избавит от необходимости искать точку физического подключения *(обладая хорошей Wi-Fi-антенной, можно действовать с расстояния в несколько сотен метров)*. На одном из заводов мы обнаружили пользовательский роутер в сети АСУ ТП, хотя, согласно документам, она была полностью изолирована. Перехватить пакеты «рукопожатия» не составило труда, подобрать пароль — тоже. В итоге мы проникли в сеть и получили доступ ко множеству технологических процессов. Оказалось, точку доступа создали инженеры АСУ ТП, чтобы лишний раз не ходить в производственные помещения.

Файловые хранилища, онлайн-версии офисных программ и другие облачные сервисы — это практически гарантированная утечка информации. Неизвестно, как, когда и кто будет обрабатывать ваши данные. Кроме того, пользователи редко используют сложные пароли и двухфакторную аутентификацию, что сильно упрощает жизнь злоумышленникам. Угрозы возникают и при пересылке рабочих данных на личную почту.

Полностью избежать появления Shadow IT в большой компании практически невозможно. Но можно минимизировать количество «теневых» элементов и сделать их управляемыми. Главное — порядок.

Павел Волчков,
заместитель директора Центра информационной безопасности компании «Инфосистемы Джет»

Управлять можно только тем, что можно измерить.

Питер Друкер

Под Shadow IT я понимаю не абсолютно всеми забытый элемент ИТ-инфраструктуры *(так тоже бывает, но это не самая частая ситуация)*, а скорее тот, что по «историческим соображениям» работает сам по себе и не попадает в область действия корпоративных процессов. Он просто есть, о его существовании могут знать и служба ИТ, и служба ИБ, но никого не интересует, что с ним происходит, — лишь бы работал.

Кроме очевидных проблем технического характера для процессов обеспечения ИБ вроде банального *«забыли — не обновили — взломали»*, Shadow IT влекут и проблемы для бизнеса.

Наличие любых неучтенных активов вносит неконтролируемую поправку в статистику, что негативным образом влияет на управленческие решения. Стремясь повысить уровень зрелости процессов ИТ и ИБ, организация проходит путь, в общем виде описываемый моделью CMMI. Ее уровни имеют много различных качественных описаний, но все они сходятся в том, что при переходе с третьего «определенного» на четвертый «управляемый» уровень происходит качественное изменение модели управления. От понятийной модели *«нам кажется, что мы знаем, как должен быть выстроен процесс, и следуем этому»* происходит переход к аналитической: *«мы мониторим и измеряем фактическую реализацию процесса, оцениваем статистические показатели и принимаем управленческие решения на их основании»*.

Оценка эффективности процессов ИБ — сама по себе задача нетривиальная. Базовые метрики рассчитываются вполне легко, но их корреляция с уровнем реальной защищенности достаточно слабая. Простой пример — метрика по соотношению количества обновленных хостов к их общему количеству. В организации с 1000 хостов такой показатель можно довести до 99,9%, то есть обновлены будут 999 из 1000 хостов. Казалось бы, это прекрасный показатель. Но если исходить из базового принципа ИБ — «самого слабого звена», то и этого одного необновленного хоста будет вполне достаточно для компрометации всей инфраструктуры. Наличие Shadow IT дополнительно искажает показатели эффективности процессов ИБ.

Как ни странно, одним из неожиданных негативных эффектов Shadow IT является не его «невидимость», а, наоборот, излишняя «видимость» — с точки зрения процесса мониторинга событий ИБ. Речь идет о ситуации, когда из-за неоптимизированных настроек аудита возрастает поток паразитических событий, забивающих СЗИ и рассеивающих внимание первой линии.

Еще одна неочевидная проблема Shadow IT — негативный экономический эффект, который в первую очередь выражается в переплате за лицензии. Причем от этого скорее страдает служба ИТ, хотя и служба ИБ может нести потери. Например, при расчете количества лицензий на агенты для рабочих станций и серверов *(endpoint)* также повышаются внутренние затраты на всех процессах, связанных с мониторингом и реагированием на инциденты ИБ за счет необходимости их дополнительного разбора.

Повышение прозрачности и видимости сети в условиях их перманентного увеличения и усложнения является первоочередной задачей как ИТ-шников, так и ИБ-шников, решать которую необходимо сообща, но, как и любая комплексная задача, она не имеет простого решения.

КАК СПРАВИТЬСЯ С НЕОПРЕДЕЛЕННОСТЬЮ ПРИ ОЦЕНКЕ РИСКОВ ИБ

ОБЪЕМ СТР.

АВТОР
Ирина Павлова,
старший консультант Центра информационной безопасности компании «Инфосистемы Джет»

В этой жизни определено только то, что нет ничего определенного.

Плиний Старший

/ КАКИЕ ВИДЫ НЕОПРЕДЕЛЕННОСТИ ПОДСТЕРЕГАЮТ КОМПАНИЮ ПРИ ОЦЕНКЕ РИСКОВ ИБ

/ КАК ЛУЧШИЕ ПРАКТИКИ В ОБЛАСТИ ИБ РЕКОМЕНДУЮТ ОЦЕНИВАТЬ КИБЕРРИСКИ

/ ОЦЕНКА РИСКОВ ИБ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ СЕРВИСОВ: 15 СПОСОБОВ МИНИМИЗАЦИИ НЕОПРЕДЕЛЕННОСТИ ДЛЯ БАНКОВ И НЕ ТОЛЬКО

Неопределенность приносит немало головной боли ИТ- и ИБ-специалистам при оценке киберрисков. Как правильно вычислить стоимость актива, приняв во внимание все его компоненты: оборудование, ПО и др.? Как объективно оценить потенциальный ущерб от реализации угрозы? Например, для ИБ-специалиста ущерб от подделки записей журнала регистрации событий, скорее всего, будет существенным, а вот бизнес-владельцу актива угроза может показаться незначительной. Как быть с оценкой вероятности реализации угроз? Ее точно так же, как и ущерб, различные специалисты определяют по-разному. Все это важно, так как неучтенные или некорректно оцененные угрозы и уязвимости влекут за собой серьезные риски для безопасности организации.

Первый шаг к исключению подобных сценариев — определение типа, характера и значения неопределенности для достоверности результатов оценки

Неопределенность

Состояние, заключающееся в недостаточности, даже частичной, информации, понимания или знания относительно события, его последствий или его возможности

ISO Guide 73 «Risk management — Vocabulary — Guidelines for use in standards» (2009)

риска ИБ. Чтобы разобраться в этом, задайте себе несколько вопросов:

- Все ли сведения об активах и источники информации учтены при анализе?
- Насколько достаточна и достоверна анализируемая информация?
- Каковы планы развития организации? Предусматривают ли они какие-либо изменения ИТ-инфраструктуры?
- Зависит ли компания от сторонних организаций: головной компании, облачных провайдеров, партнеров и т.д.?
- Учтены ли ранее возникавшие в организации угрозы и уязвимости ИБ? А те, что могут возникнуть в будущем?

ОБРАБОТКА НЕОПРЕДЕЛЕННОСТИ: ИЩЕМ ОТВЕТЫ В ЛУЧШИХ ПРАКТИКАХ

При обработке неопределенности можно руководствоваться международными стандартами NIST Special Publication 800-xx, ISO серии 310xx, 27xxx и их российскими аналогами. Рассмотрим ключевые рекомендации этих документов.

ISO/IEC 31010:2009 «Risk management – Risk assessment techniques» / ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска». Согласно этим стандартам, для получения наиболее полной информации к оценке рисков нужно подключать как можно больше заинтересованных лиц: ИТ-специалистов, владельцев активов, юристов, экономистов и т.д. Оценивать риски следует с использованием сразу нескольких методов — например, с помощью мозгового штурма, контрольных листов и метода Дельфи, основанного на обобщении экспертных мнений. В ранжировании рисков должны участвовать высококвалифицированные специалисты: владельцы активов, юристы и экономисты. При этом необходимо учитывать всю доступную информацию, включая хронологические данные, сведения об особенностях системы, специфике организации, экспериментальные данные и т.д.

ISO/IEC 27005:2018 «Information technology – Security techniques – Information security risk management» / ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». Эти стандарты рекомендуют обращаться за квалифицированной консультацией как к заинтересованным специалистам из самой организации, так и к внешним экспертам до принятия решений по вопросам оценки рисков *(идентификация активов, ранжирование рисков, возможные угрозы в отношении активов и др.)*. Следует идентифицировать угрозы как в общем, так и по их типу, а затем, где применимо, выявлять отдельные угрозы для исключения неожиданных. Например, к общим можно отнести угрозу нарушения установленных правил разграничения доступа, к отдельным — угрозу неправомерного ознакомления с защищаемой информацией, подмены действия пользователя путем обмана, обхода некорректно настроенных механизмов аутентификации и пр. Рекомендуется учитывать внутренний опыт организации, полученный по итогам ранее выявленных инцидентов, и прошлые результаты оценки рисков. Помимо этого, следует ориентироваться на базы данных угроз и уязвимостей, которые ведут госорганы, научно-исследовательские институты и другие организации. Также важно учитывать стоимость восстановления информации либо ее зачистки и последствия для бизнеса от потери или компрометации актива. Среди значимых факторов стандарт выделяет также распространяющиеся на организацию правовые и регулирующие требования, а также применимые к ней ограничения: временны́е, финансовые, технические, операционные, культурные, этические, связанные с окружающей средой, юридические, кадровые, касающиеся интеграции

новых и существующих средств защиты. Нельзя забывать и о различиях в предположениях, понятиях, потребностях и проблемах заинтересованных сторон, связанных с риском или обсуждаемыми проблемами. Важно, чтобы все они, будь то владелец актива, юрист или экономист, осознавали риски и причины их возникновения, а также понимали, какие выгоды им дают имеющиеся активы. Наконец, необходимо учитывать ценность актива исходя из его вида.

NIST Special Publication 800-30 «Guide for conducting risk assessments» (2012), NIST Special Publication 800-37 «Risk management framework for information systems and organizations. A system life cycle approach for security and privacy» (2018), NIST Special Publication 800-39 «Managing information security risk: organization, mission, and information system view» (2011). Эта группа стандартов при выборе методологии оценки рисков рекомендует исходить из сроков планирования бюджетирования или планирования изменений политик организации, а также из сложности и зрелости бизнес-процессов *(по сегментам архитектуры организации)*. Кроме того, следует ориентироваться на фазу информационной системы *(ИС)* в жизненном цикле разработки, на критичность и чувствительность информации в ИС, поддерживающих основные организационные задачи и бизнес-функции. Необходимо учитывать оценку рисков не только в отношении ИС, но и в отношении бизнес-процессов и основной деятельности организации. При оценке рисков важно принимать во внимание расчеты иных рисков организации, определять, как долго результаты конкретных оценок можно использовать для законного обоснования решений, основанных на риске. В целом данная группа стандартов рекомендует применять трехуровневый подход к оценке, направленный на устранение рисков на уровнях организации, бизнес-процесса и ИС.

РЕГУЛЯТОР РЕКОМЕНДУЕТ: БОНУС ДЛЯ БАНКОВ

Для кредитных организаций, помимо перечисленных стандартов, актуальны также банковские стандарты СТО БР ИББС. Например, стандарт **СТО БР ИББС 2.2-2009 «Методика оценки рисков нарушения информационной безопасности»** предлагает привлекать нескольких экспертов для получения разных экспертных оценок. А согласно положениям стандарта **СТО БР ИББС 1.4-2018 «Управление риском нарушения информационной безопасности при аутсорсинге»**, провайдер должен принять такой же уровень риска, как и сама организация, передающая ему функцию ИБ на аутсорсинг.

На этапе утверждения сейчас находится еще один немаловажный документ, разработанный Банком России, — **«Положение о требованиях к системе управления операционным риском в кредитной организации и банковской группе».** Нормативный акт предполагает, что при расчете операционных рисков кредитная организация должна также учитывать риски ИБ и риски информационных систем. Этими же требованиями можно руководствоваться и при обработке неопределенности.

Так, при управлении риском ИБ банк должен вести журнал учета реализованных рисков ИБ и классифицировать регистрируемые события с учетом всех источников рисков и результатов их реализации *(потери от рисков)*. Помимо этого, необходимо определять во внутренних документах и обеспечивать функционирование системы обеспечения ИБ, разрабатывать и соблюдать политику ИБ, проводить регулярную независимую оценку не реже одного раза в год.

Примерами риска ИС служат отказ или нарушение функционирования, а также недостаточность функциональных возможностей информационной системы. Для их нивелирования рекомендуется определять систему управления риском ИС. Необходимо утверждать политику по использованию ИС и применять ее на практике, выявлять и оценивать риски ИС, а также сопряженные с ними риски ИБ и проводить мероприятия по снижению уровня выявленных рисков. Следует определять и соблюдать требования к ИС, в том числе дополнительные, и пересматривать их

На заметку

Метод Дельфи предполагает получение экспертных оценок, которые могут помочь при идентификации источников и воздействии опасности, при количественной оценке вероятности и последствий и общей оценке риска. Этот метод обобщения мнений экспертов предполагает их независимый анализ и голосование.

На заметку

Что делать перед размещением активов в инфраструктуре облачного провайдера

В первую очередь нужно разобраться, какие первичные активы и активы поддержки планируется размещать в облачных сервисах. Согласно ГОСТ Р ИСО/МЭК 27005-2010, к первичным относятся бизнес-процессы, действия и информация, к активам поддержки — аппаратные средства, программное обеспечение, сеть, удаленные рабочие места, сайт и организационная структура организации. Также необходимо определить категории защищаемой информации: персональные данные, банковская тайна, платежная или иная конфиденциальная информация. Следующим шагом должна стать оценка рисков ИБ.

не реже 1 раза в год. Кроме того, документ рекомендует разрабатывать, соблюдать и отражать во внутренних документах требования по обеспечению непрерывности, безопасности и качества функционирования ИС.

НАИБОЛЕЕ ОПТИМАЛЬНЫЙ ПОДХОД

Как же справиться с неопределенностью при оценке рисков и какие именно рекомендации лучших практик и регуляторов взять на вооружение? По нашему опыту, прежде всего стоит поменять подход к сбору данных на более эффективный — например, применять метод Дельфи и формировать фокусные группы. Помимо этого, мы рекомендуем вести внутреннюю отчетность об инцидентах ИБ и собирать сведения об актуальных угрозах для конкретной отрасли организации из общедоступных источников. Так, ФинЦЕРТ выпускает обзоры инцидентов в финансовой сфере. Владея подобной информацией, можно оценить применимость угроз для отдельной организации и учесть их при оценке рисков ИБ, что поможет предотвратить вероятные потери от ущерба.

КАКИЕ НЕОПРЕДЕЛЕННОСТИ И РИСКИ НЕСУТ ОБЛАКА

Размещение активов в облачных сервисах — одна из наиболее распространенных ситуаций, когда риски ИБ возникают из-за неопределенности. Чем это грозит? Аналитики Cloud Security Alliance *(CSA)* приводят огромный список рисков. В него входят, например, потеря данных, незащищенные интерфейсы и API, недоступность сервиса, несанкционированный доступ к активам через клиентов облачного провайдера, размещенных в той же инфраструктуре. И это далеко не всё: нельзя исключать возможность контроля доступа к чувствительным данным на уровне инфраструктуры облачного провайдера или самой организации, неопределенность ответственности между провайдером и организацией и др.

Рассмотрим риски на примере типового банка, передавшего данные на обработку в облако. Кредитная организация недооценила критичность информационного актива и активов поддержки, в том числе на стороне провайдера. Как следствие, она недооценит и ущерб от потери данных. Забыв о ком-либо, кто имеет доступ к защищаемым данным, банк тоже получит риски ИБ. То же может случиться, если вам неясно, как провайдер разграничивает права доступа клиентов к своим сервисам. Большое значение имеют и особенности выбранной модели размещения в облаке. По нашему опыту, возможность доступа работников облачного провайдера к данным в ЦОДе недооценивается многими организациями. Отдельный блок неопределенностей связан с особенностями российского рынка страхования киберрисков. Речь идет о небольшом числе игроков и нехватке у многих из них ресурсов и компетенций. К тому же риски ИБ могут быть вызваны и отсутствием прозрачности в расчете страховых выплат в случае возникновения инцидента и последующего ущерба.

ПОСЛЕСЛОВИЕ

НЕСМОТРЯ НА ТО ЧТО ПРИ ОЦЕНКЕ РИСКОВ ИБ НЕЛЬЗЯ ПОЛНОСТЬЮ ИСКЛЮЧИТЬ НЕОПРЕДЕЛЕННОСТЬ, МОЖНО ПО КРАЙНЕЙ МЕРЕ СВЕСТИ ЕЕ К МИНИМУМУ, ПРИМЕНЯЯ ПРЕДЛОЖЕННЫЕ РЕКОМЕНДАЦИИ. НУЖНО КОМБИНИРОВАТЬ СПОСОБЫ ИДЕНТИФИКАЦИИ АКТИВОВ, ВЫБИРАТЬ ПРИМЕНИМЫЕ ИМЕННО ДЛЯ ВАШЕЙ ОРГАНИЗАЦИИ МЕТОДЫ ОЦЕНКИ РИСКОВ, ПРИВЛЕКАТЬ КВАЛИФИЦИРОВАННЫХ СПЕЦИАЛИСТОВ ДЛЯ ПРОВЕДЕНИЯ НЕЗАВИСИМОЙ ОЦЕНКИ И ПЕРЕСМАТРИВАТЬ РИСКИ ИБ НЕ РЕЖЕ 1 РАЗА В ГОД.

ЧЕК-ЛИСТ

15 СПОСОБОВ МИНИМИЗАЦИИ РИСКОВ ИБ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ СЕРВИСОВ

ИРИНА ПАВЛОВА

01 Адаптация опросных листов под особенности актива и специфику организации.

02 Сбор информации по методам мозгового штурма или Дельфи.

03 Проведение встреч с бизнес-владельцами для определения критичности активов.

04 Анализ влияния человеческого фактора.

05 Опрос максимального числа заинтересованных подразделений и оценка с учетом принимаемых мер безопасности.

06 Проведение встреч с бизнес-владельцами, ИТ-подразделениями, обслуживающими систему или сервис, с провайдером услуг для получения полной информации о системах и сервисах, а также связанных с ними бизнес-процессах.

07 Изучение инцидентов ИБ в общедоступных источниках, применимых к активам или выбранной модели размещения в облаке.

08 Предварительный анализ угроз и уязвимостей, анализ методом «что, если?» с подключением специалистов, которые смогут дать квалифицированную консультацию. Например, что будет, если злоумышленники предпримут попытку атаки на интерфейс? Каковы будут последствия?

09 Оценка рисков нарушения ИБ, описанных в СТО БР ИББС 1.4-2018 «Управление риском нарушения информационной безопасности при аутсорсинге».

10 Оценка репутации провайдера и изучение материалов о нем в интернете (новости, отзывы).

11 Оценка мер безопасности, принимаемых провайдером.

12 Выбор страховой компании с опытом страхования рисков ИБ, которая имеет группу реагирования на инциденты.

13 Учет расходов на восстановление и оценка периода восстановления рабочих процессов.

14 Детальная проработка условий договора в отношении рисков ИБ, возможного ущерба и последующих выплат. Помимо управления безопасности, к обсуждению условий рекомендуется подключить ИТ-подразделения и бизнес-владельцев.

15 Своевременное обновление условий договора при изменениях внутри организации (внедрение новых ИС, обновление ИТ-инфраструктуры), а также при принятии новых законов, устанавливающих штрафы в случае инцидентов ИБ.

НЕ БОЙТЕСЬ, ВАС ТОЧНО ВЗЛОМАЮТ

АВТОР
Павел Дрейгер,
руководитель управления по информационным технологиям Группы компаний «Русагро»

О КОМПАНИИ

РУСАГРО

Ключевые фигуры
Председатель совета директоров Вадим Мошкович

Отрасль
Агропромышленность

Год основания
2016

Количество сотрудников
Более 14 тыс. человек

Сайт
www.rusagrogroup.ru

КОМУ ДОЛЖНО ПОДЧИНЯТЬСЯ ИБ-ПОДРАЗДЕЛЕНИЕ

От службы ИБ я в первую очередь жду ощущения спокойствия. Мне необходимо знать, что контур защищен от внешних проникновений, у нас достаточно инструментов, способных фиксировать внутренние угрозы, есть четкий фидбэк по состоянию инфраструктуры, своевременно выявляются слабые места. Кроме того, я жду открытого диалога с другими службами и всячески его поощряю. У нас регулярно проводятся внутренние ИБ-конференции, куда мы приглашаем специалистов, отвечающих за инфраструктуру, бизнес-приложения, и ИТ-директоров, чтобы наладить горизонтальное взаимодействие.

Схема, в которой ИБ напрямую подчиняется руководству компании, не работоспособна. Это направление должны

/ КАК СЕЛЬСКОХОЗЯЙСТВЕННАЯ ОТРАСЛЬ ВЫДЕЛЯЕТСЯ В ВОПРОСАХ ОБЕСПЕЧЕНИЯ ИБ

/ ПОЧЕМУ НЕЛЬЗЯ НА 100% ЗАЩИТИТЬСЯ ОТ АТАК ЗЛОУМЫШЛЕННИКОВ

/ КАКИЕ ФАКТОРЫ НУЖНО УЧИТЫВАТЬ, ПРИОБРЕТАЯ СРЕДСТВА ЗАЩИТЫ

курировать либо ИТ, либо служба безопасности — те, кто хотя бы немного в теме. Гендиректор, может, и поймет ИБ-специалиста, когда тот будет отчитываться о проделанной работе, но поставить правильные задачи точно не сможет. У топов другие цели, они не должны глубоко погружаться в такие проблемы.

Второй вариант — подчинение ИБ-блока службе безопасности. Главный плюс: ИБ в этой схеме никак не зависит от ИТ-блока, а значит, может объективно анализировать и контролировать действия ИТ-шников со стороны. Но есть и минусы: классическая СБ в первую очередь сосредоточена на экономической и физической безопасности, а руководит подразделением, скорее всего, бывший сотрудник силовых структур без необходимого ИТ-бэкграунда. В результате интересы и нужды ИБ могут сдвинуться на второй план.

Самая эффективная схема — сделать ИБ частью вертикали ИТ. Чистых ИБ-проектов все равно не существует, это всегда работа на стыке ИТ и безопасности. Какие бы идеи у вас ни возникали, «руками» всегда будут либо инфраструктурщики, либо сетевики. Когда ИБ и ИТ находятся в разных вертикалях, возникают проблемы с коммуникациями, качество диалога снижается в разы. Единственный минус этой модели — зависимость безопасности от ИТ-блока и, как результат, невозможность оценивать корректность действий ИТ-шников со стороны. Но в нашем случае я не довлею над ИБ-специалистами и прислушиваюсь к ним. Они всегда могут указать, где инфраструктурные или сетевые службы ущемляют интересы ИБ.

Опасения по поводу того, что в такой схеме ИБ будет финансироваться по остаточному принципу — после ИТ, я считаю несостоятельными. Если в компании утвержден долгосрочный план развития информационной безопасности, никто не сможет подвинуть ИБ-блок на второй план.

В «Русагро» существует пятилетняя программа трансформации ИБ, которую мы разработали совместно со специалистами компании «Инфосистемы Джет». Раньше каждое наше бизнес-направление решало ИБ-проблемы самостоятельно, выбирая для этого разные платформы и инструменты. Позитивный опыт одного подразделения нельзя было транслировать на другие, и экспертиза не использовалась в полной мере. Поэтому мы приняли решение о разработке единой стратегии ИБ, которую будут реализовывать все бизнес-направления.

2–4

МЕСЯЦА

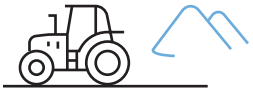
требуется на закрытие вакансии ИБ-специалиста в регионах

НАША ОТЛИЧИТЕЛЬНАЯ ЧЕРТА – АКЦЕНТ НА ЗАЩИТЕ IOT. МЫ АКТИВНО ИСПОЛЬЗУЕМ ТЕХНОЛОГИИ ИНТЕРНЕТА ВЕЩЕЙ, ПОЭТОМУ ВСЕ ИБ-ШНИКИ, КОТОРЫЕ ПРИХОДЯТ К НАМ РАБОТАТЬ, ДОЛЖНЫ ХОТЯ БЫ В ОБЩИХ ЧЕРТАХ ПРЕДСТАВЛЯТЬ, ЧТО ЭТО И КАК ЕГО ЗАЩИЩАТЬ.

В спорах ИБ с другими ИТ-службами я выступаю как бизнес-партнер и руководствуюсь интересами бизнеса.

КАДРОВЫЙ ВОПРОС: ПОКА ПЕРЕКУПАТЬ, ЗАТЕМ ВОСПИТЫВАТЬ САМИМ

В сделках M&A вы приобретаете не только оборудование и кадры, но и интеллектуальную собственность. Если рассматривать новые активы исключительно как расширение производственных мощностей, вы просто переплатите — отдельно купить станки и людей дешевле, чем действующую компанию. Мы внимательно подходим к M&A и оцениваем, сотрудников какого уровня и какую интеллектуальную собственность приобретаем. В дальнейшем мы инкорпорируем этот опыт в собственную компанию. Уровень зрелости присоединяемых активов бывает разным. Например, в прошлом году в ходе очередного слияния мы почерпнули знания и методы работы в части информационной безопасности. При этом были случаи, когда мы приобретали и компании с нулевой ИБ. Тогда мы смотрим на стратегию развития холдинга, оцениваем зрелость того направления, куда вливается актив, и создаем план его модернизации — до стандартов нашего бизнеса.



Мы идем к стандартизации и придерживаемся концепции «одна проблемная область — одна платформа». Даже если на пять бизнес-направлений у нас будут пять instance, все они будут на одной платформе, потому что это создаст предпосылки для дальнейшей централизации функции. В перспективе 4–5 лет мы планируем централизовать все сервисы. И речь не обязательно идет о «сведении» функций в Москве. Я имею в виду единую политику управления, которую можно реализовывать из любого места.

В плане защиты периметра наш агрохолдинг не отличается от других производств. Но при этом мы распределенная компания с объектами в малонаселенных районах, и здесь есть своя специфика. Все процессы должны быть хорошо отлажены, иначе ИБ-специалисты не будут вылезать из командировок по моторно-транспортным станциям, раскиданным по небольшим деревням.

Наша отличительная черта — акцент на защите IoT. Мы активно используем технологии Интернета вещей, поэтому все ИБ-шники, которые приходят к нам работать, должны хотя бы в общих чертах представлять, что это и как его защищать. В остальном сельскохозяйственная отрасль не сильно выделяется с точки зрения ИБ.

Нам нужны опытные ИБ-специалисты. Они обходятся недешево, ведь как работодатель мы конкурируем с компаниями, для которых информационная безопасность жизненно важна, — например, с банками. Логично, что они готовы платить больше, но мы привлекаем

соискателей другим. Задачи наших специалистов не сводятся к поддержке уже существующих решений, у нас можно включиться в процесс построения этих систем. Это возможность получить глубокие знания и компетенции.

У нас есть интересные проекты в регионах. Немногие могут этим похвастаться. Если хочешь расти как профессионал, в большинстве случаев тебе нужно перебираться в Москву или другие крупные города: Санкт-Петербург, Казань, Новосибирск. Наши сотрудники решают нестандартные задачи в Белгороде, Екатеринбурге, Саратове и Тамбове, и мы очень гордимся этим.

Вакансию ИБ-специалиста в регионе мы закрываем за 2–4 месяца. Подходящих экспертов мало, поскольку в регионах в целом сложно с ИТ-шниками. Берем соискателей отовсюду, хотя финансовая сфера в приоритете — оттуда приходят более крепкие специалисты с хорошим пониманием ИБ и процессным мышлением.

Нанимать студентов пока не получается. У нас прямо сейчас запускается много проектов, которыми нужно управлять. Взять студента в помощь на какой-то кейс в принципе можно, но руководить построением, например, CM *(Change Management)* у него, конечно, не получится.

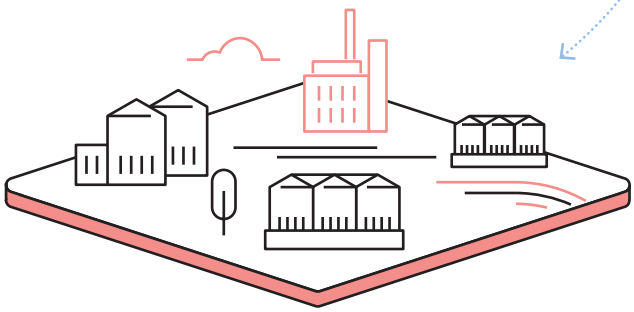
Когда система ИБ будет достроена, мы начнем активнее работать с выпускниками вузов. Ее нужно будет развивать и поддерживать, а не выстраивать — для начинающих специалистов это проще. К тому же за это время у нас сформируется институт наставников.

НЕ БОЙТЕСЬ, ВАС ВЗЛОМАЮТ

Вас точно взломают. Уверенность в том, что вам удастся поставить на пути злоумышленников непроходимые барьеры, — это иллюзия, с которой нужно немедленно расстаться. Например, есть уязвимости нулевого дня, против которых вообще нет защиты. Это нужно принять и строить ИБ исходя из этого знания. В первую очередь необходимы серьезные средства мониторинга, позволяющие вовремя зафиксировать взлом системы, и средства для локализации скомпрометированного сегмента сети.

ВАЖНЕЙШАЯ ЧАСТЬ ИБ – ОБУЧЕНИЕ ПОЛЬЗОВАТЕЛЕЙ. НЕОБХОДИМО УЧИТЬ СОТРУДНИКОВ РАСПОЗНАВАТЬ ФИШИНГ. ВЫ МОЖЕТЕ ВКЛАДЫВАТЬ ОГРОМНЫЕ СРЕДСТВА В ЗАЩИТУ СЕТИ, НО ЕСЛИ ФИШИНГОВОЕ ПИСЬМО СОСТАВЛЕНО ГРАМОТНО, ЕГО ОБЯЗАТЕЛЬНО ОТКРОЮТ И ЗЛОУМЫШЛЕННИКИ ПРОБЬЮТ ПЕРИМЕТР.

Важнейшая часть ИБ — обучение пользователей. Необходимо учить сотрудников распознавать фишинг. Вы можете вкладывать огромные средства в защиту сети, но если фишинговое письмо составлено грамотно, его обязательно откроют и злоумышленники пробьют периметр. Мы проводим специальные тренировки: сами составляем такие письма и рассылаем коллегам. Они попадаются, но с каждым разом все меньше.



№ 187-ФЗ от 26.07.2017

О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также — критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

HTTP://WWW.CONSULTANT.RU/DOCUMENT/CONS_DOC_LAW_220885

Одна из главных угроз для ИБ — публичные облака. Вы никогда не узнаете, как именно они защищены с точки зрения ИБ, не получите доступ ко всем логам. Иногда публичное облако выступает как продолжение частного и таким образом становится частью внутренней инфраструктуры. При этом защищаете его не вы, и с точки зрения ИБ — это риск. Как руководитель ИТ я выступаю за частные облака, но крупные компании сейчас просто не могут не использовать публичные решения. Например, для быстрого развертывания пилотов. Если вы хотите достичь успеха в бизнесе, вам просто придется применять гибридный подход.

Еще одна актуальная угроза — уже упомянутый мной IoT. Интернет вещей подразумевает огромное количество точек подключения к сети, но промышленные стандарты защиты еще не выработаны. На мой взгляд, обеспечивать защиту IoT в первую очередь должны производители соответствующего оборудования.

Особняком стоит тема защиты АСУ ТП. Недаром государство обратило внимание на это направление и выпустило Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Дело в том, что в подавляющем большинстве случаев оборудование АСУ ТП работает на Windows XP. Эта ОС давно не поддерживается, закончилась даже расширенная поддержка безопасности. Но лезть в эту тему страшно, потому что переход на последнюю версию Windows гарантированно остановит производство. Подобные проблемы характерны для всего EoL/EoS-оборудования.

Классический ответ на этот вызов — сделать закрытый сегмент сети. Но это самообман. Современному предприятию требуется постоянная подпитка данными, на этом строятся актуальные методы планирования производства и вся концепция Индустрии 4.0. Если информация не приходит в ERP, у вас не цифровое предприятие. А если вы хотите быть «цифровыми», придется дать доступ к сети оборудованию, которое легко взломать.

Для поддержки оборудования АСУ ТП вендору нужен внешний доступ. То есть в закрытый сегмент вашей сети нужно дать доступ специалисту из

СОВРЕМЕННОМУ ПРЕДПРИЯТИЮ ТРЕБУЕТСЯ ПОСТОЯННАЯ ПОДПИТКА ДАННЫМИ, НА ЭТОМ СТРОЯТСЯ АКТУАЛЬНЫЕ МЕТОДЫ ПЛАНИРОВАНИЯ ПРОИЗВОДСТВА И ВСЯ КОНЦЕПЦИЯ ИНДУСТРИИ 4.0.

Дании, Германии или, например, Голландии. Можно контролировать этот процесс с помощью решений класса PIM-PUM-PAM *(PIM — Privileged Identity Management, PUM — Privileged User Management, а PAM — Privileged Account/Access Management)*, но просто изолировать сегмент в современных реалиях невозможно.

НА ЧТО ТРАТИТЬ ДЕНЬГИ В ПЕРВУЮ ОЧЕРЕДЬ

Самый простой ответ на все новые вызовы — регулярное приобретение новых средств защиты. Но в реальности эта схема нежизнеспособна. Она сработает на новом производстве, где используется современное оборудование. Но у любой компании есть «историческое наследие». Что с ним делать — неизвестно, правильного ответа не существует. Причем модернизация старого оборудования зачастую стоит столько, что проще построить новое производство. Конечно, бизнес на такие траты не пойдет.

Приобретая новые средства защиты, мы отталкиваемся от проблематики. Если возникают сложности с оперативным доступом сотрудников к системам, мы обращаем внимание на IdM-решения *(системы управления доступом)*. Если видим проблему с подрядчиками, идем в класс PIM-PUM-PAM. Важно не вестись на хайп, а руководствоваться конкретными проблемами бизнеса.

Некоторые ИБ-проекты приносят компании очевидную прибыль. Выгоду от внедрения того же IdM-решения достаточно просто посчитать. Чем быстрее сотруднику выдали нужные права, тем быстрее он начал выполнять свои функции и тем выше его эффективность. Но подобные проекты — скорее исключение, чем правило.

Мы работаем по модели угроз. Каждая угроза описывается с точки зрения двух факторов: вероятности того, что она случится, и потенциальных финансовых потерь. Первый просчитывают ИБ-специалисты, второй — представители бизнеса. По итогам мы закрываем наиболее опасные угрозы.

ЧТОБЫ В ВАШЕЙ КОМПАНИИ ВОЗНИКЛИ SHADOW IT, НЕОБХОДИМЫ ПРЕДПОСЫЛКИ – НАПРИМЕР, ОТДЕЛЬНАЯ ПОДПИСКА НА ОБЛАКО ИЛИ НЕУЧТЕННЫЙ СЕРВЕР. У НАС ПРОЦЕДУРЫ ЗАКУПКИ ИТ-РЕШЕНИЙ ВЫСТРОЕНЫ МАКСИМАЛЬНО СТРОГО, ПОЭТОМУ НЕНУЖНОЕ ОБОРУДОВАНИЕ В ПРИНЦИПЕ НЕ МОЖЕТ ПОЯВИТЬСЯ В КОМПАНИИ.

Чтобы в вашей компании возникли Shadow IT, необходимы предпосылки — например, отдельная подписка на облако или неучтенный сервер. У нас процедуры закупки ИТ-решений выстроены максимально строго, поэтому ненужное оборудование в принципе не может появиться в компании. M&A тоже не приносит новых Shadow IT, поскольку перед каждым поглощением мы проводим тщательный аудит.

Сегодня рынок ИБ-аутсорсинга не конкурентен и поэтому перегрет. Есть несколько компаний, предоставляющих качественные, но все же слишком дорогие услуги. Скорее всего, причина в нехватке ИБ-специалистов. Мы готовы отдавать на аутсорсинг вещи, в которых нужен взгляд со стороны. Например, аудит ИБ, проводить который собственными силами совершенно неэффективно.

Чтобы мы начали аутсорсить ИБ, цены на некоторые услуги должны упасть в 5–10 раз. Например, на использование SOC. Но есть и адекватные расценки: на мой взгляд, пентесты сейчас стоят своих денег.

CMDB

КЛЮЧ К УПРАВЛЕНИЮ АКТИВАМИ

АВТОР
Алексей Акопян,
руководитель отдела систем мониторинга Дирекции вычислительных комплексов, сервиса и аутсорсинга компании «Инфосистемы Джет»

/ ПОЧЕМУ ОТСУТСТВИЕ БАЗЫ ИТ-АКТИВОВ МЕШАЕТ РАЗВИТИЮ КОМПАНИИ

/ ЧТО НУЖНО УЧЕСТЬ ПЕРЕД ПОСТРОЕНИЕМ CMDB

/ ЧЕК-ЛИСТ ВНЕДРЕНИЯ CMDB

Чтобы управлять ИТ-ландшафтом, необходимо создать единое информационное пространство, используя проверенные источники данных обо всех ИТ-сервисах, компонентах и их взаимосвязях. Для решения таких задач нужна CMDB *(Configuration Management Database)* — база данных управления конфигурациями. Это репозиторий, содержащий детальную информацию об активах компании.

ОБЪЕМ СТР.

ПЕРЕД ВНЕДРЕНИЕМ

Процесс управления сервисными активами и конфигурациями — один из самых сложных с точки зрения реализации. Зная это, компании зачастую откладывают его построение и внедрение CMDB. К тому же есть кадровая проблема: среди штатных сотрудников сложно найти специалистов, способных создать подобную базу активов и сопутствующих процессов. В большинстве случаев приходится обращаться к сторонним консультантам или консалтинговым компаниям, услуги которых стоят дорого.

Многие компании с головой бросаются в инвентаризацию всего подряд, месяцами собирают информацию об активах в единую базу, а в итоге всего лишь узнают, из чего состоит их ИТ-инфраструктура. Это самая распространенная ошибка: создание базы ради создания. Перед внедрением CMDB нужно обязательно задать себе два вопроса: 1) для решения каких задач нужна система; 2) кто будет потребителем полученной информации.

Другой важный фактор — наличие в компании четко регламентированного процесса управления данными. Без него внедрение CMDB не имеет смысла: инструмент не принесет пользы, но станет гигантской статьей расходов.

Отсутствие единой базы ИТ-активов мешает развитию компании.

Вы не можете быстро реагировать на ИБ-инциденты. Без CMDB вы не узнаете, какие системы затронул инцидент и как он повлияет на бизнес. В результате не сможете оперативно локализовать проблему, а это прямой путь к остановке бизнес-сервисов и финансовым потерям.

Если вы изменяете элементы ИТ-ландшафта, то можете негативно повлиять на зависящие от них сервисы. Нельзя эффективно управлять изменениями, не имея информационной основы для оценки рисков.

Вы не можете оптимизировать затраты и планировать развитие ИТ-инфраструктуры. Типичная ситуация: при введении в эксплуатацию нового сервиса инициируется закупка нового оборудования, хотя в компании есть необходимые ресурсы. Просто об этом никто не знает.

КАК ПРАВИЛЬНО ВНЕДРЯТЬ

Построение CMDB не должно быть самоцелью. Это средство для решения более глобальных, в том числе управленческих, задач. Сразу привлекайте к проекту сотрудников, которые будут потребителями информации, чтобы сформировать у них понимание ценности решения.

Правильно определите охват CMDB — выделите объекты и атрибуты, учет которых реально повысит эффективность использования информации. Не забывайте, что за актуальностью данных придется следить, поэтому лучше сразу решить вопрос автоматизации их сбора. Учитывайте, что в компании могут быть системы, содержащие инвентарную информацию о некоторых объектах ИТ-инфраструктуры. Их нужно использовать как источники данных, особенно если это доверенные системы — например, финансового учета. Соответственно, возникает необходимость в их интеграции с CMDB. Задача сложная, но ее нужно решить, чтобы унифицировать подход к управлению активами. При этом автоматизация не исключает ручной работы с информацией в CMDB. Во-первых, вы не всегда сможете автоматически получить все необходимые атрибуты объекта. Во-вторых, есть статичные объекты, которые не отображаются в сети, но тоже

ГЛАВНЫЕ ФУНКЦИИ CMDB:

- ПРЕДОСТАВЛЕНИЕ АКТУАЛЬНОЙ ИНФОРМАЦИИ ОБ ИТ-АКТИВАХ И КОНФИГУРАЦИЯХ
- ОБЕСПЕЧЕНИЕ СКВОЗНОЙ ВИДИМОСТИ ИТ-ИНФРАСТРУКТУРЫ С ТОЧКИ ЗРЕНИЯ БИЗНЕС-ПРОЦЕССОВ

НЕ ОБЛАДАЯ ЗНАНИЯМИ ОБ ИТ-СРЕДЕ, ВЫ НЕ СМОЖЕТЕ ЕЕ ОБСЛУЖИВАТЬ, ЗАЩИЩАТЬ И РАЗВИВАТЬ.

являются активами. Например, серверный шкаф или монитор.

Проектирование ресурсно-сервисных моделей — важный этап построения CMDB. Это схемы, отражающие зависимость объектов ИТ-инфраструктуры от ИТ- и бизнес-сервисов. Конфигурационные единицы не имеют ценности сами по себе, без определения связей между ними и с зависящими от них бизнес-сервисами.

Внедрение CMDB не ограничивается наполнением базы. Важно поддерживать актуальность собранной информации. На момент заполнения, CMDB отражает базовое состояние активов. Фактически это снимок ИТ-инфраструктуры. Для сохранения актуальности данных необходимо регламентировать контроль изменений и отслеживать действия по всем объектам. Кроме того, в процесс управления активами и конфигурациями нужно изначально заложить аудит и определить цикл пересмотра структуры CMDB с заданной периодичностью. Это необходимо для выявления расхождений и корректировки конфигурационных данных.

Подберите продукт, который позволит решить именно ваши задачи. Нужно ориентироваться на его гибкость, простоту настройки, внешний вид и тип интерфейса, интеграционные возможности, стоимость. Если в компании применяется процессный подход к управлению ИТ и часть процессов уже автоматизирована, вполне логично использовать имеющиеся инструменты *(как правило, все решения для автоматизации включают в себя CMDB-инструменты)*.

При внедрении не пытайтесь описать сразу всю ИТ-инфраструктуру. Пока вы будете это делать, многие данные потеряют актуальность, а интерес к системе у потенциальных потребителей информации снизится. Нужно максимально быстро демонстрировать результаты, поэтому лучше разбить процесс на этапы. Начинайте с критичных бизнес-сервисов и активов и постепенно увеличивайте охват.

Помните, что CMDB — инструмент автоматизации. База не оправдает затраченных на ее создание усилий без правильно выстроенных процессов управления ИТ. Кроме того, вы должны гарантировать наличие в CMDB актуальной, достоверной и востребованной информации об активах и конфигурациях.

Комментарий

Мария Романычева,
консультант Центра информационной безопасности компании «Инфосистемы Джет»

В настоящее время бизнес как никогда зависит от поддерживающих его ИТ-технологий и процесса управления активами. Последний является базой для построения других процессов, обеспечивает их взаимодействие и связность. К сожалению, статистика указывает на частую проблему в коммуникациях между ИТ- и ИБ-подразделениями. Как следствие, ИБ-служба часто не обладает надлежащими данными для корректной работы.

Необходимо понимать, что при выстраивании процессов ИБ-специалисты в первую очередь опираются на данные об активах. Актуальная база информационных активов и сведения об их взаимосвязях являются

неотъемлемой частью многих процессов ИБ: контроль соответствия требованиям регуляторов, управление инцидентами, уязвимостями, рисками и т.д.

Таким образом, для эффективного обеспечения информационной безопасности необходимо рассмотреть бизнес-процессы компании, оценить и классифицировать все активы — как первого, так и второго рода.

Несоответствие требованиям регуляторов *(compliance)* грозит штрафами. Процесс управления активами *(и использование его основного инструмента CMDB)* позволяет маркировать информационные активы, подпадающие под требования стандартов PCI DSS и ISO/IEC 27001, федеральных законов «О персональных данных», «О безопасности критической информационной инфраструктуры Российской Федерации» и других нормативных актов. Благодаря этому администратор безопасности может формировать выборку активов — контур — с целью проведения внутренних аудитов на соответствие требованиям и осуществлять контроль защищенности активов.

Также без ясного представления о существующих информационных активах совершенно невозможно реализовать качественное управление инцидентами ИБ. При наступлении нелегитимного события, службе ИБ прежде всего необходимо обладать информацией о критичности затронутого инцидентом актива, а также о его взаимосвязях с остальной инфраструктурой. Единая консолидация активов позволяет оперативно обнаружить затронутые инцидентом объекты и увидеть зону его воздействия.

Представление о расположении узлов сети и их взаимодействии помогает повысить качество контроля и анализа сетевого трафика в части выявления подозрительной сетевой активности, несанкционированного удаленного доступа и т.д. Как результат, формируется картина защищенности сети.

То же самое относится и к процессу управления уязвимостями: критичность актива напрямую влияет на результирующую критичность выявленной уязвимости и на приоритет ее устранения.

Данные о версиях или планируемых изменениях в конфигурациях полезны для процесса патч-менеджмента. Достаточно запросить текущую конфигурацию актива из CMDB — и можно не тратить дополнительные ресурсы на проведение сканирования *(при условии актуальности и достоверности базы)*.

Активы — база для оценки и дальнейшей обработки рисков. Процесс включает определение ценности актива для бизнеса, выявление в нем уязвимостей и угроз, оценку вероятности их реализации и расчет возможного ущерба. Другими словами, на входе нужно получить максимально полную информацию об активе. Соответственно, прозрачность технической и программной архитектуры компании и агрегация сведений об активах повышают эффективность процесса управления рисками.

Еще одной общей проблемой для ИТ и ИБ являются теневые ресурсы. Подобные активы не контролируются с точки зрения выполнения корпоративных стандартов и требований надежности, а также не подчиняются правилам централизованной безопасности. Отсутствие обновлений, патч-менеджмента, изменения конфигураций порождает риски ИБ. Наличие CMDB в компании частично помогает снять эту головную боль, внося определенность в состояние инфраструктуры компании.

Кроме того, CMDB может служить инструментом оценки эффективности ИТ- и ИБ-процессов компании. Большое количество метрик так или иначе связано с активами и действиями с ними *(например, доля АРМ с установленными агентами антивирусного ПО в общем количестве АРМ)*. Актуальная база помогает осуществлять мониторинг «здоровья» инфраструктуры компании.

Сотрудники ИТ- и ИБ-подразделений должны знать, где что «лежит» и насколько это критично как для предоставления ИТ-услуг, так и для соблюдения требований безопасности. Согласованные действия повышают осведомленность о состоянии инфраструктуры компании, способствуя бесперебойной работе бизнеса.

ЗАЩИТА

BIG DATA

/ КАК ПРАВИЛЬНО СТРОИТЬ ЗАЩИТУ БОЛЬШИХ ДАННЫХ
/ КАКИЕ ИБ-ПРОБЛЕМЫ ЕСТЬ У HADOOP
/ СУЩЕСТВУЕТ ЛИ УНИВЕРСАЛЬНАЯ ПИЛЮЛЯ ОТ ВСЕХ УЯЗВИМОСТЕЙ BIG DATA

АВТОР
Андрей Черных,
руководитель отдела систем мониторинга ИБ и защиты приложений Центра информационной безопасности компании «Инфосистемы Джет»

Вокруг термина Big Data идет множество споров. На мой взгляд, за ним скрываются два понятия: «объем» и «технологии». Большой объем данных без эффективной обработки — это свалка, а использование технологий без должного количества информации бессмысленно.

Hadoop — одно из самых распространенных и активно развивающихся решений для работы с Big Data. Это платформа с открытым исходным кодом, в основе которой лежит распределенная файловая система. Поверх нее функционируют различные сервисы для обработки информации. Hadoop позволяет реализовывать распределенные вычисления и хранение данных. На действительно больших объемах информации — десятках и сотнях терабайт — платформа работает эффективнее классических реляционных БД.

У большинства крупных заказчиков решение Hadoop либо уже есть, либо скоро появится. В основном используются сборки от трех вендоров: американской компании Cloudera, вошедшего в ее состав разработчика Hortonworks и российского производителя Arenadata.

ОБЪЕМ СТР.

ИБ-ПРОБЛЕМЫ HADOOP И МЕТОДЫ ИХ РЕШЕНИЯ

По умолчанию в Hadoop отключена аутентификация пользователей. Сегодня поисковик Shodan выдает около 900 публично доступных сервисов HDFS *(распределенная файловая система Hadoop)* без какой-либо аутентификации. Среди результатов поиска можно найти даже такие примеры, как почти 500 ТБ общедоступных данных (рис. 1).

На первый взгляд может показаться, что разграничение прав все-таки присутствует и получить доступ к данным мы не можем (рис. 2).

Но это ограничение можно легко обойти, если представиться системным пользователем (рис. 3).

Из-за отсутствия аутентификации злоумышленники могут получить доступ к данным компании, представившись

Рисунок 1. Пример результатов поискового запроса в Shodan

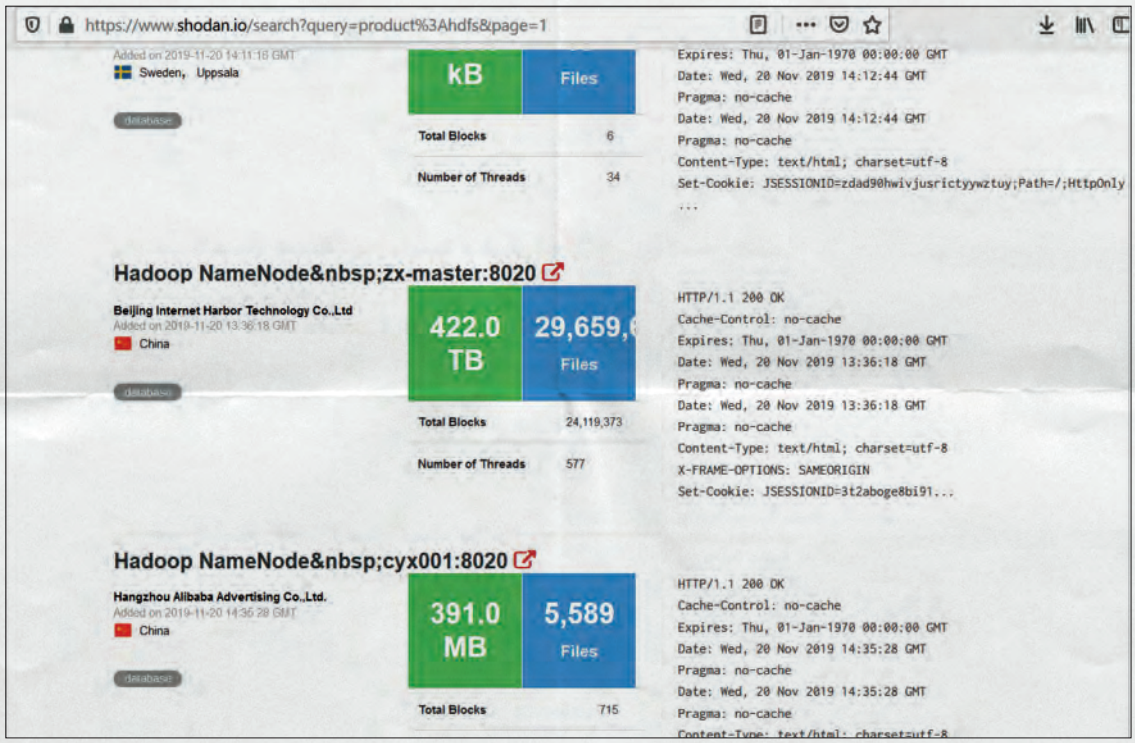
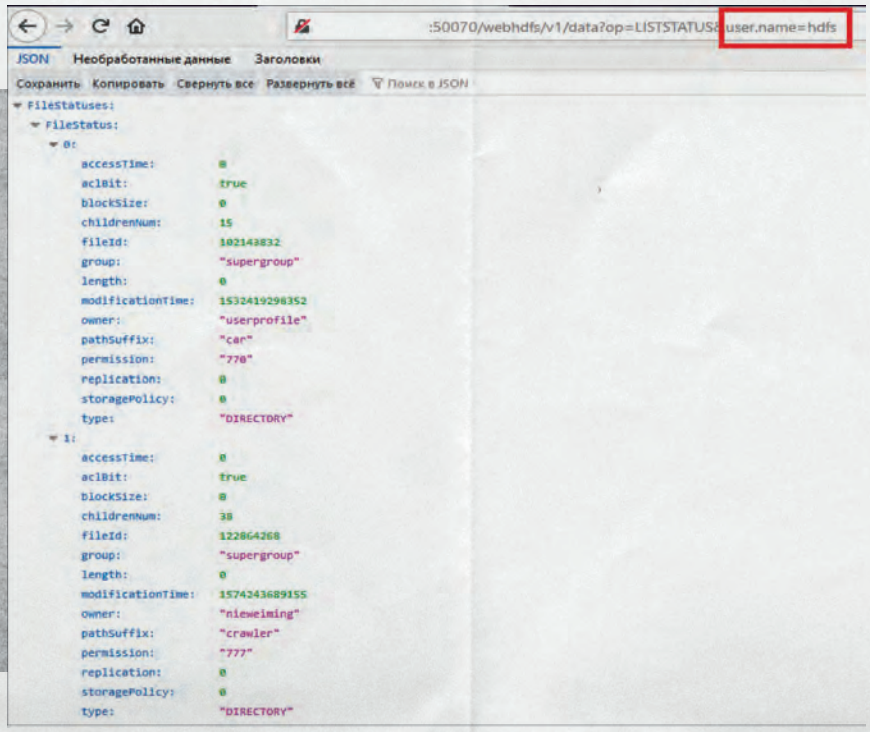


Рисунок 2. Обращение к WebHDFS без указания конкретного пользователя

Рисунок 3. Обращение к WebHDFS с указанием конкретного пользователя



ВОПРОС ПРАВ ДОСТУПА ЧАСТО ВСКРЫВАЕТ В КОМПАНИИ БОЛЬШОЙ ПЛАСТ ПРОБЛЕМ, НАПРЯМУЮ НЕ СВЯЗАННЫХ С BIG DATA. ЭТО НЕПОНИМАНИЕ ТОГО, КАКИЕ ЗАДАЧИ РЕШАЕТ БИЗНЕС-ПОДРАЗДЕЛЕНИЕ И КАКИЕ ДАННЫЕ ДЕЙСТВИТЕЛЬНО НЕОБХОДИМЫ ДЛЯ ЕГО РАБОТЫ; ОТСУТСТВИЕ ИЛИ ПЛОХАЯ РАБОТА МЕХАНИЗМОВ КЛАССИФИКАЦИИ И ОБЕЗЛИЧИВАНИЯ ИНФОРМАЦИИ; НЕХВАТКА КОНТРОЛЯ ДЕЙСТВИЙ АДМИНИСТРАТОРОВ.

системным пользователем. Эта проблема решается либо настройкой аутентификации отдельно для каждого сервиса, либо включением Kerberos для кластера целиком *(керберизацией)*. Последний вариант значительно удобнее, но практика показывает, что не на всех инсталляциях процесс проходит гладко. Мы столкнулись с такой проблемой на проекте для одного из российских промышленных предприятий. Попытки керберизации кластера заканчивались безуспешно, поэтому мы включили механизм аутентификации отдельно для каждого используемого сервиса.

Многие сервисы Hadoop по умолчанию работают без SSL. Проблема особенно актуальна, когда данные выходят за пределы защищенного контура компании *(если он вообще существует)*. Решается она очевидным образом — включением SSL для каждого сервиса.

КЕЙС

ПРОБЛЕМА

В одном из банков мы решали ИБ-задачу на стыке проблем защиты контура и разграничения прав доступа пользователей. Тестовая инсталляция Hadoop содержала продуктивные данные, и они поступали с задержкой в несколько недель. Но за это время информация не теряла актуальности и оставалась критичной для бизнеса. При этом обезличивание не применялось, а в тестовом контуре, помимо кластера Hadoop, находились и другие системы. Соответственно, компрометация любого из серверов могла привести к утечке данных из Hadoop.

РЕШЕНИЕ

Мы рекомендовали выделить тестовый кластер в отдельный VLAN и использовать механизмы обезличивания данных как в тестовых системах-источниках, так и в самом Hadoop.

Еще одна ИБ-проблема — отсутствие защищенного контура у кластера Hadoop. Так, у платформы полно точек входа, данные поступают из множества систем, поэтому она представляет собой лакомый кусочек для злоумышленников. Если не ограничить поток пользователей *(например, средствами межсетевого экранирования)*, вполне возможна утечка. Другой вариант — организация единой точки входа в систему встроенными средствами Hadoop. Но если у вас нет защищенного контура, это не сработает.

Слишком широкие права доступа пользователей (администраторов, разработчиков, датамайнеров, представителей бизнеса и т.д.) тоже создают сложности. Но это не лишние пользователи, которых можно просто отсечь, — специалисты должны продолжать работать, иначе бизнес встанет.

Вопрос прав доступа часто вскрывает в компании большой пласт проблем, напрямую не связанных с Big Data. Это непонимание того, какие задачи решает бизнес-подразделение и какие данные действительно необходимы для его работы; отсутствие контроля действий администраторов. Решить все эти проблемы исключительно средствами Hadoop или только за счет наложенных средств защиты не удастся. Нужно менять либо создавать определенные процессы внутри организации *(как минимум реализовать классификацию данных)*.

Универсальной «пилюли», способной решить все ИБ-проблемы Hadoop, к сожалению, не существует. Нужно использовать и встроенные, и наложенные средства защиты.

БЕЗОПАСНОСТЬ BIG DATA

Начинаем с инфраструктуры

01 Формируем защищенный контур с помощью межсетевого экрана.

02 Организуем доступ пользователей к сервисам Hadoop через Apache KNOX. Это встроенное средство защиты, обеспечивающее единый прокси для сервисов платформы.

03 Сканируем инфраструктуру и установленное на серверах ПО при помощи сканеров уязвимостей.

04 Контролируем доступ и действия администраторов на уровне операционной системы через решения класса PIM/PUM/PAM. Как минимум, целесообразно записывать сессию администратора.

Движемся к защите данных

01 Шифруем данные на уровне распределенной файловой системы встроенными средствами защиты Hadoop.

02 Организуем разграничение доступа к данным с помощью Apache Ranger. Это средство защиты, которое встраивается плагином в каждый сервис Hadoop. Оно позволяет определить привилегии доступа каждого пользователя и проаудировать действия, которые проводились с конкретными данными. Как показывает практика, не все заказчики сразу готовы приступить к разграничению доступа, особенно если Hadoop раньше работал без этого механизма. В таких случаях лучше начать с аудита, оценить текущую ситуацию и постепенно переходить к созданию правил.

03 Проводим мониторинг активности пользователей Hadoop при обращении к данным. Можно сделать это и средствами Apache Ranger, но в нем достаточно топорная отчетность (всего один вариант отчета без каких-либо глубоких настроек). Еще хуже обстоит ситуация с интеграцией с системами мониторинга событий ИБ и отправкой уведомлений: штатные средства интеграции фактически отсутствуют. Гораздо более удачный вариант — решения класса Database Activity Monitoring (DAM). Среди их преимуществ можно отметить более гибкую отчетность, возможности интеграции с другими системами и интерфейс управления политиками безопасности.

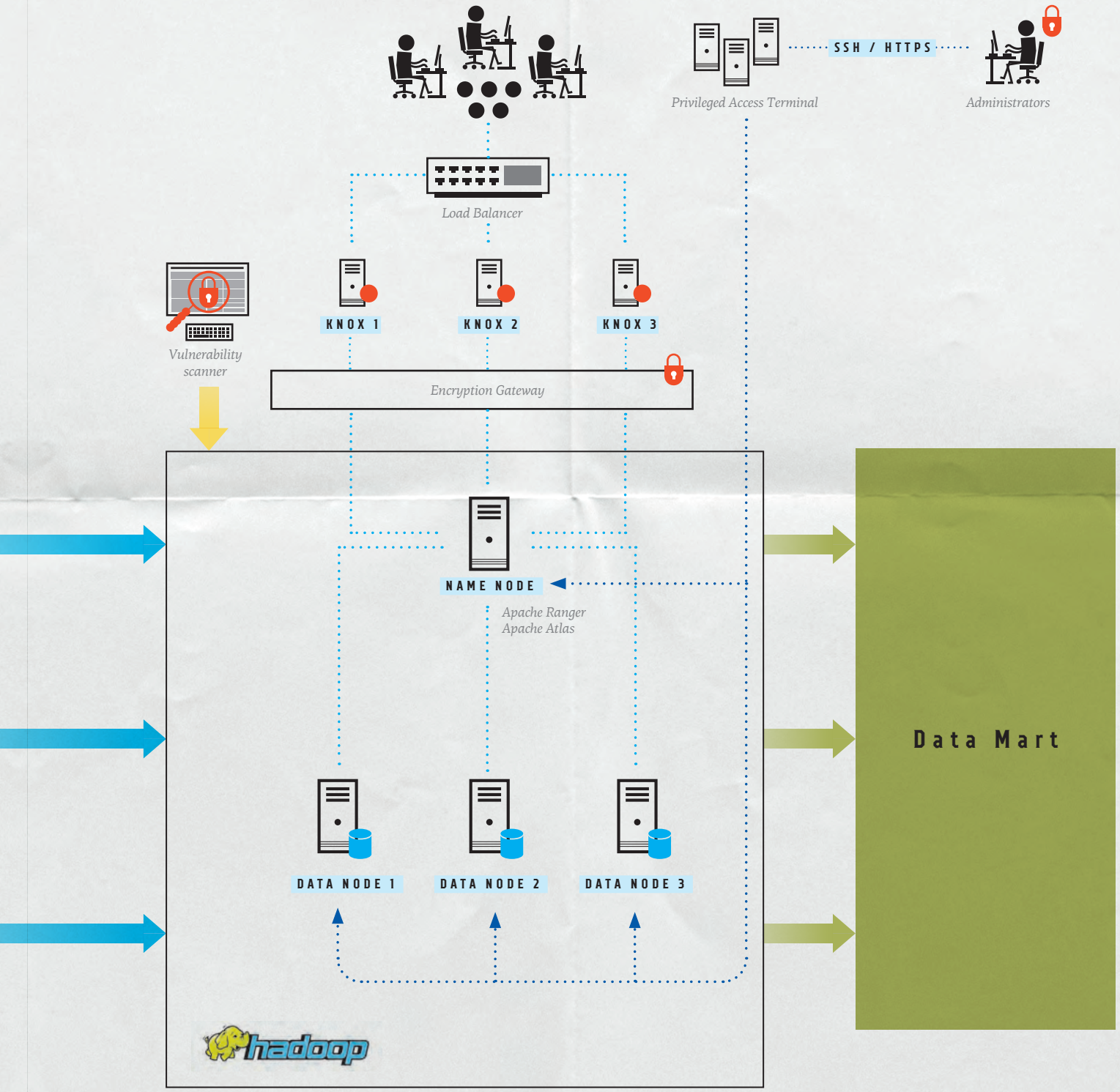
04 Маркируем и тегируем данные средствами Apache Atlas. В дальнейшем теги можно использовать в политиках Ranger, что существенно упрощает процесс разграничения доступа. Вместо нескольких сотен и даже тысяч объектов мы получаем считанное число тегов. Инструмент не предполагает какой-либо встроенной автоматизации, но у него есть API. Так, на одном промышленном предприятии мы размечали объекты в Excel (благо их было не слишком много) и передавали результаты в Atlas по API. Это позволило сократить число ручных операций в Atlas.

05 Выполняем шифрование, маскирование или токенизацию данных. Это, пожалуй, лучшее, что может произойти с ними, поскольку метод защищает данные вне зависимости от того, кто и откуда к ним обращается. Если большому числу пользователей, например разработчикам или датамайнерам, требуется работать с разнообразной информацией, ограничивать их политиками доступа нельзя. Критичные данные нужно зашифровать или замаскировать, чтобы избежать утечки через этот канал. При этом важно как можно раньше определить, каким пользователям действительно нужно видеть те или иные данные с точки зрения их бизнес-задач, — без этого весь процесс теряет смысл.

Data Sorces (DBs, External systems, etc.)

Если собрать все средства защиты вместе, выглядеть это будет примерно так (рис. 4).

Рисунок 4 **Средства защиты Big Data**



КАДРОВЫЙ ГОЛОД В ИБ

— Кадровый голод — это тема, о которой говорят постоянно. Когда вы впервые с ним столкнулись?

Дмитрий Гадарь: Кадровый голод есть всегда и во всех сферах рынка, просто в ИБ он более заметен, поскольку это достаточно новое направление. На рынке есть молодые ребята, которые занимаются анализом защищенности, подтягивают технические навыки. В то же время не хватает вовлеченных в профессию людей, своего рода идеологов, способных сделать так, чтобы уязвимости в принципе не появлялись.

Ольга Елисеева: Для интегратора кадровый голод — вечная тема. Мы воспринимаем его не как проблему,

ОБЪЕМ СТР.

/ КАК РЕГУЛЯТОРЫ ВЛИЯЮТ НА РЫНОК ИБ
/ ПОЧЕМУ TINKOFF.RU НЕ ТОРГУЕТСЯ С СОИСКАТЕЛЯМИ
/ ЧТО ОБЩЕГО МЕЖДУ POSITIVE TECHNOLOGIES И ГНЕСИНКОЙ

АВТОР
Дмитрий Гадарь,
руководитель департамента информационной безопасности Tinkoff.ru*
* Должность и место работы спикера на момент публикации.

АВТОР
Ольга Елисеева,
руководитель департамента проектирования и внедрения Центра информационной безопасности компании «Инфосистемы Джет»

АВТОР
Максим Филиппов,
директор по развитию бизнеса компании Positive Technologies в России

а как реальность, в которой нужно уметь жить. Я работаю в компании «Инфосистемы Джет» уже 9 лет, и все это время есть ощущение дефицита кадров.

Максим Филиппов: Кадровый голод в ИБ был всегда, и с годами он только усиливается. Рынок растет, регуляторы стимулируют его развитие, и бизнес осознает важность вопроса. ФСБ, ФСТЭК, ЦБ РФ выпускают свои стандарты. Например, Банк России рекомендует финансовым организациям в обязательном порядке выполнять анализ кода своих приложений. Но для этого нужны соответствующие профильные специалисты. То есть банально: берем количество приложений, множим на число аналитиков — вот тебе и кадровый голод.

У нас есть несколько профилей сотрудников: BizDev и sales, R&D, исследователи информационной безопасности, бэк-офис, маркетинг, инженеры. По каждому из них наши кадровые потребности различаются. Возьмем, например, пентестеров и экспертов, которые расследуют инциденты или выявляют атаки. Порой, чтобы попасть в этот блок, люди проходят собеседования по три года *(как в Гнесинку)*. Здесь у нас всегда есть вакансии, и если появится сильный эксперт, то мы его обязательно возьмем. Проблема в том, что их на российском рынке мало, прямо несколько десятков. Напротив, найти специалиста в BizDev и sales очень легко, поскольку наши решения просто продавать. Еще одно направление, по которому мы находимся в условиях жесткой кадровой конкуренции, — R&D. И конкурировать нам приходится с ИТ-гигантами с международными амбициями. Однако наши проекты все равно вызывают интерес у специалистов, скажем, из «Яндекса» или Сбербанка, которые приходят к нам в разработку.

Можно сказать, что кадровый голод неоднороден. Не хватает программистов,

которые быстро находят привлекательную работу вне ИБ. В дефиците пентестеры, реверсы, рисерчеры, потому что на рынке их мало и этому не учат в вузах. Инженеров тоже не хватает, но в несколько меньшей степени.

— Есть три способа закрыть кадровую проблему: привлекать специалистов с рынка, растить молодежь и переучивать собственных сотрудников из смежных областей. Как поступает ваша компания?

Дмитрий Гадарь: Мы комбинируем три способа. Регулярно работаем со студентами, иногда перекупаем отдельных специалистов. Много сил вкладываем в развитие персонала: проводим обучение для коллег из других подразделений и берем к себе лучших. Так, мы вырастили очень крутого безопасника из HR-специалиста. Я приветствую рост внутри команды, а не поиск лидеров на рынке.

ИБ не может быть замкнута сама на себе, она связана с поведением каждого сотрудника. Важно продвигать культуру информационной безопасности, обучать людей, которые занимаются проектной деятельностью, аналитиков и кодеров. Для этого у нас есть программы подготовки Security Champions — людей, которые транслируют культуру ИБ в свои команды.

Ольга Елисеева: Конечно же, используем все три способа. Вариант с переучиванием специалистов из других департаментов — реже. Нельзя, решая свои проблемы, создавать кадровый дефицит у коллег. Зато мы активно вкладываемся во внутреннее развитие — повышение компетенций, кросс-обучение с соседними департаментами.

Перекупать сотрудников не очень любим. Если человека в первую очередь интересуют деньги, скорее всего, он уйдет в другую компанию на чуть большую зарплату. Но мы идем и на такие меры, если уверены, что специалист принесет что-то ценное: выстроит процесс, наберет команду, даст редкую для рынка экспертизу.

Отмечу, что все актуальнее становится развитие софт-скиллов — одних технических знаний недостаточно. Заказчикам хочется, чтобы им человеческим языком объясняли, как их будут защищать. Представители бизнеса

ИБ – ЭТО СВОЕГО РОДА ПАРАНОЙЯ. ХОРОШИМ ИБ-СПЕЦИАЛИСТОМ СТАНОВИТСЯ ТОТ, КТО СПОСОБЕН МЫСЛИТЬ КРИТИЧЕСКИ, ПЕРЕПРОВЕРЯТЬ УТВЕРЖДЕНИЯ КОЛЛЕГ И КОНТРОЛИРОВАТЬ ПРОЦЕССЫ.

Дмитрий Гадарь, Tinkoff.ru

активнее погружаются в процесс, чтобы понять, куда тратятся деньги. Хорошему ИБ-специалисту нужны развитые навыки переговорщика, презентации материала.

Максим Филиппов: У нас была потрясающая история, когда F5 Networks решила уйти из России и закрыла офис в Томске. Едва заслышав об этом, мы вышли на их сотрудников и практически полностью забрали к себе команду экспертов — так появился офис в Томске.

Мы не видим большого смысла в переманивании специалистов оффером с высокой зарплатой. Наш рецепт борьбы с нехваткой кадров — стать привлекательными для соискателей. И только деньгами этот вопрос не решить — нужно, чтобы люди хотели работать в Positive Technologies. Например, мы вкладываем большие средства в обучение и рост сотрудников — десятки миллионов рублей ежегодно.

— Вы готовы брать студентов на стажировку и давать им необходимые знания?

Максим Филиппов: Мы периодически запускаем стажерские программы. По большей части в тех случаях, когда чувствуем комплексную потребность в молодых специалистах по какому-то конкретному направлению. Так, например, в прошлом году мы открыли большую программу для начинающих

HTTPS://WWW.PTSECURITY.COM/RU-RU/ABOUT/EVENTS/291308/

TINKOFF.RU – ПРИВЛЕКАТЕЛЬНЫЙ БРЕНД, К НАМ ХОТЯТ ПОПАСТЬ. ПОЭТОМУ ДЛЯ НАС ИБ-РЫНОК – ЭТО РЫНОК РАБОТОДАТЕЛЯ: МЫ САМИ ВЫБИРАЕМ ТЕХ, КТО БУДЕТ У НАС РАБОТАТЬ.

Дмитрий Гадарь, Tinkoff.ru

разработчиков Python в Томске. В итоге взяли на работу 10 человек и сформировали кадровый резерв. Время от времени запускаем похожие программы для пентестеров. Конечно, у нас в планах есть и запуск программ, нацеленных, например, на реверсов или, скажем, специализированных — для студентов и начинающих ИБ-специалистов. Мы считаем это важным, поскольку индустрия развивается быстро и уже сейчас понятно, что чем дальше, тем сильнее будет нехватка нужных нам экспертов. В таких условиях вполне логично уже сейчас работать на перспективу.

Дмитрий Гадарь: Не так давно мы проводили финтехшколу для выпускников технических вузов, в частности МФТИ. Выбрали пятерых наиболее перспективных студентов и взяли на позиции джуниоров. Очень способные ребята, в некоторых вопросах дадут фору состоявшимся ИБ-специалистам.

Ольга Елисеева: Раньше в «Инфосистемы Джет» стажерские программы

У НАС НЕТ ПРАКТИКИ ПОГЛОЩЕНИЯ СТАРТАПОВ. В САМОЙ КОМПАНИИ ВЫСОКАЯ КОНЦЕНТРАЦИЯ НОВЫХ ИДЕЙ, ТАК ЧТО НАМ ИНТЕРЕСНЕЕ ТРАТИТЬ РЕСУРСЫ НА СВОИХ, СКАЖЕМ ТАК, ВНУТРЕННИХ СТАРТАПЕРОВ. ЕСЛИ ВОЗЬМЕМ ЕЩЕ И ВНЕШНИХ, РИСКУЕМ ПОЛУЧИТЬ ГОЛОВНУЮ БОЛЬ, А НЕ РЕШЕНИЕ ПРОБЛЕМЫ.

Максим Филиппов, Positive Technologies

были поставлены на поток, многие наши студенты выросли до экспертов и тимлидов. Затем мы перешли на формат наставничества: каждому стажеру назначается куратор, который обучает его, дает практические задачи и вкладывается в его развитие. В настоящее время решили возобновить стажерские программы. Опыт показывает, что в студента нужно инвестировать примерно год, чтобы компания начала получать профит от его работы.

— Рассматриваете ли вы вариант с созданием собственного учебного центра?

Дмитрий Гадарь: За редкими исключениями *(Security Operation Center, управление изменениями, Application Security)* нам хватает людей, а раз потребности нет, мы не думаем в этом направлении. К тому же перенасыщение компании младшими специалистами может вызвать негативные последствия: когда больше половины команды составляют джуниоры, она малоэффективна. Молодые ребята не смогут качественно выстроить ИБ-процессы.

Ольга Елисеева: На поддержку такого центра необходимо много ресурсов. Придется создать дополнительные рабочие места или сильно увеличить нагрузку на имеющихся специалистов, поэтому строить его я не вижу смысла. Логичнее регулярно запускать стажерские программы — так мы будем находить нужных людей, прикладывая гораздо меньше усилий.

Максим Филиппов: Обучающий центр пока вне зоны наших интересов. Мы сотрудничаем с учебным центром «Информзащиты»: передаем разработанные нами курсы, а они их проводят. Возможно, со временем мы тоже до этого дорастем.

— Каких специалистов вам не хватает прямо сейчас и кто будет в дефиците в ближайшие 5–7 лет?

Дмитрий Гадарь: Сильно не хватает людей, способных выстраивать процессы по управлению уязвимостями в приложениях. Еще ощущается нехватка людей в области выявления инцидентов ИБ и реагирования на них.

Кроме того, в ИБ набирает популярность машинное обучение, поэтому возникнет спрос на ML-специалистов.

Максим Филиппов: Соглашусь с тем, что есть нехватка специалистов, способных обрабатывать инциденты, а это очень перспективное направление: количество SOC увеличивается, регуляторы выпускают новые требования и рекомендации. Также не хватает сотрудников в R&D. Сейчас на российских разработчиков установился высокий спрос из-за соотношения цена-качество. Это спровоцировало рост конкуренции с международными компаниями. Ну и конечно же, высококлассные пентестеры всегда в дефиците.

Ольга Елисеева: В дефиците всё, что связано с новыми технологиями — DevSecOps, защитой Big Data, IoT, машинным обучением. В перспективе будет не хватать экспертов по роботизации и блокчейну, если технология все же станет массовой. Последние годы стабильно не хватает людей, умеющих работать с SOC или имеющих практический опыт в Application Security. Еще, как бы банально это ни звучало, нам всегда нужны сетевики, поскольку сетевые проекты появляются постоянно.

— Как вы оцениваете рынок ИБ в России: это рынок соискателя, где компании готовы перекупать сотрудников друг у друга, или работодателя?

Дмитрий Гадарь: Tinkoff.ru — привлекательный бренд, к нам хотят попасть. Поэтому для нас это рынок работодателя — мы сами выбираем тех, кто будет у нас работать.

Ольга Елисеева: Мне кажется, это рынок соискателя. У Дмитрия высокая конкуренция на одно место, поэтому они сами выбирают людей. В нашем случае конкуренция ниже, поэтому мы инвестируем в HR-бренд, в маркетинг, стараемся быть привлекательнее как работодатель.

Максим Филиппов: Это очень неоднородный рынок. Как я уже говорил, BizDev и sales для нас — рынок работодателя: мы сами выбираем, кто будет у нас работать. В случае с R&D, скорее, рынок соискателя, хотя тоже не всегда. По большому счету нет однозначного понятия, чей это рынок,

КАДРОВЫЙ ГОЛОД В ИБ БЫЛ ВСЕГДА, И С ГОДАМИ ОН ТОЛЬКО УСИЛИВАЕТСЯ. РЫНОК РАСТЕТ, РЕГУЛЯТОРЫ СТИМУЛИРУЮТ ЕГО РАЗВИТИЕ. НАПРИМЕР, БАНК РОССИИ РЕКОМЕНДУЕТ ФИНАНСОВЫМ ОРГАНИЗАЦИЯМ ВЫПОЛНЯТЬ АНАЛИЗ КОДА СВОИХ ПРИЛОЖЕНИЙ. НО ДЛЯ ЭТОГО НУЖНЫ СООТВЕТСТВУЮЩИЕ СПЕЦИАЛИСТЫ. ТО ЕСТЬ БАНАЛЬНО: БЕРЕМ КОЛИЧЕСТВО ПРИЛОЖЕНИЙ, МНОЖИМ НА ЧИСЛО АНАЛИТИКОВ – ВОТ ТЕБЕ И КАДРОВЫЙ ГОЛОД.

Максим Филиппов, Positive Technologies

как нет и одинаковых правил по поводу того, как собрать талантливых людей в одном месте. Мы считаем важным предложить крутую, увлекательную задачу, и если она совпадает с интересами конкретного человека, то ни о каких искусственных методах мотивации речь даже не заходит.

— Замечаете ли вы разницу между поколениями X, Y и Z или эта теория для вас не актуальна?

Дмитрий Гадарь: У нас молодая команда, практически всем до 30, поэтому я не вижу разницы. Но небольшие различия есть: чем старше человек, тем важнее ему стабильность и какая-то «база», молодых легче завлечь развитием и интересной работой.

Ольга Елисеева: Почти все наши сотрудники — представители поколения Y. Поколение Z еще слишком юное, чтобы идти к нам, поэтому пока не могу сказать, как оно проявит себя в деле.

Максим Филиппов: У нас есть представители разных поколений, но благодаря работе HR это люди с одинаковыми ценностями. Разницы мы не ощущаем.

— Можно ли решить проблему отсутствия кадров в ИБ с помощью стартапов? Например, полностью выкупить команду и интегрировать ее в компанию?

Дмитрий Гадарь: Нет. Вопрос даже не в том, что в компанию придется разом интегрировать много новых людей, а в нужности их компетенций. К тому же стоимость команды стартапа в разы больше, чем приобретение их продукта. Логичнее просто купить решение.

Ольга Елисеева: Возможно, для вендоров это рабочий вариант, но нам он точно не подходит. Стартап — это всегда продукт, а мы не концентрируемся на их приобретении.

Максим Филиппов: У нас нет практики поглощения стартапов. В самой компании высокая концентрация новых идей, так что нам интереснее тратить ресурсы на своих, скажем так, внутренних стартаперов. Если возьмем еще и внешних, рискуем получить головную боль, а не решение проблемы. Да и переманивать отдельных специалистов тоже бессмысленно. Стартап создают увлеченные люди, которые работают за идею.

Если их интересуют деньги, со временем они сами придут и ты рассмотришь их кандидатуры в общем порядке.

— А что насчет аутсорсинга? Он может сгладить нехватку людей?

Максим Филиппов: По большому счету, нам отдавать на аутсорсинг нечего, мы сами можем оказывать такие услуги. Кстати, в масштабах всего рынка ИБ это тоже не решит проблему кадрового голода, потому что количество кадров по сути не изменится. Хотя конкретному бизнесу это может помочь быстро закрыть брешь.

Дмитрий Гадарь: У меня был опыт работы с аутсорсерами, но все сводилось к оперативному управлению этими командами. По сути, не было никаких отличий от работы со штатными сотрудниками.

Насчет чистого аутсорсинга я не уверен — сейчас на рынке сложно найти хороший сервис. Если речь идет о крупной и быстро развивающейся компании, все равно нужно находиться внутри, чтобы держать руку на пульсе и быстро приспосабливаться к новым условиям. Но схема аутсорсинга может сработать с небольшими компаниями или для формализованных базовых процессов.

Ольга Елисеева: К нам поступают запросы заказчиков, которые не могут справиться с нехваткой специалистов. Причины могут быть разными: ограниченность штата или бюджета, невозможность найти людей своими силами. Для них аутсорсинг — выход, возможность справиться с рисками ИБ.

ВСЕ АКТУАЛЬНЕЕ СТАНОВИТСЯ РАЗВИТИЕ СОФТ-СКИЛЛОВ – ОДНИХ ТЕХНИЧЕСКИХ ЗНАНИЙ НЕДОСТАТОЧНО. ЗАКАЗЧИКИ ХОТЯТ, ЧТОБЫ ИМ ЧЕЛОВЕЧЕСКИМ ЯЗЫКОМ ОБЪЯСНЯЛИ, КАК ИХ БУДУТ ЗАЩИЩАТЬ.

Ольга Елисеева, «Инфосистемы Джет»

Как долго ищут ИБ-специалистов (мес.)

	ЗАКАЗЧИК	ИНТЕГРАТОР	ВЕНДОР
МЛАДШИЙ СПЕЦИАЛИСТ	ДО 1	1–1,5	ДО 1
РУКОВОДЯЩАЯ ПОЗИЦИЯ	ДО 6	ДО 6	ДО 3*

* В случае Positive Technologies речь идет о senior-разработчиках.
Сотрудников на руководящие позиции в компании ищут от 2 месяцев до года (в некоторых случаях более года).

Раздел I

Энциклопедия безопасной разработки. Наш подход к IdM-проектам

IdM

- Какие IdM-решения представлены на российском рынке
- Как обычно происходит подготовка к IdM-проектам и почему стандартный подход не всегда работает
- Сколько IdM-проектов реализуется в России ежегодно

DevSecOps

- Какие проблемы возникают при интеграции процессов разработки, ИТ и ИБ
- Как выбрать инструменты для автоматизации процесса безопасной разработки

Кадровый вопрос

- Каких ИБ-специалистов не хватает прямо сейчас и кто будет в дефиците в ближайшие 5–7 лет
- ИБ-рынок в России — рынок соискателя или работодателя?
- Каким образом аутсорсинг решает проблему кадрового голода

«Нужно оставить позади парадигму рынка “все свое”. Она формировалась в то время, когда технологии для выхода на сервисные модели бизнеса просто отсутствовали. Конечно, вы можете сами построить ЦОД, в котором будет определенное количество серверов, дисковых мощностей, а также ноль возможностей для масштабирования. И быстро останетесь в прошлом».

Сергей Фомиченко,
начальник отдела информационной безопасности Корпорации МСП, MBA

РОССИЙСКИЙ РЫНОК IdM-РЕШЕНИЙ

2014–2018 ГГ.

Исследование компании «Инфосистемы Джет»

/ КАКИЕ IDM-РЕШЕНИЯ ПРЕДСТАВЛЕНЫ НА РОССИЙСКОМ РЫНКЕ

/ СКОЛЬКО IDM-ПРОЕКТОВ РЕАЛИЗУЕТСЯ ЕЖЕГОДНО

/ В КАКИХ ОБЛАСТЯХ ЭТИ РЕШЕНИЯ НАИБОЛЕЕ ВОСТРЕБОВАНЫ

/ КАК ИЗМЕНИЛОСЬ СООТНОШЕНИЕ ВНЕДРЕНИЙ РОССИЙСКИХ И ЗАРУБЕЖНЫХ IDM С 2014 ПО 2018 Г.

РОССИЯ	1IDM
	AVANPOST
	REDSYS
	«РОСТЕЛЕКОМ-СОЛАР»
	TRUSTVERSE
США	ORACLE
	ONE IDENTITY
	MICROSOFT
	SAILPOINT
	IBM
ГЕРМАНИЯ	SAP

ОБЪЕМ СТР.

Исследование посвящено рынку систем управления доступом — Identity Management *(IdM)*, или, как их часто называют в последнее время, Identity Governance & Administration *(IGA)*. Назначение этих систем — централизация и автоматизация управления учетными записями пользователей и правами доступа к информационным системам предприятия, повышение уровня контроля над использованием информационной инфраструктуры.

IdM подключается к системам компании и становится единой точкой управления учетными записями и контроля прав доступа. Как правило, IdM интегрируется с системой кадрового учета для получения информации о сотрудниках. На основании данных из кадрового источника автоматизируются бизнес-процессы управления доступом при приеме на работу, увольнении, переводе на другую должность или уходе в отпуск. Автоматизация этих процессов может включать как полностью автоматические действия, так и заранее заданную последовательность согласований.

IdM-решения часто путают с системами класса Access Management *(AM)*. В отличие от IdM, AM обеспечивают централизованную аутентификацию и авторизацию пользователей в системах, а также механизмы однократной *(SSO)* и строгой аутентификации. Эти решения в наш отчет не включены.

В 2017 г. наша компания провела первое в России исследование рынка управления доступом. Исследование российского рынка IdM-решений выпущено в конце 2019 г. Оно дополняет отчеты Gartner и Forrester статистикой внедрений IdM-решений в отечественных компаниях.

Мы подробнее проанализировали рынок за последние 5 лет *(с 2014 по 2018 г.)*, выбрав большее количество критериев.

99

IDM-ПРОЕКТОВ БЫЛО РЕАЛИЗОВАНО В РОССИИ В 2014–2018 ГГ.

Это в 2 раза больше, чем за предыдущую пятилетку. 49 внедрений IdM было реализовано в 2009–2013 гг.

ИСТОЧНИКИ

- **Запросы вендорам и дистрибьюторам.** Во второй половине 2019 г. мы направили запросы всем представленным на отечественном рынке вендорам IdM-решений и дистрибьюторам с просьбой предоставить информацию по внедрению их систем в России в 2014–2018 гг.
- **Открытые источники:** сайты вендоров, интернет-ресурсы с публикациями о проектах.
- **Собственная статистика.** Мы работаем на рынке IdM с 2005 г., отслеживаем и фиксируем ключевые события.
- **Данные наших архитекторов.** Эксперты в области IdM — довольно закрытое сообщество, внутри которого постоянно идет обмен информацией. Наши специалисты общаются с сотрудниками других компаний, благодаря чему могут проверить данные, поступающие из других источников.

Таблица 1 **Компании — разработчики IdM-решений, представленные в исследовании**

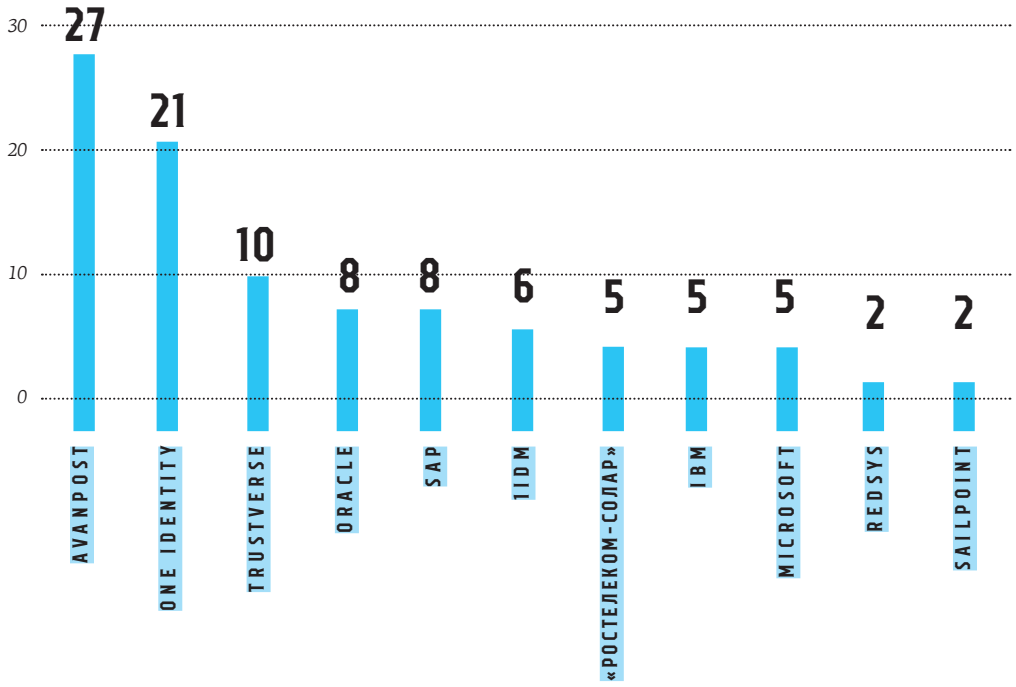
К сожалению, часть производителей и их представителей не предоставили нам информацию о внедрениях. Однако, по нашим данным, суммарная доля их проектов на российском рынке не превышает 1%. Эта цифра не может существенно повлиять на общие показатели.

СТАТИСТИКА ВНЕДРЕНИЙ

В связи с тем, что проекты по внедрению IdM длительные и масштабные, у нас не было возможности получить данные о качестве реализации и степени завершенности проектов, поэтому при оценке количества внедрений IdM-решений мы учитывали только старт проекта и факт поставки лицензий (см. рис. 1).

Три отечественных вендора *(1IDM, «Ростелеком-Солар» и Redsys)* вышли на рынок IdM в 2015 г. За несколько лет им удалось сравняться с игроками, внедряющими эти решения в России с 2000 гг.

Рисунок 1 **Количество внедрений IdM-решений отечественных и зарубежных вендоров в России, 2014–2018 гг.**



КОММЕНТАРИЙ

Александр Санин,
коммерческий директор компании Avanpost

Хотелось бы увидеть в исследовании финансовые показатели. Количество проектов, безусловно, главный признак востребованности продукта. Но когда у одной компании 5 проектов по 1 млн руб. каждый, а у другой 1 проект на 20 млн, это также важно для конкурентной оценки. Было бы полезно, если бы отчет включал данные об объеме и потенциале рынка в деньгах.

Наш ответ: «Задачей исследования было расширить спектр критериев выбора IdM-решения и осветить картину российского рынка. Это второе наше исследование, до этого статистика по российскому рынку отсутствовала. При выборе решения заказчики обращаются к отчетам Gartner и Forrester, но известно, что они занимаются аналитикой только зарубежного рынка и не учитывают отечественных вендоров. Мы планируем продолжать выпускать наш отчет, и, возможно, в следующий раз мы попробуем учесть финансовые показатели для более ясной картины».

ОТРАСЛЕВАЯ СЕГМЕНТАЦИЯ

Мы проанализировали изменение востребованности IdM-решений в разных отраслях за несколько периодов (см. рис. 2).

Компании финансового и государственного секторов лидируют по количеству внедрений IdM. Принципиальное различие между ними в том, что пик интереса финансовых компаний к IdM-решениям приходится на период с 2009 по 2013 г., а сейчас наблюдается небольшой спад. В то же время у организаций государственного сектора повышается интерес к IdM-проектам.

Рисунок 2 Отраслевая сегментация рынка IdM, %

Таблица 2. Отраслевая сегментация рынка IdM в разные периоды, %

Сектор	2004–2008	2009–2013	2014–2018
Финансы	**17,65**	**38,78**	**30,30**
Нефть и газ	**29,41**	**24,49**	**12,12**
Государственный сектор	**5,88**	**16,33**	**17,17**
Другие	**47,06**	**20,41**	**40,40**

Нефтегазовые компании проявляли наибольший интерес к подобным решениям в 2004–2008 гг., в этот период они лидировали на фоне других отраслей. За последний рассматриваемый период доля нефтегазового рынка сократилась вдвое.

Рассмотрим востребованность российских и зарубежных решений в зависимости от отрасли (см. рис. 3).

Традиционно считается, что в государственном секторе преобладают российские IdM-системы, и наши данные это подтверждают. Но, несмотря на политику импортозамещения, здесь все еще присутствуют решения зарубежных вендоров.

СЕГМЕНТАЦИЯ ПО КОЛИЧЕСТВУ ПОЛЬЗОВАТЕЛЕЙ В КОМПАНИЯХ

Существует мнение, что IdM-решения востребованы в компаниях со штатом от 1000 человек. На рис. 4 мы видим, что количество проектов в этом сегменте сравнимо с числом внедрений в компаниях с численностью сотрудников от 1001 до 5 000 и выше. Обозначить один из сегментов в качестве лидирующего невозможно, так как показатели существенно не отличаются.

Рисунок 3 Разделение сегментов рынка между российскими и зарубежными решениями, %

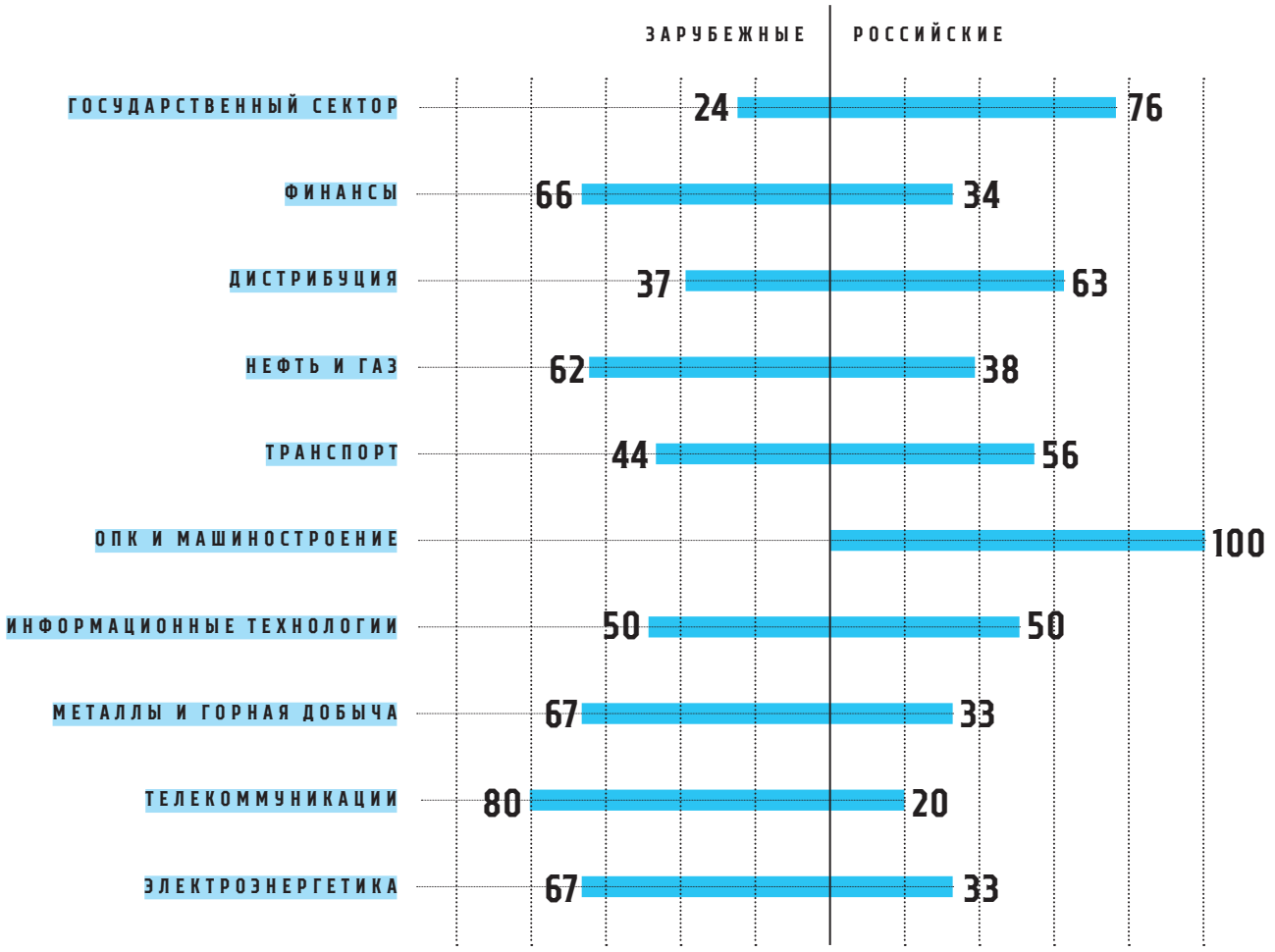
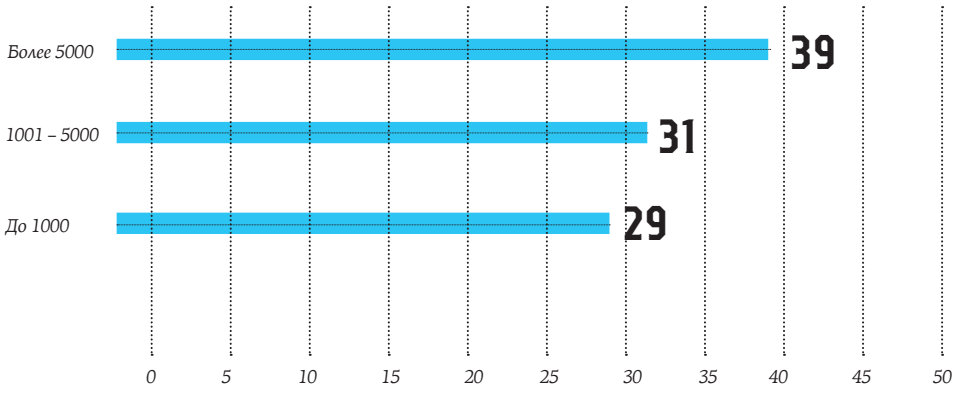


Рисунок 4 Количество внедрений IdM-решений в зависимости от численности сотрудников компаний



КОММЕНТАРИЙ

Олег Файницкий,

ведущий консультант по технологиям информационной безопасности компании Oracle СНГ

Было бы интересно понять сегментацию вендоров относительно масштаба компаний *(хотя бы относительно количества пользователей)*.

Наш ответ: представлен на рис. 5.

Рисунок 5 Распределение вендоров по количеству внедрений IdM-решений в компаниях с разной численностью

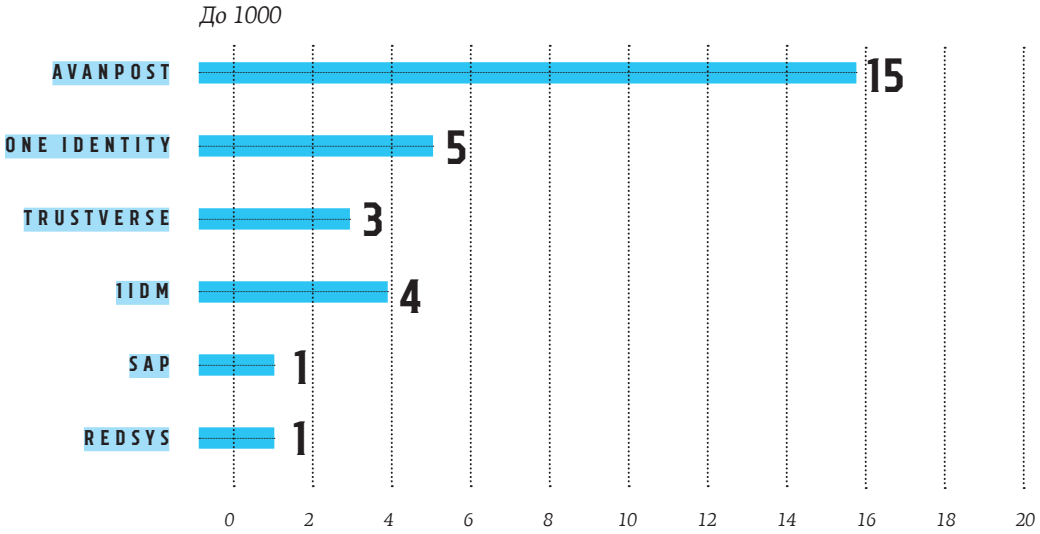
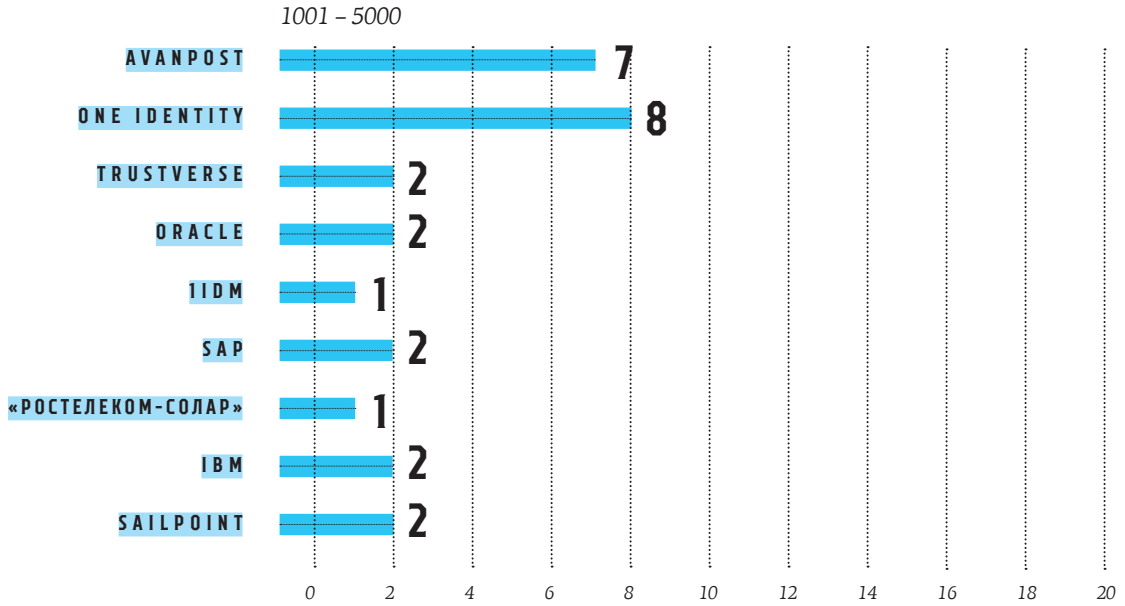
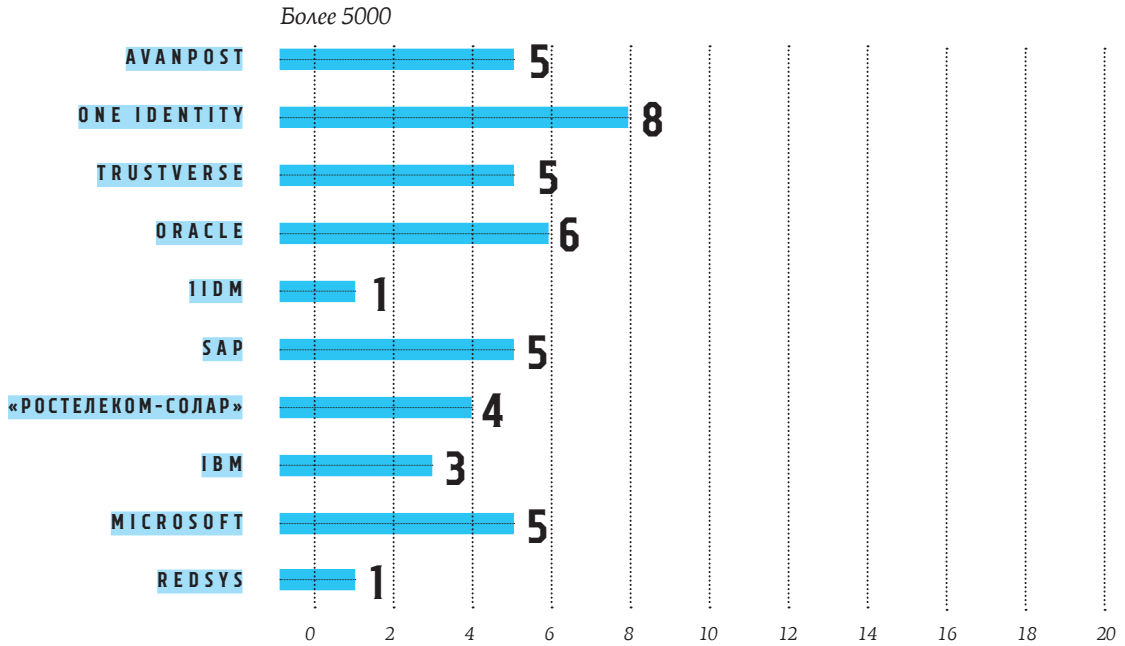


Рисунок 5 **Распределение вендоров по количеству внедрений IdM-решений в компаниях с разной численностью**

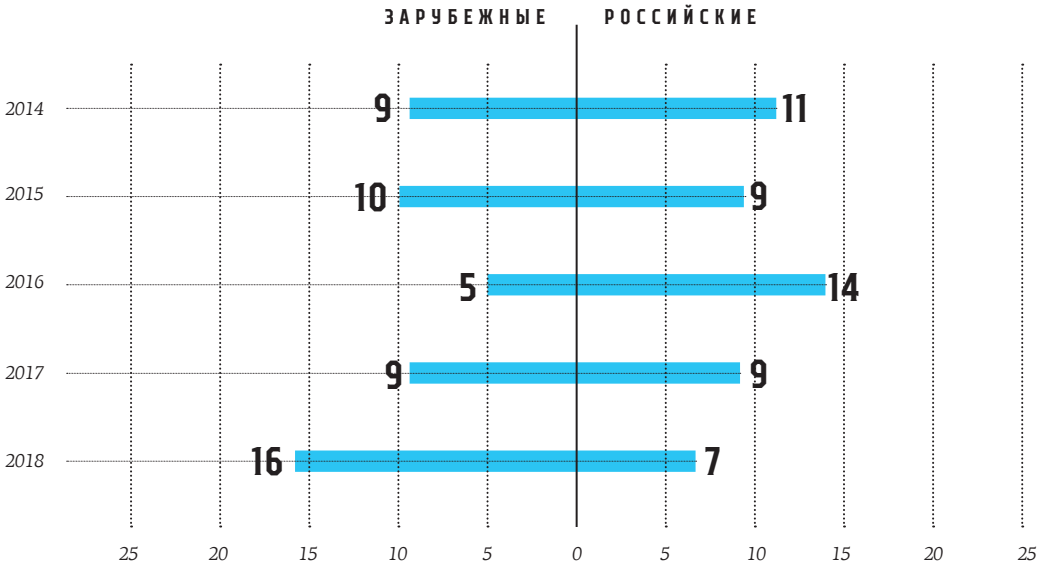




Если проанализировать распределение вендоров по количеству пользователей, можно заметить, что лидеры в разных сегментах меняются. В некоторых из них определенные производители не присутствуют, это может свидетельствовать о фокусировке на других сегментах. Однако разрыв между вендорами незначителен, и утверждать о сосредоточении на одном из типов заказчиков будет некорректно.

ДИНАМИКА ВНЕДРЕНИЙ

Рисунок 6 Количество внедрений IdM-решений по годам



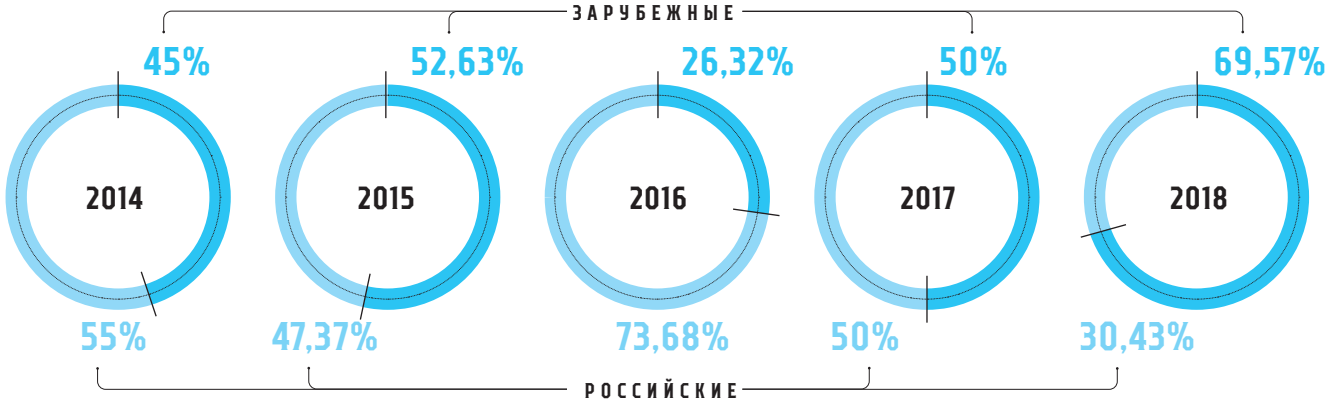


Таблица 3. Количество внедрений IdM-решений в разные годы

Год	Российские решения	Зарубежные решения	Итого
2014	11	9	20
2015	9	10	19
2016	14	5	19
2017	9	9	18
2018	7	16	23
2019	7	5	12
Итого (без 2019)	50	49	

КОММЕНТАРИЙ

Яков Фишелев,

руководитель представительства One Identity в России и СНГ:

Действительно, в 2014–2016 гг. появилось множество проектов на основе продуктов российских вендоров. У кого-то возникла иллюзия, что можно быстро заменить зарубежные решения, но затем рынок расставил все на свои места. Заказчики хотят качественные, зрелые системы. Никто не будет покупать решение просто потому, что оно российское *(кроме государственных организаций)*. Постепенно отечественные решения становятся более зрелыми, но это длительный процесс. Так, за последние 2 года уже 3 компании из числа тех, кто внедрял IdM в 2014–2016 гг., мигрировали на наш продукт. Это свидетельствует о том, что заказчики теперь гораздо тщательнее выбирают продукты, делают пилоты, ходят на референсы и не полагаются лишь на маркетинговую информацию. Надеюсь, что наша активная позиция на рынке будет способствовать дальнейшему развитию российских IdM-решений.

МИГРАЦИЯ ВНЕДРЕНИЙ

Мы решили рассмотреть еще один параметр — количество переходов с решения одного вендора на решение другого вендора.

Миграция началась только в 2016 г. и составляет более 11% относительно первоначальных внедрений. Мы связываем это с несколькими факторами. Во-первых, госкомпании мигрируют с зарубежного на отечественный софт. Во-вторых, организации, внедрившие IdM более 5 лет назад, вынуждены мигрировать на новое ПО, чтобы не тратить ресурсы на разработку функционала, который уже появился в новых версиях решений.

Рисунок 7 Соотношение первоначальных и миграционных внедрений IdM-решений по годам, %

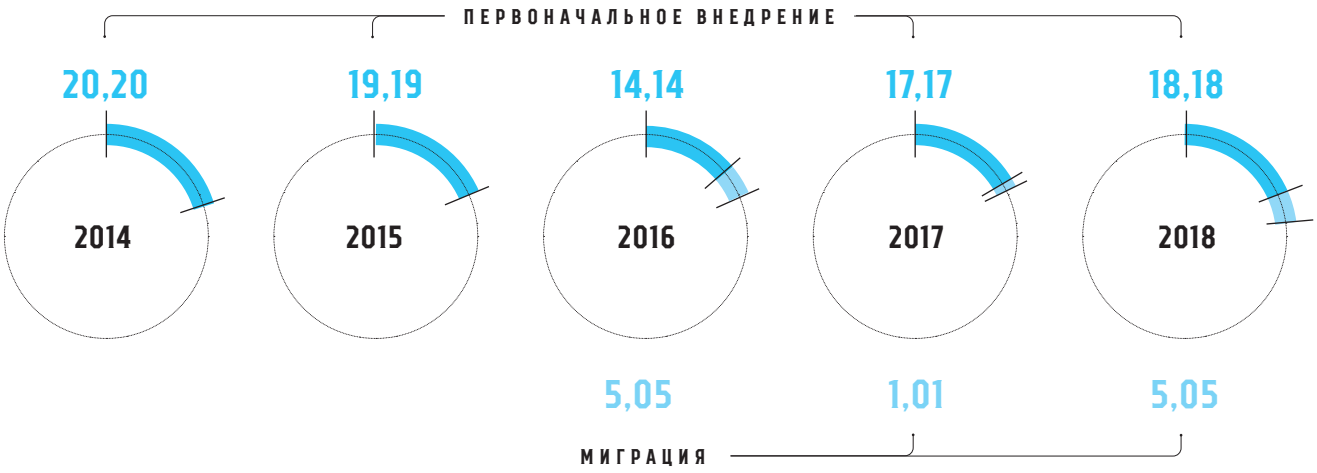
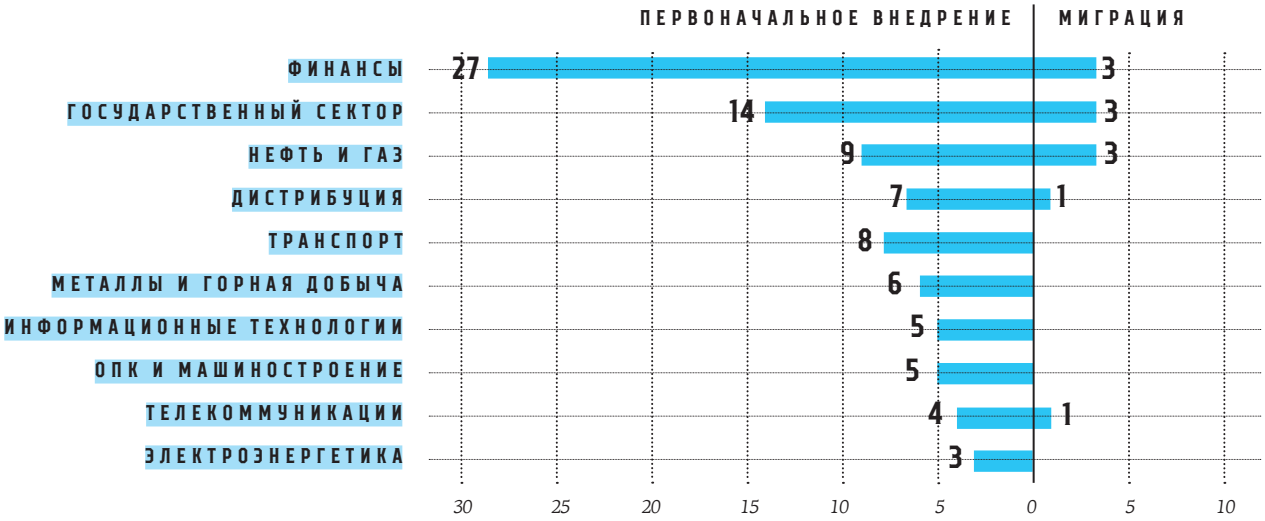


Рисунок 8 Отраслевое деление по количеству первоначальных и миграционных внедрений



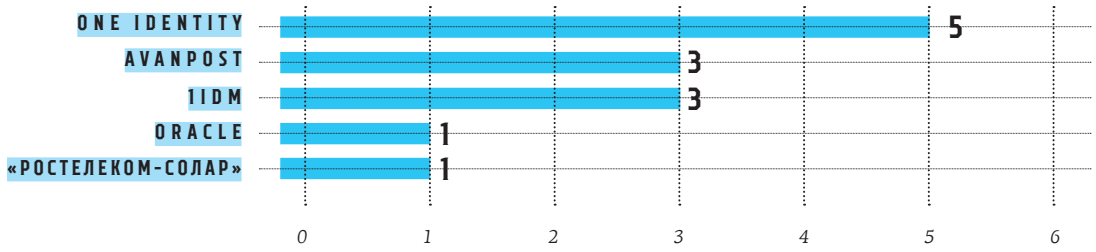
НАШ ПРОГНОЗ

За последние 5 лет популярность IdM значительно возросла. Количество внедрений с 2014 по 2018 г. составило 99, а за предыдущую пятилетку — 49. Наши эксперты ожидали подобного роста в связи с новым уровнем развития продуктов и политикой импортозамещения.

В перспективе ближайших трех лет серьезных изменений на рынке IdM не предвидится. Выделились два лидера, остальные игроки продолжают бороться за увеличение доли рынка, что подтверждает статистика 2019 г. Динамика внедрений сохранится на прежнем уровне, количество проектов не снизится по двум причинам. Во-первых, наметился спрос на IdM-решения в новых секторах: ИТ, пищевой промышленности, ритейле и др. Во-вторых, растет спрос на облачные IdM. На сегодняшний день подобные проекты — пока экзотика, по нашим данным, они составляют примерно 2% от общего числа всех внедрений, но мы ожидаем роста в этом сегменте рынка.

Не стоит также забывать о курсе на импортозамещение, которого придерживаются госкомпании. За последние несколько лет отечественные разработчики существенно продвинулись на пути создания IdM. Но это продолжительный процесс, и на данный момент по-прежнему наблюдается спрос на решения зарубежных вендоров.

Рисунок 9 Количество внедрений IdM-решений в России, 2019 г.



ТАК СЛОЖИЛОСЬ, ЧТО НЕ ПОЛУЧИЛОСЬ!

ПРАВИЛЬНЫЙ ПОДХОД К ВНЕДРЕНИЮ IDM

/ КАК ОБЫЧНО ОСУЩЕСТВЛЯЕТСЯ ПОДГОТОВКА К IDM-ПРОЕКТАМ И ПОЧЕМУ СТАНДАРТНЫЙ ПОДХОД НЕ ВСЕГДА РАБОТАЕТ

/ КАКИЕ ЭТАПЫ ДОЛЖНА ВКЛЮЧАТЬ ПОДГОТОВКА К ВНЕДРЕНИЮ IDM

/ ЧТО ДАЕТ АУДИТ ПЕРЕД СТАРТОМ IDM-ПРОЕКТА

АВТОР
Елизавета Тарасова,
аналитик отдела IdM-решений Центра прикладных систем безопасности компании «Инфосистемы Джет»

ОБЪЕМ СТР.

В процессе реализации проектов нам приходится решать различные проблемы. При этом многие из них возникают из-за того, что на этапе подготовки проекта остаются неучтенными важные детали, о которых становится известно уже в процессе внедрения. Например, в крупном банке в ходе выполнения проекта по внедрению IdM выяснилось, что в автоматизированной банковской системе *(АБС)*, которую требовалось подключить к IdM, не было механизма для взаимодействия — API. Произошло это, когда первый этап проекта уже был выполнен и стартовали работы по второму этапу. При этом управление учетными записями в АБС являлось основной целью внедрения IdM и ключевым требованием на проекте, а без API подключение этой системы не представлялось возможным. Банку пришлось привлечь разработчика АБС и приостановить проект по внедрению IdM — до реализации механизма. В результате бюджет проекта увеличился на сумму затрат на доработку системы, а сроки сдвинулись на 6 месяцев. Почему компании сталкиваются с подобными трудностями и как можно избежать неприятных сюрпризов при внедрении системы управления доступом, расскажем в статье.

ПОЧЕМУ НЕЛЬЗЯ ПРОСТО ВЗЯТЬ И ВНЕДРИТЬ IDM-РЕШЕНИЕ

Как правило, компании подходят к внедрению IdM так же, как и к реализации любого другого проекта. Обычно данный подход состоит из нескольких этапов.

Этап 1. Формирование общих требований

Сначала компании формируют перечень требований к IdM-решению. В большинстве случаев это происходит следующим образом. Компании отправляют запрос подрядчику с просьбой оценить стоимость IdM-решения. Подрядчик в ответ присылает опросный лист, состоящий из типовых вопросов. Как правило, они касаются четырех факторов:

- количество пользователей *(внутренних и внешних)*;
- подключаемые информационные системы;
- автоматизируемые процессы;
- разрабатываемые документы.

Далее компании формируют перечень требований. Такими требованиями могут быть:

- автоматизация процессов: прием на работу, перевод, увольнение;
- наличие штатного коннектора к системам MS AD, Exchange, 1С;
- запрос прав доступа по заявке;
- ведение справочника внешних пользователей.

Эти требования являются верхнеуровневыми и не отражают всех особенностей того, как это должно быть сделано в проекте. Так, в крупной металлургической компании одним из требований было ведение справочника внешних пользователей — работников подрядных организаций. Данный функционал был реализован в следующем объеме: куратор в IdM-системе регистрирует внешнего пользователя, после чего IdM-система предоставляет ему необходимый доступ в информационные системы. Однако в ходе промышленной эксплуатации системы выяснилось, что данного функционала недостаточно. Из компании уволился сотрудник, за которым было закреплено больше 50 внешних пользователей, и всех их потребовалось перевести на другого работника. Для этого компании пришлось создавать 50 отдельных заявок, так как в системе не было возможности массового переноса подрядчиков в рамках одной заявки. В результате решение пришлось дорабатывать, что привело к дополнительным расходам на реализацию проекта. Однако этого можно было избежать, добавив на начальном этапе требование реализовать массовый перенос внешних пользователей в рамках одной заявки.

Этап 2. Выбор платформы

На данном этапе компании ищут решение, которое бы соответствовало общим

требованиям. При выборе они используют сведения из открытых источников, а также запрашивают данные у вендоров и интеграторов. На основе этой информации компании формируют сравнительную таблицу, в которой отмечают наличие того или иного функционала, стоимость решения, количество внедрений, наличие решения в рейтингах аналитических агентств Gartner и Forrester. В большинстве случаев ключевыми критериями для выбора являются функционал и стоимость. Если провести сравнение представленных на российском рынке решений на основе общих требований, то можно прийти к выводу, что все они одинаковые. Соответственно, это приводит к тому, что зачастую выбор осуществляется на основе одного критерия — стоимости решения. На самом деле отличия в системах есть, только для их выявления требуется проводить более детальное сравнение.

Этап 3. Пилотный проект

Еще одним фактором, влияющим на окончательный выбор решения, является демонстрация его работы. Для этого вендор или интегратор выполняет пилотный проект. Как правило, для пилота создаются «лабораторные условия»: выделяются тестовая среда и тестовые данные в кадровой и информационных системах, а также выбирается наиболее простой для реализации и последующей демонстрации функционал *(например, интеграция с системами AD и Exchange, управление учетными записями при приеме на работу и увольнении сотрудников)*. Однако зачастую «лабораторные условия» в корне отличаются от реальных данных и процессов. В ходе пилотного тестирования крайне сложно обнаружить ситуации, которые могут возникнуть при промышленной эксплуатации системы. Как это произошло в случае с внешними пользователями. В ходе пилотного проекта был продемонстрирован функционал по регистрации внешних пользователей, что соответствовало требованию к решению. А потребность в массовой заявке по переназначению внешних пользователей не была выявлена, так как в лабораторных условиях подобная ситуация едва ли может возникнуть.

ЗАЧАСТУЮ «ЛАБОРАТОРНЫЕ УСЛОВИЯ» В КОРНЕ ОТЛИЧАЮТСЯ ОТ РЕАЛЬНЫХ ДАННЫХ И ПРОЦЕССОВ. В ХОДЕ ПИЛОТНОГО ТЕСТИРОВАНИЯ IDM КРАЙНЕ СЛОЖНО ОБНАРУЖИТЬ СИТУАЦИИ, КОТОРЫЕ МОГУТ ВОЗНИКНУТЬ ПРИ ПРОМЫШЛЕННОЙ ЭКСПЛУАТАЦИИ СИСТЕМЫ.

После проведения всех процедур компания уже может начать проект по внедрению IdM: сформированы общие требования, выбрано подходящее решение, подтвержденное пилотным тестированием. Осталось только найти подрядчика для выполнения проекта. С этой целью компании запускают процедуру сбора предложений RFP. В ответ на запрос они получают предложения от подрядчиков, стоимость работ в которых может варьироваться от миллиона до сотни миллионов рублей, а длительность — от нескольких месяцев до нескольких лет. Такую существенную разницу мы объясняем тем, что одни подрядчики учитывают в предложении выполнение дополнительных работ, которые могут возникнуть в ходе выполнения проекта, а другие этого не делают (см. рис. 1 и рис. 2).. Рассмотрим пример одного из требований — автоматизации процесса приема сотрудника на работу. Если смотреть на него «в лоб», его реализация будет представлять процесс, состоящий из нескольких простых шагов. Несмотря на то что процесс будет автоматизирован, а требование формально выполнено, на практике может оказаться, что данный функционал окажется неудобным для использования. Произойдет это потому, что в таком варианте учитываются не все кейсы, возникающие при приеме на работу: совместительство, повторный прием на работу, отправка SMS-сообщения сотруднику с первоначальным паролем от учетных записей и т.д. Для решения проблемы в процесс нужно добавить дополнительные условия и действия.

Это, в свою очередь, приводит к увеличению стоимости и сроков IdM-проекта.

Тем не менее компании считают разницу в стоимости и сроках парадоксальной: им кажется, что в предложения включены одинаковые работы. Поэтому в большинстве случаев делается выбор в пользу предложений с минимальной стоимостью услуг. Как результат — множество проблем на проекте. И дело не только в последующем увеличении бюджета и сроков проекта. Бывают случаи, когда подрядчик выполняет проект формально: «реализует систему строго по ТЗ», а не в соответствии с реальными требованиями компании. В итоге реализованной системой просто невозможно пользоваться.

КАК МЫ ПЫТАЛИСЬ РЕШИТЬ ЭТИ ПРОБЛЕМЫ «ПО-ПРОСТОМУ»

Казалось бы, чтобы избежать перечисленных проблем, необходимо составлять более детальные требования и проводить пилотное тестирование наиболее сложного функционала с использованием реальных данных. Но, по нашему опыту, на практике такой сценарий не работает. Для составления детальных требований мы отправляли компаниям расширенные опросные листы, сгруппированные по тематикам: бизнес-процессы, интеграция с информационной системой, нефункциональные требования и т.д. Каждый из них содержал в среднем 70–80 вопросов. Однако мы ни разу не получили полностью и корректно заполненные опросные листы. Это связано с тем, что, во-первых, ответы на такое большое количество вопросов *(для компании с 5 системами — около 800 вопросов)* требуют много времени, а во-вторых, делать это должен опытный специалист, понимающий специфику работы IdM-системы и особенности ее внедрения.

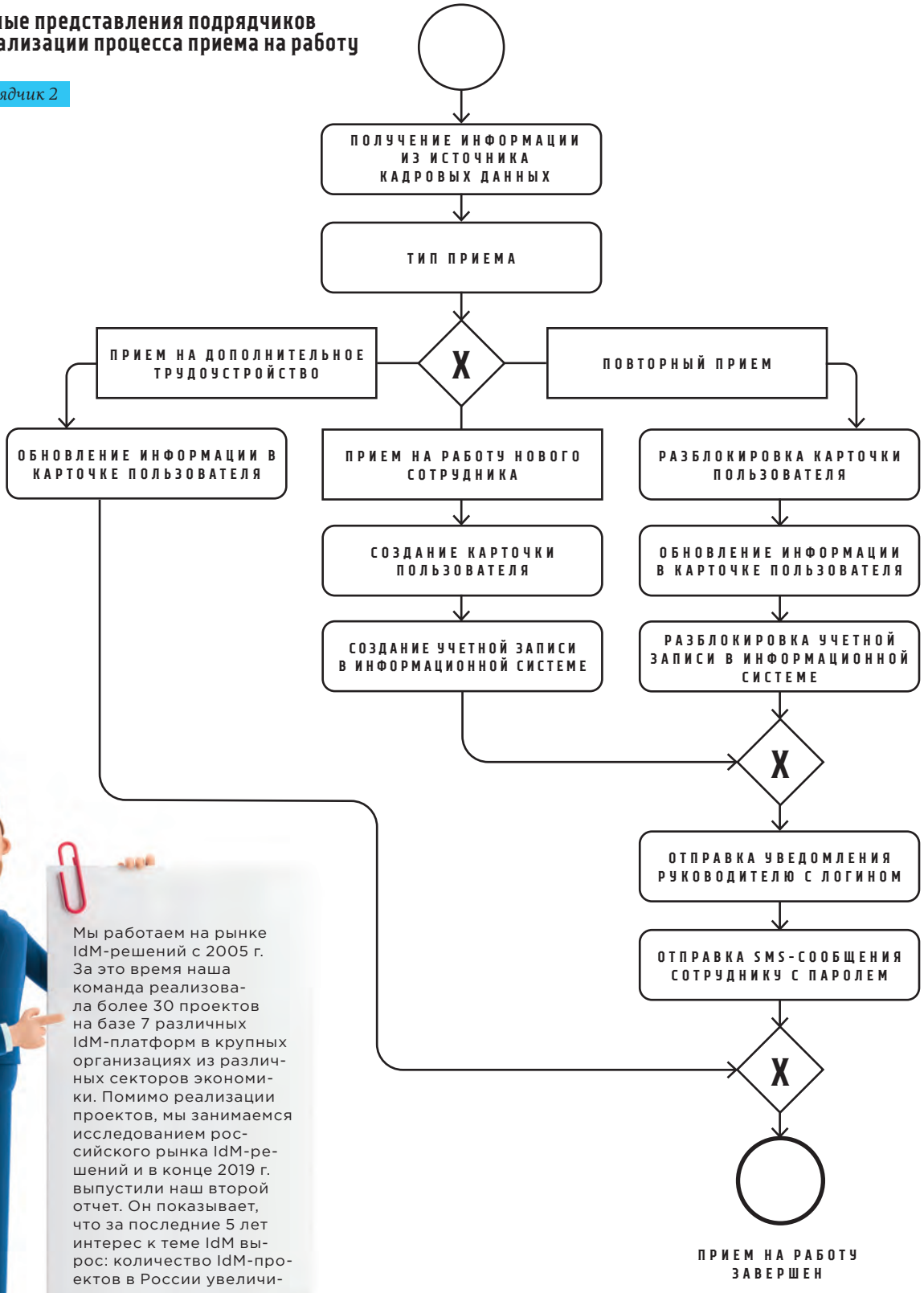
Что касается пилотного проекта, то для его проведения в условиях, наиболее приближенных к реальным, необходимо выполнить большой объем подготовительных работ. В основном это обследование автоматизируемых процессов и подключаемых систем, доработка IdM-системы, созда-

Рисунок 1. **Разные представления подрядчиков о реализации процесса приема на работу**

БЫВАЮТ СЛУЧАИ, КОГДА ПОДРЯДЧИК ВЫПОЛНЯЕТ IDM-ПРОЕКТ ФОРМАЛЬНО: «РЕАЛИЗУЕТ СИСТЕМУ СТРОГО ПО ТЗ», А НЕ В СООТВЕТСТВИИ С РЕАЛЬНЫМИ ТРЕБОВАНИЯМИ КОМПАНИИ. В ИТОГЕ РЕАЛИЗОВАННОЙ СИСТЕМОЙ ПРОСТО НЕВОЗМОЖНО ПОЛЬЗОВАТЬСЯ.

Рисунок 2. Разные представления подрядчиков о реализации процесса приема на работу

Подрядчик 2



Мы работаем на рынке IdM-решений с 2005 г. За это время наша команда реализовала более 30 проектов на базе 7 различных IdM-платформ в крупных организациях из различных секторов экономики. Помимо реализации проектов, мы занимаемся исследованием российского рынка IdM-решений и в конце 2019 г. выпустили наш второй отчет. Он показывает, что за последние 5 лет интерес к теме IdM вырос: количество IdM-проектов в России увеличилось почти вдвое.

ние копий продуктивных данных. В этом случае пилотный проект перерастает в полноценный проект по внедрению, что приводит к увеличению стоимости и срока его проведения. Поэтому в большинстве случаев ни компания, ни подрядчик не готовы брать на себя такие расходы.

ПРАВИЛЬНЫЙ ПОДХОД К ПОДГОТОВКЕ IDM-ПРОЕКТА

Чтобы не столкнуться с вышеописанными проблемами, мы предлагаем использовать следующий подход при подготовке к проекту по внедрению IdM (см. рис. 3).

Шаг первый. Определение проблем

Сначала необходимо выяснить, какие проблемы должно решить внедрение IdM, и определить, подходит ли для этого подобный класс систем. Мы сталкивались с ситуациями, когда средствами IdM компании пытались решить задачи, для которых она не предназначена. Так, например, в одной компании ключевой задачей перед проектом по внедрению IdM было мгновенное оповещение специалистов ИБ о несанкционированном изменении прав доступа в информационных системах. Действительно, эту задачу можно решить и с помощью IdM, разработав модуль, реализующий такой функционал. Однако IdM не предназначена для выполнения подобного рода задач. Для этого целесообразно применять другой класс решений — SIEM. Поэтому на данном этапе важно определить, правильный ли инструмент компания планирует использовать для решения существующих проблем.

Шаг второй. Аудит процессов и ИС

Как правило, IdM-проекты являются сложными и масштабными и затрагивают множество областей в компании. Поэтому на следующем этапе после определения проблем необходимо провести аудит, то есть обследовать те области, на которые влияет и от которых зависит внедрение IdM. Мы предлагаем аудит следующих областей (см. рис. 4).

В ходе обследования процессов управления доступом важно определить два основных момента. Во-первых, необходимо выяснить, как в действительности в компании осуществляются процессы управления доступом. Ведь зачастую процессы, описанные в регламентах или других документах компании, в жизни исполняются лишь частично либо по совершенно другому сценарию. Во-вторых, нужно оценить возможность автоматизации этих процессов. В случае, если текущие процессы автоматизировать невозможно, нужно определить необходимость и возможность их изменения. Бывают ситуации, когда текущие процессы изменить нельзя и это становится стоп-фактором для внедрения IdM. Например, в одной компании в начале каждого месяца существует 10-дневный тайм-аут по внесению информации о кадровых мероприятиях в кадровую систему, то есть

Рисунок 3. Правильный подход к подготовке IdM-проекта

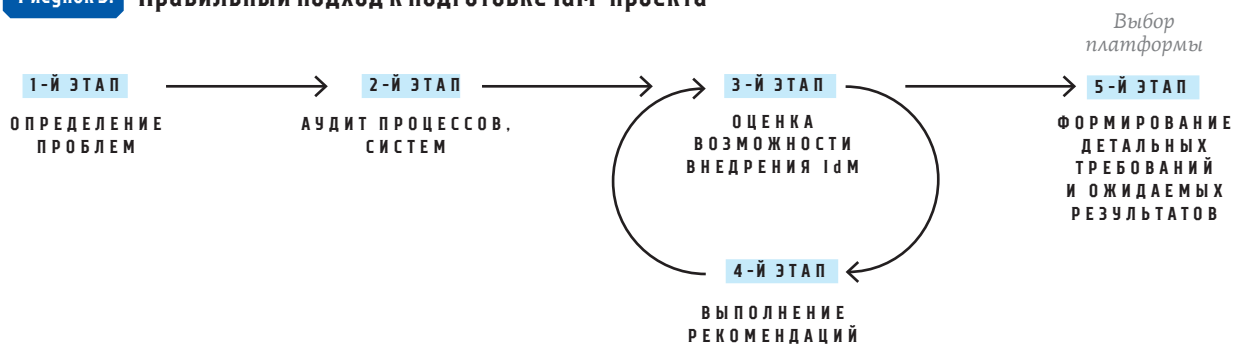
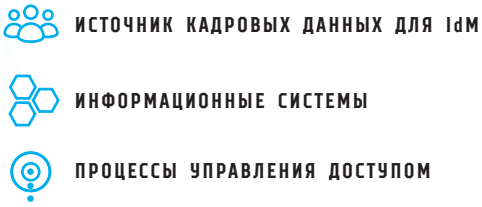


Рисунок 4. **Аудит процессов, информационных систем и источника кадровых данных**



в этот период IdM не сможет получать данные о кадровых мероприятиях и выполнять операции по управлению правами доступа. Изменение текущего процесса не представлялось возможным, поскольку это требовало изменений процедуры расчета заработной платы и работы кадровой системы. В результате кадровые процессы были автоматизированы частично.

На следующем шаге нужно провести аудит систем компании. Требуется сформировать их перечень, определить критичность, а также необходимость и целесообразность подключения к IdM. Кроме того, необходимо выявить внутреннюю логику управления доступом и выбрать способы подключения информационных систем к IdM. В случае, если у системы нет механизма для взаимодействия, рассматриваются варианты его разработки либо подключения системы как неуправляемой[1]. После этого следует выяснить внутреннюю логику управления доступом в системах, то есть установить, какие объекты внутри них отвечают за предоставление доступа. Это делается, для того чтобы определить варианты переноса такой логики в IdM. Идеология работы IdM-решений основана на модели RBAC *(Role Based Access Control)*. Это означает, что IdM управляет доступом только на основе ролей без управления атомарными полномочиями. Однако существуют системы, в которых, помимо ролей для управления доступом, используются дополнительные параметры. Это могут быть профили, группы, справочники и т.д. Для распространенных систем, например SAP, производители IdM-решений разработали коннектор, который позволяет управлять доступом, используя не только роли, но и дополнительные параметры. Однако это единичные примеры, и для нераспространенных или самописных систем есть два варианта подключения к IdM. Первый подразумевает, что IdM будет управлять доступом в этих системах только на уровне ролей, а второй — что вся внутренняя логика управления доступом будет перенесена в IdM. В последнем случае компании должны быть готовы к существенному увеличению стоимости подключения данной системы, а также к тому, что любое изменение логики управления доступом внутри системы потребует переработки функционала подключения этой системы.

Еще одна область, которую необходимо обследовать в рамках аудита, — кадровая система. Следует проанализировать текущие кадровые данные, чтобы выявить их специфику и определить полноту. Это нужно, для того чтобы оценить, достаточно ли текущих данных в кадровой системе для автоматизации процессов в IdM. Предположим, в компании 5000 сотрудников и десятой части из них не требуются рабочее место и доступ в системы. Создание учетных записей в IdM и информационных системах для них влечет за собой избыточный расход лицензий. Чтобы этого не произошло, IdM-решение должно получать информацию о том, что для этих сотрудников не требуется создавать учетные записи. Соответственно, нужно, чтобы в кадровой системе существовал признак необходимости рабочего места и его корректно заполняли специалисты кадрового учета.

Шаги третий и четвертый. Оценка возможности внедрения IdM и выполнение рекомендаций

После проведения аудита необходимо оценить, возможно ли в текущий момент внедрить IdM в компании и достичь поставленных целей. На данном этапе анализируются все данные, полученные в ходе аудита, проверяется, есть ли стоп-факторы, и определяются дальнейшие действия. **Здесь может быть множество вариантов:**

[1] Неуправляемая информационная система — система, управление правами доступа пользователей в которой автоматизируется посредством создания заявки на ее администратора в IdM. После этого он выполняет ее вручную.

Таблица 1. Оценка возможности подключения систем и автоматизации процессов

СИСТЕМА	КОЛИЧЕСТВО ПОЛЬЗОВАТЕЛЕЙ	КРИТИЧНОСТЬ	СТАТУС
КАДРОВАЯ СИСТЕМА 1С	-	Высокая	Подключение
MICROSOFT ACTIVE DIRECTORY	5000	Высокая	Подключение
MICROSOFT EXCHANGE	5000	Высокая	Подключение
1С УПРАВЛЯЕМАЯ СИСТЕМА	300	Средняя	Требуемая разработка механизма взаимодействия
СИСТЕМА БУХГАЛТЕРСКОГО УЧЕТА	10	Средняя	Подключение нецелесообразно
ITSM-СИСТЕМА	5000	Средняя	Требуется доработка системы

ПРОЦЕСС	СТАТУС
ПРИЕМ НА РАБОТУ, ПЕРЕВОД, УВОЛЬНЕНИЕ	Возможна частичная автоматизация Отсутствует признак необходимости рабочего места
ПРИЕМ НА ПОДОЛНИТЕЛЬНОЕ ТРУДОУСТРОЙСТВО	Полная автоматизация
ИЗМЕНЕНИЕ УЧЕТНОЙ ЗАПИСИ ПРИ ИЗМЕНЕНИИ ФИО	Полная автоматизация
ДОБАВЛЕНИЕ ОБЪЕКТА В ОРГАНИЗАЦИОННО-ШТАТНУЮ СТРУКТУРУ	Частичная автоматизация Неактуальная ОШС в кадровой системе
УДАЛЕНИЕ ОБЪЕКТА ИЗ ОРГАНИЗАЦИОННО-ШТАТНОЙ СТРУКТУРЫ	Частичная автоматизация Неактуальная ОШС в каждой системе
СМЕНА КУРАТОРА ДЛЯ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ	Автоматизация возможна Требуется доработка
ПРЕДОСТАВЛЕНИЕ ДОСТУПА К СИСТЕМЕ ПО ЗАЯВКЕ	Автоматизация возможна Требуется доработка

Таблица 2. Оценка возможности внедрения IdM

	ПРОЦЕССЫ	СИСТЕМЫ
ЭТАП 1	· ПРИЕМ НА РАБОТУ, ПЕРЕВОД, УВОЛЬНЕНИЕ · ИЗМЕНЕНИЕ УЧЕТНОЙ ЗАПИСИ ПРИ ИЗМЕНЕНИИ ФИО · ДОБАВЛЕНИЕ ОБЪЕКТА В ОРГАНИЗАЦИОННО-ШТАТНУЮ СТРУКТУРУ · УДАЛЕНИЕ ОБЪЕКТА ИЗ ОРГАНИЗАЦИОННО-ШТАТНОЙ СТРУКТУРЫ	КАДРОВАЯ СИСТЕМА 1С MICROSOFT ACTIVE DIRECTORY MICROSOFT EXCHANGE
ЭТАП 2	· ОБРАБОТКА ПРИЗНАКА РАБОЧЕГО МЕСТА ПРИ ПРИЕМЕ НА РАБОТУ · ПРЕДОСТАВЛЕНИЕ ДОСТУПА К СИСТЕМЕ ПО ЗАЯВКЕ · ПРЕКРАЩЕНИЕ ДОСТУПА К СИСТЕМЕ ПО ЗАЯВКЕ	1С УПРАВЛЯЕМАЯ СИСТЕМА ITSM-СИСТЕМА

- старт проекта по внедрению IdM-решения в полном объеме;
- выполнение рекомендаций, доработка систем и изменение процессов, старт проекта после выполнения этих действий;
- разделение проекта по этапам, старт первого этапа, доработка систем и изменение процессов, подключаемых на дальнейших этапах;
- и др.

Суть этапа наглядно продемонстрирована в табл. 1. В результате этих действий мы получаем перечень подключаемых систем, процессов и разделение работ по этапам.

Исходя из нашего опыта, мы можем сказать, что проведение оценки помогает снизить вероятность возникновения проблем на проекте. Так, в одной энергетической компании на начальном этапе требовалось за полгода внедрить централизованную IdM-систему в 40 юридических

лицах компании и подключить к ней 16 информационных систем. После проведения аудита стало понятно, что в каждом юридическом лице был собственный кадровый источник, большинство информационных систем не имели механизмов взаимодействия и во многих из них управление происходило без использования ролей. Результаты оценки возможности внедрения показали, что IdM-проект можно запустить лишь после выполнения определенных действий. При этом проект по внедрению требовалось разделить на этапы: 1) сначала подключить системы, в которых есть механизмы для взаимодействия и используется ролевое управление доступом; 2) параллельно доработать другие информационные системы; 3) только после этого подключить оставшиеся системы. При таком сценарии первоначально запланированные 6 месяцев реализации превращаются в 3 года. Нетрудно представить, к каким проблемам привел бы запуск проекта без проведения аудита.

Шаг пятый. Формирование детальных требований

Удостоверившись в том, что рекомендованные действия выполнены и внедрение возможно, переходим к следующему этапу — формированию детальных требований. После проведения аудита подготовить этот документ не составит труда. По результатам аудита формируется детальный отчет, в котором отражается текущая ситуация по всем обследуемым системам и процессам. Информация из данного отчета упрощает процесс формирования требований, а сам отчет можно использовать в качестве приложения к RFP. К тому же еще один этап подготовки к проекту — выбор решения — будет происходить как бы в фоновом режиме, так как при наличии детальных требований сделать это гораздо проще: нужно лишь направить перечень требований вендору или интегратору, который ответит, удовлетворяет ли предлагаемый им продукт указанным требованиям.

МЫ СТАЛКИВАЛИСЬ С СИТУАЦИЯМИ, КОГДА СРЕДСТВАМИ IDM КОМПАНИИ ПЫТАЛИСЬ РЕШИТЬ ЗАДАЧИ, ДЛЯ КОТОРЫХ ОНА НЕ ПРЕДНАЗНАЧЕНА.

ПРАВИЛЬНЫЙ ПОДХОД: ЗА И ПРОТИВ

ЗА ПОЧТИ 15 ЛЕТ РАБОТЫ НА РЫНКЕ IDM-РЕШЕНИЙ МЫ ПРИНЯЛИ УЧАСТИЕ В БОЛЬШОМ КОЛИЧЕСТВЕ КОНКУРСОВ. НА НАШ ВЗГЛЯД, В СРАВНЕНИИ С ПОДХОДОМ БЕЗ АУДИТА, ПРЕДЛАГАЕМЫЙ НАМИ ПОДХОД К ПОДГОТОВКЕ ПРОЕКТОВ ПО ВНЕДРЕНИЮ IDM ВЫИГРЫШНО ОТЛИЧАЕТСЯ ТЕМ, ЧТО ПОЗВОЛЯЕТ СУЩЕСТВЕННО МИНИМИЗИРОВАТЬ РИСКИ И ПОВЫСИТЬ ВЕРОЯТНОСТЬ ДОСТИЖЕНИЯ ПОСТАВЛЕННЫХ ЦЕЛЕЙ. ДЛЯ ПОДТВЕРЖДЕНИЯ ЭТОГО ВЫВОДА ПРИВЕДЕМ РЕЗУЛЬТАТЫ СРАВНЕНИЯ ДВУХ ВЫШЕОПИСАННЫХ ПОДХОДОВ. МЫ ПРОАНАЛИЗИРОВАЛИ ДАННЫЕ ОБ ОТКРЫТЫХ КОНКУРСАХ (СМ. ТАБЛ. 3).

В ПРОЕКТАХ С АУДИТОМ КОЛИЧЕСТВО УЧАСТНИКОВ БЫЛО ЗАМЕТНО МЕНЬШЕ. ПРИ ЭТОМ РАЗНИЦА В СТОИМОСТИ ПРЕДЛОЖЕНИЙ В ТАКИХ ПРОЕКТАХ ОКАЗАЛАСЬ НЕЗНАЧИТЕЛЬНОЙ, В ОТЛИЧИЕ ОТ ТЫСЯЧЕКРАТНОГО РАЗБРОСА, КОТОРЫЙ МЫ ВИДИМ В КОНКУРСАХ, ГДЕ ПОДГОТОВКА ПРОИСХОДИЛА БЕЗ АУДИТА. ИСХОДЯ ИЗ ЭТИХ ДАННЫХ, МОЖНО ПРЕДПОЛОЖИТЬ,

Таблица 3. **Сравнение конкурсов с использованием традиционного и предлагаемого нами подходов к подготовке к IdM-проекту**

	ТРАДИЦИОННЫЙ ПОДХОД	ПРАВИЛЬНЫЙ ПОДХОД
КОЛИЧЕСТВО УЧАСТНИКОВ В КОНКУРСЕ	6—8	3—4
КОЛИЧЕСТВО ВЕНДОРОВ В КОНКУРСЕ	4—7	1—3
РАЗБРОС ПО СТОИМОСТИ РАБОТ МЕЖДУ УЧАСТНИКАМИ	До 1000%	10—30%

ЧТО ИЗ МЕНЬШЕГО ЧИСЛА УЧАСТНИКОВ С РАВНЫМИ ПО СТОИМОСТИ ПРЕДЛОЖЕНИЯМИ ВЕРОЯТНОСТЬ ВЫБРАТЬ ПОДРЯДЧИКА, КОТОРЫЙ ВЫПОЛНИТ ПРОЕКТ, СУЩЕСТВЕННО ВЫШЕ.

НЕСМОТРЯ НА ВСЕ ПРЕИМУЩЕСТВА, ПРЕДЛАГАЕМЫЙ НАМИ ПОДХОД ИМЕЕТ И МИНУСЫ. ПЕРВЫЙ И САМЫЙ СУЩЕСТВЕННЫЙ ИЗ НИХ — ФИНАНСОВЫЙ. ПРОВЕДЕНИЕ АУДИТА ТРЕБУЕТ ДЕНЕГ, ВРЕМЕНИ И РЕСУРСОВ НЕЗАВИСИМО ОТ ТОГО, БУДЕТ ЛИ ОН ПРОВОДИТЬСЯ ПОДРЯДЧИКОМ ИЛИ СИЛАМИ КОМПАНИИ. В ПОСЛЕДНЕМ СЛУЧАЕ ОБЯЗАТЕЛЬНЫМ УСЛОВИЕМ ЯВЛЯЕТСЯ НАЛИЧИЕ СПЕЦИАЛИСТОВ, ОБЛАДАЮЩИХ ЭКСПЕРТНЫМИ ЗНАНИЯМИ И ОПЫТОМ ВНЕДРЕНИЯ IDM-РЕШЕНИЙ. КАК ПРАВИЛО, СТОИМОСТЬ АУДИТА ПРИМЕРНО РАВНА СТОИМОСТИ ЭТАПА ПРОЕКТИРОВАНИЯ. АУДИТ НЕ ДАЕТ ГАРАНТИИ ГОТОВНОСТИ КОМПАНИИ К ВНЕДРЕНИЮ И ВОЗМОЖНОСТИ ЗАПУСКА ПРОЕКТА. КОМПАНИЯ МОЖЕТ ПОТРАТИТЬ ДЕНЕЖНЫЕ СРЕДСТВА НА ПРОВЕДЕНИЕ АУДИТА, А ЕГО РЕЗУЛЬТАТЫ ПОКАЖУТ, ЧТО НА ТЕКУЩИЙ МОМЕНТ ВНЕДРЕНИЕ IDM НЕ ПРЕДСТАВЛЯЕТСЯ ВОЗМОЖНЫМ. ДЛЯ КОМПАНИИ ЭТО БУДЕТ ОЗНАЧАТЬ, ЧТО ДЕНЬГИ И ВРЕМЯ ПОТРАЧЕНЫ ВПУСТУЮ. С ДРУГОЙ СТОРОНЫ, ПРЕДПОЛОЖИМ, ЧТО КОМПАНИЯ ЗАПУСТИЛА ПРОЕКТ БЕЗ ПРОВЕДЕНИЯ АУДИТА И ЗАЛОЖИЛА ДЕСЯТКИ МИЛЛИОНОВ РУБЛЕЙ И ДЕСЯТКИ МЕСЯЦЕВ НА ЕГО ВЫПОЛНЕНИЕ. ПРИ ЭТОМ ПОСЛЕ ВЫПОЛНЕНИЯ ПОЛОВИНЫ РАБОТ ВЫЯВИЛИСЬ СТОП-ФАКТОРЫ ИЛИ ПРОБЛЕМЫ, УСТРАНЕНИЕ КОТОРЫХ ПОТРЕБОВАЛО ДОПОЛНИТЕЛЬНЫХ СРЕДСТВ И ВРЕМЕНИ. ПОЛУЧАЕТСЯ, ЧТО ВО ВТОРОМ СЛУЧАЕ КОМПАНИЯ ТЕРЯЕТ ЗНАЧИТЕЛЬНО БОЛЬШЕ ВРЕМЕНИ И СРЕДСТВ.

ВТОРОЙ НЕДОСТАТОК ЗАКЛЮЧАЕТСЯ В ТОМ, ЧТО ПОСЛЕ ПОЛУЧЕНИЯ РЕЗУЛЬТАТОВ АУДИТА КОМПАНИИ ПРЕКРАЩАЮТ АКТИВНОСТЬ ПО ПОДГОТОВКЕ К ПРОЕКТУ ПО ВНЕДРЕНИЮ IDM. МНОГИЕ РУКОВОДИТЕЛИ, УЗНАВ, КАКОЙ ОБЪЕМ РАБОТ ТРЕБУЕТСЯ ВЫПОЛНИТЬ ПЕРЕД ВНЕДРЕНИЕМ IDM-РЕШЕНИЯ, «ОПУСКАЮТ РУКИ» И ОТКАЗЫВАЮТСЯ ОТ ПРОЕКТА.

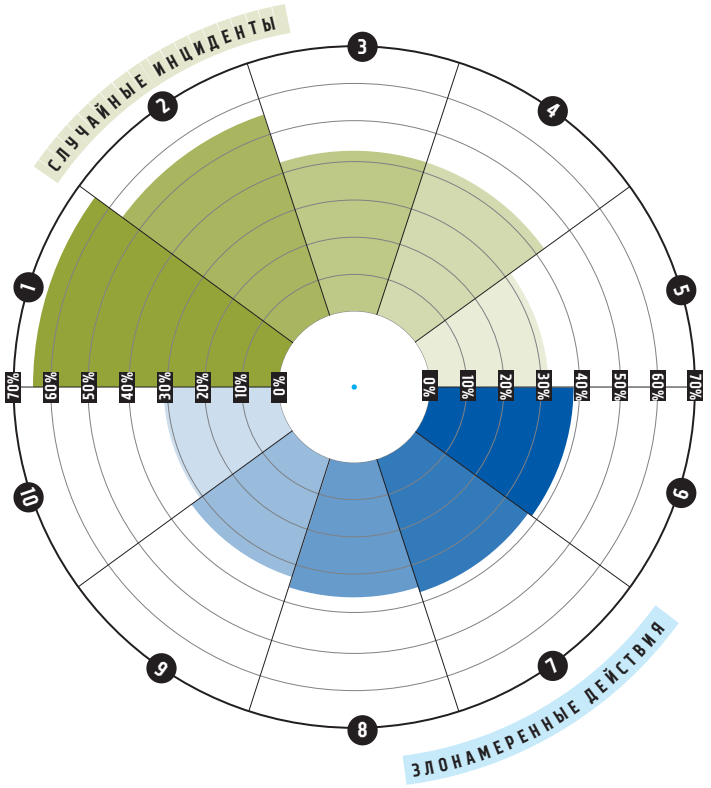
В ЗАВЕРШЕНИЕ ОТМЕТИМ, ЧТО ВЫ САМИ ДОЛЖНЫ РЕШИТЬ, КАКОЙ ПОДХОД ВЫБРАТЬ. ГОТОВЫ ЛИ ВЫ ПОЙТИ НА РИСК И СЫГРАТЬ ПО-КРУПНОМУ, ПОСТАВИВ НА КОН ВСЕ? ИЛИ ДЛЯ ВАС ЛУЧШЕ СДЕЛАТЬ «ПРОВЕРОЧНУЮ СТАВКУ»?

ВНУТРЕННИЕ УГРОЗЫ

В ЦЕЛЯХ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ НЕОБХОДИМО КОНТРОЛИРОВАТЬ ДЕЯТЕЛЬНОСТЬ НЕ ТОЛЬКО СОТРУДНИКОВ ПРЕДПРИЯТИЯ, НО И ПОДРЯДЧИКОВ / ТРЕТЬИХ ЛИЦ, ИМЕЮЩИХ ДОСТУП К ВНУТРЕННИМ ДАННЫМ КОМПАНИИ. ВНУТРЕННИЕ ЗЛОУМЫШЛЕННИКИ, ЖЕЛАЮЩИЕ НАНЕСТИ ВРЕД *(НАПРИМЕР, НЕДОВОЛЬНЫЕ ЧЕМ-ЛИБО РАБОТНИКИ)*, **ПРЕДСТАВЛЯЮТ СЕРЬЕЗНУЮ ОПАСНОСТЬ, НО СЛЕДУЕТ ИМЕТЬ В ВИДУ, ЧТО ВОЗНИКШИЕ ИЗ-ЗА НЕБРЕЖНОСТИ ИЛИ ХАЛАТНОСТИ БРЕШИ В СИСТЕМЕ БЕЗОПАСНОСТИ НЕ МЕНЕЕ ОПАСНЫ — ОНИ ЯВЛЯЮТСЯ ПРИЧИНОЙ БОЛЬШОГО ЧИСЛА УТЕЧЕК ДАННЫХ И КИБЕРИНЦИДЕНТОВ.**

Что способствует возникновению внутренних угроз?

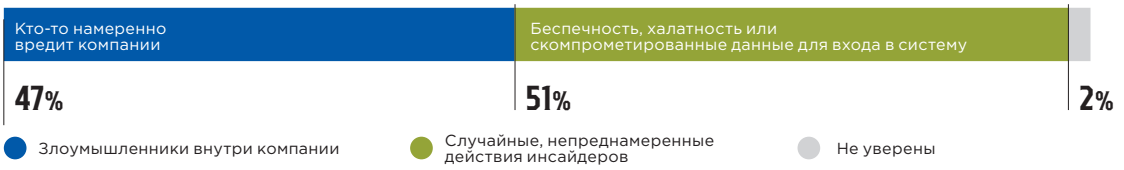
Количество *(%)* **профессионалов в области кибербезопасности, которые считают, что следующие факторы способствуют возникновению внутренних угроз**



1. Случаи фишинга
2. Практика совместного использования ненадежных паролей
3. Слабые / ранее использованные пароли
4. Незащищенные Wi-FI-сети
5. Незапароленные устройства
6. Слишком много пользователей с широкими правами доступа
7. Растущее число устройств с доступом к чувствительным данным
8. Усложнение технологий
9. Рост количества конфиденциальных данных
10. Недостаточный уровень обучения/ информирования сотрудников

Случайные инциденты беспокоят экспертов не меньше, чем злонамеренные атаки

Наиболее беспокоящие профессионалов внутренние угрозы

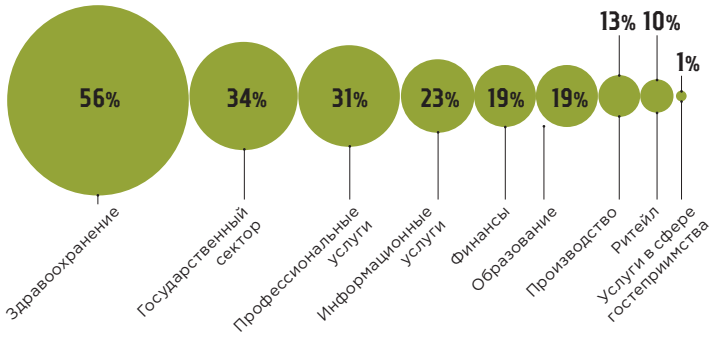


- Злоумышленники внутри компании
- Случайные, непреднамеренные действия инсайдеров
- Не уверены

Исследование компании Cybersecurity Insiders, 2018 г.

Инсайдерские угрозы в процентах по секторам

Процент всех инцидентов в сфере безопасности и утечек данных, в которых виновны инсайдеры



Исследование компании Verizon, 2018 г.

Сдерживание и выявление

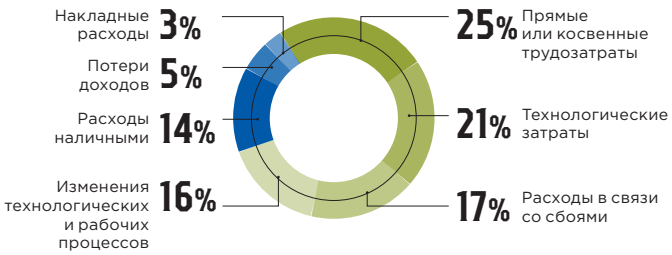
Наиболее распространенные способы контроля, которые применяются компаниями *(по ранжированию)*

СДЕРЖИВАНИЕ	ВЫЯВЛЕНИЕ
01 Предупреждение утечек данных	01 Выявление и предупреждение проникновения
02 Шифрование данных	02 Контроль входа
03 Системы идентификации и обеспечения контроля доступа	03 Информационная безопасность и управление событиями
04 Обеспечение комплексной и мобильной безопасности	04 Предиктивная аналитика
05 Облачная безопасность	05 Аналитика поведения пользователей и организаций

Исследование компании Cybersecurity Insiders, 2018 г.

Структура расходов в связи с инсайдерскими инцидентами

Данные о 3269 инцидентах в крупных организациях в 2018 г.



Исследование Института Понемона, 2018 г.

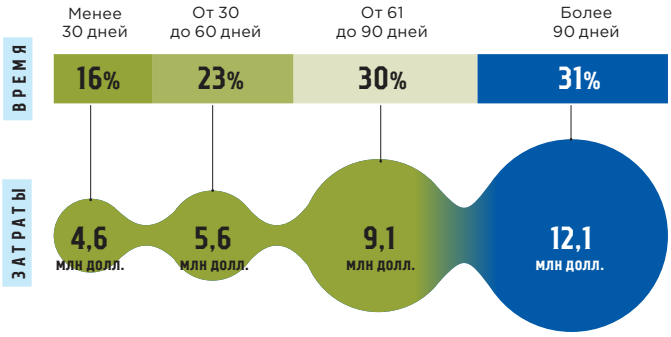
Как выглядят инсайдеры

Количество *(%)* **профессионалов в области кибербезопасности, которые утверждают, что следующие лица представляют угрозу безопасности**

Исследование компании Cybersecurity Insiders, 2018 г.

Временны́е и финансовые затраты на устранение последствий внутренних инцидентов

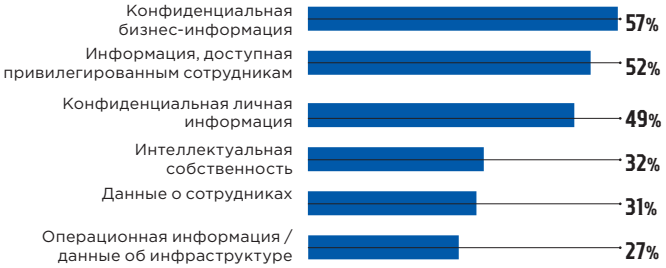
Данные о 3269 инцидентах в крупных организациях в 2018 г.



Исследование института Понемона, 2018 г.

Цели для инсайдерских атак

Типы данных, наиболее уязвимых для инсайдерских атак



Исследование компании Cybersecurity Insiders, 2018 г.

БЕЗОПАСНАЯ РАЗРАБОТКА: АДАПТИВНАЯ ЭВОЛЮЦИЯ[1]

Форма эволюции, при которой окончательно устанавливается новое равновесие с внешней средой

АВТОР
Анастасия Дитенкова,
старший инженер-проектировщик Центра информационной безопасности компании «Инфосистемы Джет»

АВТОР
Антон Гаврилов,
эксперт Центра информационной безопасности компании «Инфосистемы Джет»

ОБЪЕМ СТР.

/ КАКИЕ ПРОБЛЕМЫ ВОЗНИКАЮТ ПРИ ИНТЕГРАЦИИ ПРОЦЕССОВ РАЗРАБОТКИ, ИТ И ИБ
/ КАК ПРАВИЛЬНО СФОРМИРОВАТЬ ИБ-КОМАНДУ ДЛЯ DEVSECOPS
/ КАК ВЫБРАТЬ ИНСТРУМЕНТЫ ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССА БЕЗОПАСНОЙ РАЗРАБОТКИ

Служба информационной безопасности постоянно забрасывает своими суперсрочными запретами всех подряд вне зависимости от последствий для всей организации, поэтому мы не особо любим приглашать их на общие встречи.

Проект «Феникс»

Методологии разработки ПО постоянно развиваются: сегодня, помимо модели Waterfall, широко практикуются Agile и DevOps. С одной стороны, это обусловлено стремлением бизнеса привносить новые функции в продукты для удовлетворения потребностей клиентов, с другой — связано с появлением инструментов, ускоряющих разработку. Речь идет, например, о платформах Continuous Integration и Continuous Delivery, а также о контейнерах. Вместе с тем стали популярны альтернативные подходы к архитектуре: «монолитное ПО» постепенно заменяют Service Oriented Architecture *(SOA)* и микросервисы.

Развитие технологий имеет и обратную сторону: количество уязвимостей постоянно растет, появляются новые способы реализации вроде бы уже известных угроз ИБ. Быть специалистом во всем и в одиночку разбираться во всех технологиях практически невозможно. Сделать качественный и безопасный продукт при сохранении существующих взаимоотношений между разработкой, ИТ и информационной безопасностью не получится.

Цитата, приведенная в эпиграфе, отлично иллюстрирует проблему в отношении к ИБ. Безопасность зачастую воспринимается лишь как фактор ограничения, особенно если дело касается разработки ПО, где time-to-market является одной из наиболее значимых метрик успешности.

36%

РЕСПОНДЕНТОВ ФИКСИРУЮТ СОПРОТИВЛЕНИЕ СО СТОРОНЫ РАЗРАБОТКИ ПРИ ВСТРАИВАНИИ ИБ-ПРОВЕРОК В CI/CD-PIPELINE

«DevSecOps Realities and Opportunities», Synopsys, апрель 2018 г.

Взаимные претензии разработки и ИБ лишь подчеркивают невозможность использования привычного подхода для взаимодействия сторон. Чтобы реализовать сценарий win-win в рамках DevSecOps, необходимо перестать искать правых и виноватых, потому что каждая сторона права по-своему.

Необходимы изменения, переосмысление собственных действий и адаптация подхода, для того чтобы можно было выпускать максимально качественный и защищенный продукт при минимально возможной нагрузке на time-to-market.

Задача не из легких, но решить ее можно.

С какими наиболее частыми проблемами можно столкнуться, если соединить мир разработки, ИТ и ИБ?

БЕЗОПАСНОСТЬ «ПРОСЫПАЕТСЯ» ТОЛЬКО ТОГДА, КОГДА ПРИЛОЖЕНИЕ УЖЕ ГОТОВО К РЕЛИЗУ! ПОЧЕМУ ОНА РАНЬШЕ НЕ ПРЕДЪЯВЛЯЛА НИКАКИХ ТРЕБОВАНИЙ?

ПОЧЕМУ НИКТО НЕ СКАЗАЛ, ЧТО КОМАНДА РАЗРАБОТКИ ЗАРЕГИСТРИРОВАЛА НОВЫЙ ПРОЕКТ В СРЕДЕ КОНТЕЙНЕРНОЙ ВИРТУАЛИЗАЦИИ?

Я НЕ МОГУ ПРОСКАНИРОВАТЬ ИСХОДНЫЙ КОД, ПОТОМУ ЧТО У МЕНЯ НЕТ ИНСТРУМЕНТОВ. ТЕ, ЧТО ВНЕДРИЛА БЕЗОПАСНОСТЬ, НЕ ПОДХОДЯТ, ПОТОМУ ЧТО ОЧЕНЬ ДОЛГО РАБОТАЮТ И ДАЮТ ОТЧЕТЫ, В КОТОРЫХ СЛИШКОМ МНОГО FALSE POSITIVE!

«МОЕ ДЕЛО – РАЗРАБОТКА!», – ГОВОРЯТ ПРОГРАММИСТЫ. У НИХ ОТСУТСТВУЕТ МОТИВАЦИЯ ВЫПОЛНЯТЬ ДОПОЛНИТЕЛЬНУЮ РАБОТУ.

ПРИ УПРАВЛЕНИИ ТЕХНИЧЕСКИМ ДОЛГОМ ПРИОРИТЕТ КАЖДЫЙ РАЗ ОТДАЕТСЯ УСТРАНЕНИЮ ИТ-НЕДОСТАТКОВ ИЛИ ДОРАБОТКЕ ФУНКЦИОНАЛА. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЕСПЕЧИВАЕТСЯ ПО ОСТАТОЧНОМУ ПРИНЦИПУ.

БЕЗОПАСНОСТЬ СТАРОМОДНА. ИБ-СПЕЦИАЛИСТЫ НЕ ХОТЯТ ПОДСТРАИВАТЬ СОБСТВЕННЫЕ ПРОЦЕССЫ ПОД СУЩЕСТВУЮЩИЕ РЕАЛИИ И ФОКУСИРУЮТСЯ «НА ИСПОЛЬЗОВАНИИ МЕЖСЕТЕВЫХ ЭКРАНОВ».

«ВНЕДРЕНИЕ ИБ-РЕШЕНИЙ СТОИТ ОЧЕНЬ ДОРОГО». А КАК ЖЕ ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА РФ И РЕГУЛЯТОРОВ В ОБЛАСТИ ИБ?

...

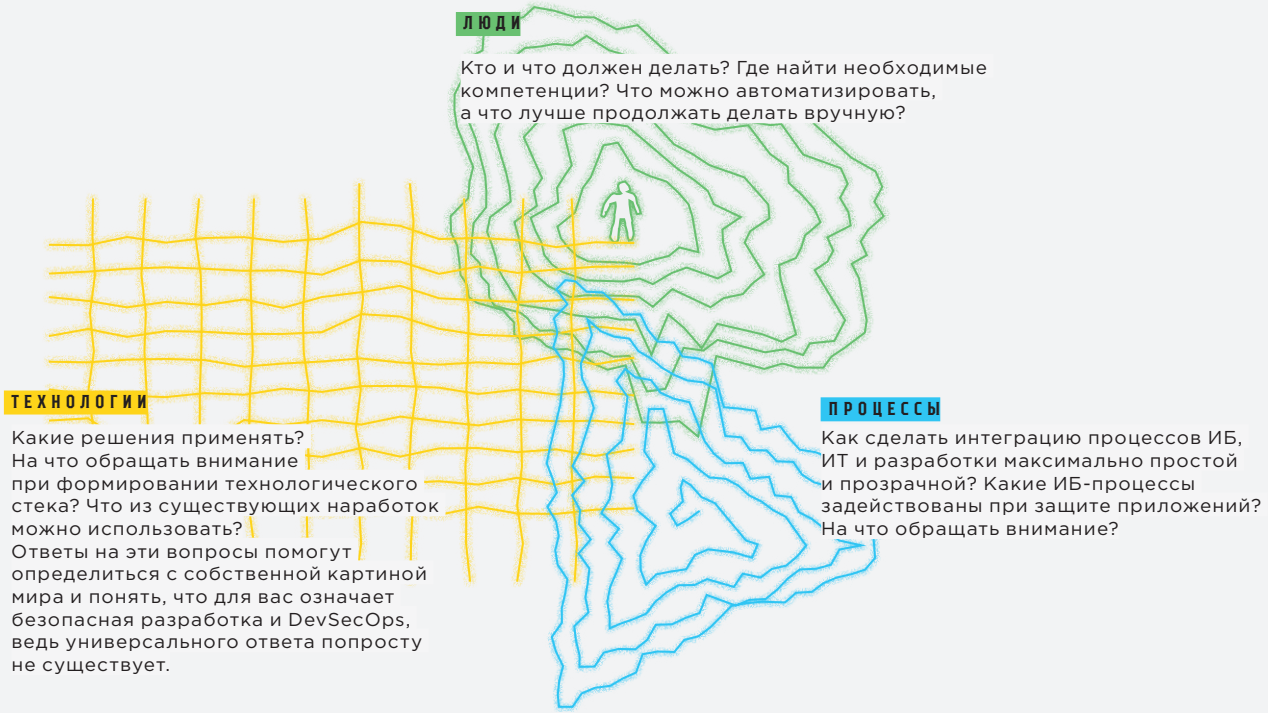
СО СТОРОНЫ РАЗРАБОТКИ И ИТ:

СО СТОРОНЫ ИБ ТОЖЕ ЕСТЬ ПРЕТЕНЗИИ:

СЦЕНАРИЙ WIN-WIN В РАМКАХ DEVSECOPS ВОЗМОЖЕН ТОЛЬКО ТОГДА, КОГДА ИБ-СПЕЦИАЛИСТЫ И РАЗРАБОТЧИКИ ПЕРЕСТАНУТ ИСКАТЬ ПРАВЫХ И ВИНОВАТЫХ, ПОТОМУ ЧТО КАЖДАЯ СТОРОНА ПРАВА ПО-СВОЕМУ.

ПОСТАНОВКА ЗАДАЧИ

Для определения решения, подходящего именно вам, мы рекомендуем рассмотреть классическую триаду:



ПРОЦЕССЫ

Одна из возможных проблем, с которой сталкивается ИБ при погружении в мир безопасной разработки, заключается в том, что она «слишком справа», ближе к эксплуатации. Что это значит? Представим жизненный цикл разработки ПО в виде прямой линии *(процесса)* — от сбора требований до эксплуатации (рис. 1).

Зачастую безопасность располагается где-то между развертыванием и эксплуатацией. И допустим, она просит провести тестирование на проникновение. Обычно по его результатам идентифицируется перечень уязвимостей, которые необходимо устранить. Естественно, это вызывает резонанс у команд разработки:

> МЫ УЖЕ ПРОШЛИ ПОЛНЫЙ ЦИКЛ! НЕУЖЕЛИ НЕЛЬЗЯ БЫЛО НАЙТИ ЭТИ НЕДОСТАТКИ РАНЬШЕ?

Кроме разногласий с командами разработки, это приводит к увеличению стоимости ПО. Почему? Потому что тратится время. Время безопасности и разработки.

Еще в 2002 г. исследователи Американского национального института по стандартам

(NIST) в отчете «The Economic Impacts of Inadequate Infrastructure for Software Testing» показали, что стоимость устранения дефектов, найденных в коде, зависит от времени их обнаружения (см. таблицу):

- дефект, найденный и устраненный на стадии проектирования архитектуры, стоит 1*X, где X — человеко-часы, выраженные в денежном эквиваленте;
- аналогичный дефект, обнаруженный на этапе интеграции и тестирования, будет стоить уже 10*X.

Чем раньше обнаружен дефект, тем меньше стоимость его устранения. То же относится к уязвимостям в исходном коде и нарушениям требований в области ИБ — их можно приравнять к дефектам кода.

Для решения этой проблемы используется подход Shift Left: безопасность начинают привлекать к разработке ПО начиная со стадии проектирования. При этом ИБ подключается не просто как «контролер», а как активный участник рабочей группы, который вносит свой вклад в проектирование приложения или сбор функциональных требований. Это позволяет, хотя и не в полной мере, реализовать концепт Security By Design.

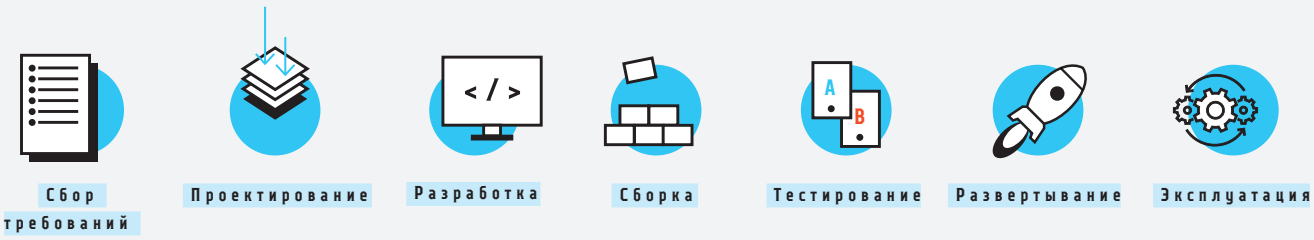
Далее ИБ определяет Security Gates — точки контроля по информационной безопасности, которые встраиваются в pipeline. Диалог с командами разработки очень важен и на этой стадии. Ведь если добавить безопасность повсюду, можно получить огромное количество данных, которые необходимо анализировать, а по результатам делать выводы и принимать решения. Это не всегда необходимо, а кроме того, требует больших ресурсозатрат. Например, контроль над DEV-средой может быть менее серьезным, чем над PROD-средой. А вот контроль feature-ветки при разработке ПО может содержать все проверки: анализ исходного кода, сканирование контейнеров, проверку используемых библиотек. Только после их успешного прохождения код получает возможность merge'а в master-ветку репозитория. В самой же master-версии большое количество проверок может отсутствовать *(предполагаем, что код из feature-ветки не поменялся и попал в master в том виде, в котором был согласован)*. ИБ может быть одной из сторон, которая должна согласовать код, для того чтобы master-ветка обновилась.

Более детально о проверках и их месте в pipeline расскажем чуть позже *(в блоке «Технологии»)*.

Помимо новых процессов, которые информационной безопасности необходимо создать, важно помнить о существующих и о том, как правильно реализовать интеграцию.

Управление рисками ИБ. Решение о реализации ИБ или новой killer-feature *(которая может быть уязвимой)* принимает не безопасность, а бизнес-владелец приложения. Задача ИБ — показать, какие риски может принести реализация нового функционала в текущем исполнении. Дальше нужно действовать по обстоятельствам: отойти в сторону и настроить exception в системах мониторинга и сканирования, реализовать «запрет» или совместными

Рисунок 1. **Общий вид жизненного цикла разработки** *(pipeline)*



Относительная себестоимость устранения ошибок, обнаруженных на разных стадиях создания программного продукта *(только в качестве примера)*

X — приведенная мера себестоимости, которая может быть выражена в человеко-часах, долларах, и т.д.

Сбор и анализ требований / проектирование архитектуры	Программирование/ UNIT-тестирование	Интеграция/ RAISE-тестирование	Предварительный сбор обратной связи / бета - тестирование	Поддержка после выхода ПО
1X	5X	10X	15X	30X

усилиями с разработчиками и ИТ-специалистами придумать комплекс компенсирующих мер.

Управление инцидентами ИБ. Необходимо понять, что является инцидентом ИБ при разработке ПО. Например, это может быть нарушение SLA об устранении критичной уязвимости или же все, что подходит под классификацию инцидентов ИБ, принятую в компании для ПО в продуктиве.

Управление уязвимостями и несоответствиями — процесс, который превращается в управление бесконечным техническим долгом. Одной из хороших практик считается обязательное устранение уязвимостей, выявленных в новой сборке. Команда «разбирает» уязвимости, полученные при первичном сканировании, в зависимости от степени их критичности и своей загрузки. Такой подход позволяет гарантировать, что угрозы *(по крайней мере те, что были идентифицированы в новой сборке)* будут устранены. Еще одна задача, которая стоит перед ИБ, — создание единого окна, где будут отображаться статусы по уязвимостям в ПО с точки зрения не только кода, но и инфраструктуры, используемой разработчиками и командой эксплуатации.

Управление доступом. При разработке используется большое количество секретов *(ниже, в пункте Secret Management, мы рассказываем, что это такое)*, которые необходимы для взаимодействия сервисов: требуется выстроить корректную ротацию, организовать процесс управления доступом к системе версионности кода и хранилищу артефактов ПО, например, с использованием групп AD.

Управление регуляторными требованиями (compliance) релевантно для компаний, которые подпадают под действие стандартов или федеральных законов, устанавливающих требования в том числе к обеспечению ИБ при разработке ПО. Пример — требования PCI/DSS, в которых указано, что не следует использовать реальные данные для нужд тестирования/разработки.

Управление взаимодействием с подрядчиками. Необходимо убедиться в том, что код, который получает компания от третьих лиц, не содержит уязвимостей или backdoors. Это можно установить с помощью сканирования исходного кода и проведения ручного анализа. А что делать потом? Как вариант, можно разработать формы SLA, которые будут явно указывать на необходимость устранения уязвимостей внешней стороной в случае их обнаружения.

Управление эффективностью ИБ. Мы рекомендуем подготовить набор метрик, которые будут показывать прогресс команд разработки с точки зрения ИБ. Например, «количество уязвимостей в текущей сборке по отношению к таковому в предыдущей», «процент выполненных SLA по устранению недостатков в коде», «процент кодовой базы, которая сканируется на наличие уязвимостей» и т.д.

Рассмотренные выше примеры далеко не избыточны. Мы хотели показать, что информационной безопасности потребуется не только создать новые процессы, но и адаптировать существующие, чтобы они смогли работать в pipeline.

БЕЗОПАСНОСТЬ ПОСТЕПЕННО СТАНОВИТСЯ СИНОНИМОМ КАЧЕСТВА, ОСОБЕННО В УСЛОВИЯХ РЫНКА ПОВЫШЕННОЙ КОНКУРЕНЦИИ.

Рисунок 2. **Наиболее значимые вызовы для ИБ при встраивании проверок в CI/CD-pipeline** *(%)*

Данные отчета «DevSecOps Realities and Opportunities», Synopsys, апрель 2018 г.

Новые процессы лучше создавать общаясь с командами разработки. Они смогут подсказать ИБ оптимальные варианты, которые устроят обе стороны. ИБ может попутно объяснять, что такое безопасность и зачем она вообще нужна, почему грамотно выстроенная функция минимально повлияет на разработку.

Если вы думаете, что разработчики будут сопротивляться, просто посмотрите на данные отчета «DevSecOps Realities and Opportunities» **(рис. 2).**

Наш опыт говорит о схожей ситуации: были случаи, когда команды разработки просили дать им удобный и надежный инструмент для сканирования кода на наличие уязвимостей. Ведь безопасность постепенно становится синонимом качества, особенно в условиях рынка повышенной конкуренции, где любой фактор может оказаться тем самым преимуществом, которое позволит именно этой компании обогнать конкурентов.

5 СОВЕТОВ ПРИ ВЫСТРАИВАНИИ ПРОЦЕССОВ

01

Обращайте внимание на методику, используемую командой при разработке ПО. Если одна команда практикует DevOps, это не означает, что в компании отсутствуют команды, использующие Waterfall. Разные методики требуют разных подходов хотя бы потому, что у них отличаются сроки релизов и потенциальная степень автоматизации процессов ИБ.

02

Подключайтесь к разработке ПО с самого начала — еще на стадии сбора функциональных требований — и прорабатывайте продукт вплоть до приемки в эксплуатацию.

03

При формировании новых процессов (например, при идентификации Security Gates) обсуждайте с командами разработки точки интеграции и возможные методы их контроля. Вряд ли вы захотите согласовывать все попытки обновления master-версии в контуре разработки, ведь их может быть не один десяток в день.

04

Не добавляйте безопасность везде, где возможно. Такая ситуация осложнит жизнь и вам, и разработчикам.

05

Адаптируйте существующие ИБ-процессы, которые будут пересекаться с разработкой. В качестве примера приведем управление уязвимостями: далеко не все их можно устранить, просто обновившись до новой версии. Бывают случаи, когда обновление одной библиотеки затронет еще семь сопутствующих, что может привести к неработоспособности ПО. Эти аспекты в обязательном порядке необходимо обсуждать с командами разработки.

В итоге мы должны получить ситуацию, диаметрально противоположную той, что отражена в эпиграфе. Ведь множественные ограничения обусловлены, как правило, недостаточным пониманием, а его невозможно сформировать без постоянного взаимодействия сторон и их взаимного обучения.

ЛЮДИ

Формирование правильной процессной карты ИБ, необходимой для обеспечения безопасности разработки, поможет ответить на вопрос «Что надо делать?». Ну а следующий вопрос, на который желательно получить ответ:

КТО БУДЕТ ЭТО ДЕЛАТЬ?

Выше мы описали ряд трудностей, с которыми можно столкнуться в поисках ответа. Приведем наиболее актуальные из них.

- Адаптация существующих и создание новых процессов влекут за собой огромное количество активностей, которые повышают загрузку специалистов.
- Необходимо наладить взаимодействие с большим количеством команд разработки в условиях, когда подход «one size fits all» не работает *(хотя бы из-за вероятности использования различных методологий разработки и технологического стека)*.
- Где взять людей, которые обладают необходимым набором компетенций? В вузах, например, будущим ИБ-специалистам дают лишь основы разработки на первых курсах, а разработчикам вряд ли читают лекции об ИБ.

Ситуация усугубляется тем, что ИБ-специалистов в организациях, как правило, не так много и в одиночку им не справиться с амбициозными целями, сформированными при проектировании процессной карты безопасной разработки (рис. 3).

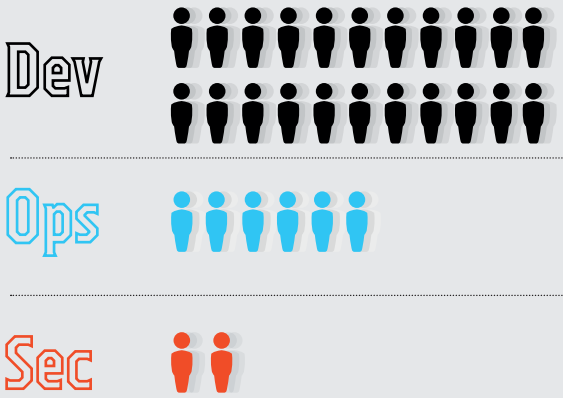
Есть несколько возможных вариантов решения проблемы:

- **Расширение штата ИБ.** Потенциально возможный способ при наличии необходимых мест в организационно-штатной структуре, фонда оплаты труда и свободных специалистов необходимой квалификации на рынке *(хотя найти их вряд ли удастся)*.

ОДНА ИЗ ФУНКЦИЙ SECURITY CHAMPION — МИНИМИЗИРОВАТЬ КОЛИЧЕСТВО ПРОБЛЕМ ИБ ПУТЕМ РАСПРОСТРАНЕНИЯ ПОЛУЧЕННЫХ ЗНАНИЙ СРЕДИ ОСТАЛЬНЫХ ЧЛЕНОВ КОМАНДЫ.

- **Аутсорсинг и/или аутстаффинг.** Даже при условии, что вы найдете компанию, оказывающую подобные услуги, в реалиях Российской Федерации этот способ вряд ли заработает: придется давать доступ «сторонним» людям к самому «святому» — исходному коду программного обеспечения. И не просто давать, а давать для анализа на наличие уязвимостей и несоответствий требованиям в области ИБ.
- **Стажерские программы**. Неплохой способ, однако у него есть недостаток: программы длятся долго, к тому же найти сильную команду менторов, способных «быстро воспитать» подрастающее поколение, сложно. Вряд ли кто-нибудь согласится выделить много времени на запуск приложения

Рисунок 3. Соотношение экспертов в командах разработки



Данные отчета «2018 DevSecOps Community Survey», Sonatype

в production. Скорее всего, риски будут приняты, а проблемы станут решаться по мере появления.

последующие Security Champions смогут перенимать опыт «первопроходцев» и им будет чуть проще.

«ПРИОТКРЫВАТЬ ДВЕРЬ В МИР ИБ» НУЖНО НЕ ТОЛЬКО ДЛЯ SECURITY CHAMPIONS. НЕОБХОДИМА И ОБРАТНАЯ СВЯЗЬ – ПОГРУЖЕНИЕ ИБ-СПЕЦИАЛИСТОВ В МИР РАЗРАБОТКИ. В КАКОЙ-ТО СТЕПЕНИ ЭТУ ЗАДАЧУ ВОЗЬМЕТ НА СЕБЯ SECURITY CHAMPION, НО ОГРАНИЧИВАТЬСЯ ЭТИМ НЕ СЛЕДУЕТ. НАПРИМЕР, МОЖНО ПРИГЛАШАТЬ ИБ-СПЕЦИАЛИСТОВ НА ОБСУЖДЕНИЕ ФУНКЦИОНАЛЬНОЙ АРХИТЕКТУРЫ ИЛИ ПЛАНИРОВАНИЕ СПРИНТОВ.

А почему бы не обратить внимание на имеющихся специалистов? Например, на программистов. Они есть в каждой команде разработки. Они знают создаваемый продукт и его особенности. И знают, как можно, например, обновить версию библиотеки так, чтобы приложение «не рассыпалось». И, что самое важное для достижения цели безопасного продукта, среди них, с очень большой долей вероятности, найдутся те, кому интересно разбираться в информационной безопасности и повышать качество разрабатываемого продукта. Именно их стали называть Security Champions.

Security Champion не является специалистом по информационной безопасности в полной мере, он остается разработчиком. Но, согласитесь, научить разработчика основам ИБ гораздо проще, чем научить ИБ-специалиста писать код на многих языках и понимать тонкости работы всех приложений. **Для реализации этого концепта и создания такой роли ИБ-специалист может сделать следующее:**

- Найти человека из команды разработки, которому интересна информационная безопасность. Как это сделать? Достаточно просто: пойти и поговорить с коллегами, объяснить им, что предполагается делать, и спросить, кто хочет поучаствовать в «эксперименте». Мы рекомендуем выбирать из команд, которые наиболее лояльны по отношению к ИБ, так как
- Показать и рассказать, какие требования в области ИБ *(применительно к разработке ПО)* существуют в компании и как их трактовать.
- При необходимости провести общий курс по информационной безопасности: объяснить, что такое конфиденциальность, целостность, доступность информации, что такое CVE, зачем отправлять логи в SIEM *(а также, что такое SIEM)*.
- Предоставить этому специалисту все необходимые инструменты — например, статический анализ исходного кода, инструментарий по сканированию образов контейнеров *(об этом подробнее будет рассказано в следующем разделе)*.
- Научить пользоваться предоставленными инструментами: провести очные курсы, «показать консоль», предоставить техническую документацию *(например, описание API)*. Разработчик поймет, как он может максимально автоматизировать собственную деятельность с точки зрения ИБ.

Основная цель — сформировать понимание важности обеспечения ИБ у разработчика и предоставить ему возможности для реализации поставленных перед ним задач. Еще одна функция Security Champion — минимизировать количество проблем ИБ путем распространения полученных знаний среди остальных членов команды. В итоге получается, что «интерфейс ИБ в команду разработки» — это мостик, который

6 СОВЕТОВ ПРИ ФОРМИРОВАНИИ КОМАНДЫ

01

Привлекайте Security Champions: важно не забывать о мотивации, которая не обязательно должна быть выражена прибавкой к зарплате. Например, поездка на конференцию по обмену опытом будет классным вариантом!

02

ИБ — это часть команды: как минимум при планировании спринтов и обсуждении наиболее значимых задач.

03

Обучайте друг друга: постоянно обменивайтесь опытом и используйте знания друг друга. Разработчик в разы быстрее напишет Stage в Jenkins для интеграции SAST. ИБ-специалист может предоставить всю необходимую информацию для этого.

04

Развивайте кросс-командное взаимодействие: Security Champions различных команд могут устраивать периодические Security-митапы для обсуждения собственных подходов к реализации требований в сфере ИБ и обмена опытом. ИБ-специалисты также должны быть частью этой активности.

05

Исследуйте встроенные возможности технологий разработки: специалисты ИБ могут очень сильно обрадоваться, узнав, какой функционал есть, например, в git-системах или хранилищах артефактов, который можно применять для нужд ИБ.

06

Используйте инструментарий, привычный для разработчика (например, JIRA, Confluence): скорость и качество обратной связи могут значительно улучшиться.

связывает два мира, ранее практически не пересекавшихся.

«Приоткрывать дверь в мир ИБ» нужно не только для Security Champions. Необходима и обратная связь — погружение ИБ-специалистов в мир разработки. В какой-то степени эту задачу возьмет на себя Security Champion, но ограничиваться этим не следует. Например, можно приглашать ИБ-специалистов на обсуждение функциональной архитектуры или планирование спринтов, что позволит устранить принцип «остаточности» при решении вопросов ИБ *(может быть, не в полной степени, но начало будет положено!)*.

Помимо внедрения взаимного обучения, также рекомендуется изменить «каналы взаимодействия» — адаптировать ИБ для использования инструментария, привычного и понятного разработчику. Почта? Нет, зачем? Есть JIRA и Slack. Документы в формате *.docx? А может быть, лучше Confluence *(у него даже мобильное приложение есть!)*? Отчеты в Excel и CSV? Возможно. Но что, если подумать об использовании API и прямой интеграции, например, с git-системами?

Эти знания помогут ИБ-специалисту не только глубже узнать функциональные возможности, которыми часто *(практически всегда)* обладают используемые в разработке технологии, но и выстроить более простое и понятное взаимодействие между сторонами, для того чтобы ускорить устранение ИБ-недостатков в ПО.

ТЕХНОЛОГИИ

Мы определили, «что нам надо делать», подумали над тем, «кто это будет делать». Осталось найти ответ на вопрос:

КАКИМИ ИНСТРУМЕНТАМИ ПОЛЬЗОВАТЬСЯ, ДЛЯ ТОГО ЧТОБЫ СДЕЛАТЬ ЭТО МАКСИМАЛЬНО УДОБНО И БЫСТРО?

Это особенно актуально при постоянно увеличивающейся скорости разработки ПО и сокращении time-to-market.

Как можно максимально быстро решить проблему, возникающую из-за потребности в большом количестве различного рода проверок? На ум приходит только одно: автоматизировать все, что только можно! И этот концепт отлично соответствует современным реалиям, в которых используются специализированные решения, позволяющие автоматизировать весь процесс сборки и развертывания приложений *(например, CI/CD tools)*. Важно, чтобы каждый инструмент, применяемый для защиты, был «на своем месте». Что это значит? Вспомним наш конвейер разработки (см. рис. 1) и рассмотрим, что применять на каждом этапе. Да, практически в каждый этап может быть встроено средство, позволяющее автоматизировать часть задач ИБ!

МНОГИЕ SAST-РЕШЕНИЯ, ПРЕДСТАВЛЕННЫЕ НА РЫНКЕ, ПОЗВОЛЯЮТ ИНТЕГРИРОВАТЬСЯ В CI/CD-PIPELINE, ЧТО ПОМОГАЕТ АВТОМАТИЧЕСКИ ЗАПУСКАТЬ ТЕСТИРОВАНИЕ, КАК ТОЛЬКО РАЗРАБОТЧИК СОВЕРШИТ ОБНОВЛЕНИЕ КОДА В СИСТЕМЕ КОНТРОЛЯ ВЕРСИЙ. ОТ ИБ-СПЕЦИАЛИСТОВ НЕ ТРЕБУЕТСЯ НИЧЕГО! РАЗВЕ ЧТО ВНЕДРИТЬ И НАСТРОИТЬ РЕШЕНИЕ НАДЛЕЖАЩИМ ОБРАЗОМ.

Разработка ПО

Commit Hooks. Даже не внедряя какие-либо дополнительные средства, информационная безопасность может частично автоматизировать деятельность с помощью имеющихся инструментов. Большинство git-систем позволяют добавлять «согласующих», без одобрения которых исходный код не попадет в master-версию. В качестве одного из таких согласующих можно добавить информационную безопасность.

SAST. На этой стадии можно применять одно из самых известных решений — статический анализатор исходного кода *(Static Application Security Testing, SAST)*. В названии анализатора не зря указано «статический»: SAST позволяет проанализировать весь код приложения *(который является «статичным», «написанным на бумаге»)*, чтобы обнаружить уязвимости и потенциальные проблемы в информационной безопасности еще до его запуска *(execution)*.

Вот что, например, могут содержать результаты анализа исходного кода.

- Информацию о том, что используются некриптостойкие библиотеки шифрования или возможна реализация SQL-инъекции.
- Идентификацию того, что для проверки отсутствия в пароле части логина *(admin/admin123)* используются регулярные выражения. Представьте, что злоумышленник создаст логин вида «(x+x+)+y», а пароль будет «xxxxxxxxxxxxxxxxxxxxxxxxxx». При использовании регулярных выражений потребуется совершить более 2 млн операций, что, скорее всего, вызовет отказ в обслуживании сервиса. От проверки применения регулярного выражения к строке лучше воздержаться, логика работы ПО детально описана по ссылке: https://www.regular-expressions.info/catastrophic.html.

Многие SAST-решения, представленные на рынке, позволяют интегрироваться в CI/CD-pipeline, что помогает автоматически запускать тестирование, как только разработчик совершит обновление кода в системе контроля версий. От ИБ-специалистов не требуется ничего! Разве что внедрить и настроить решение надлежащим образом. Некоторые производители SAST предоставляют надстройки, которые интегрируются в Interactive Development Environment *(IDE)* — программы, используемые разработчиками для написания кода *(например, Intellij IDEA, Visual Studio)*. Таким образом, разработчик может получать уведомления о потенциальных ошибках прямо во время работы, что способствует максимально раннему обнаружению и устранению погрешностей.

У решений этого класса есть недостатки, которые обусловливаются срабатываниями false positive или negative: возможен сценарий ошибочной идентификации уязвимости и, наоборот, пропуска присутствующей. Решению этой проблемы в том числе были посвящены первые два раздела статьи. При обнаружении false positive разработчик может обратиться к Security Champion для разбора ситуации с последующим информированием ИБ-специалиста. Иногда бывают случаи, когда разработчик не может устранить уязвимость из-за сложности реализации задачи. Тогда он просит ИБ-специалиста внести исключение *(exception)* в логику работы SAST — применение раздела «Люди». Последний, в свою очередь, знает, что делать дальше, — ведь процесс управления рисками теперь учитывает потребности команд разработки! После получения ответа от владельца продукта происходит оценка ситуации: можно ли делать exception или разработчику придется искать альтернативные способы решения проблемы *(применение раздела «Процессы»)*?

Сборка приложения

SCA. Исходный код проверен на наличие уязвимостей, началось время сборки. На этом этапе могут помочь решения класса Software Composition Analysis *(SCA)*. SCA позволяют определить полный перечень компонент open source, используемых при разработке приложения *(например, frameworks, plugin, библиотеки)*.

Также решения помогают идентифицировать потенциальные проблемы в найденных артефактах. Указанные проблемы не всегда заключаются в том, что библиотеки содержат уязвимости или их «срок действия истек». Бывают случаи, когда подключаются библиотеки open source, обладающие лицензионными соглашениями.

Вот один из потенциальных сценариев использования SCA. Допустим, стало известно об уязвимости нулевого дня в какой-либо библиотеке. Как конкретной команде разработки понять *(и быстро)*, используется ли уязвимая библиотека в ее ПО, а ИБ-специалистам оценить глобальный масштаб проблемы в рамках компании? Как раз в этой ситуации SCA сможет помочь как ничто другое. Уязвимая библиотека будет идентифицирована, варианты «альтернативных библиотек» предложены самим решением, и останется только установить обновление или перейти к аналогичной проблеме, что займет время и ресурсы, но спасет от уязвимостей нулевого дня.

SCA-решения могут быть интегрированы в CI/CD-pipeline для автоматического запуска проверки ПО на наличие проблем, обусловленных использованием решений open source. Некоторые производители предоставляют специализированные надстройки для наиболее популярных инструментов CI/CD, что упрощает интеграцию.

Тестирование и развертывание ПО

DAST. На стадии разработки программного обеспечения мы рассматривали статический анализ кода: приложение только создавалось и не было готово к запуску. На стадии тестирования и развертывания ситуация изменилась: приложение работает, осуществляются тестирования различного вида

(функциональные, нагрузочные). А безопасность начинает использовать динамические анализаторы *(Dynamic Application Security Testing, DAST)*.

Ключевым отличием DAST от SAST является период тестирования. SAST анализирует приложение до запуска, DAST — после. Можно сказать, что SAST использует подход whitebox, а DAST — blackbox. С одной стороны, это плюс *(можно проанализировать приложение, полученное от контрагента)*, с другой — минус *(для проведения качественного DAST-тестирования требуется полная сборка приложения)*.

Зачастую тестирование с помощью DAST применяется для анализа веб-приложений. Решения этого класса позволяют выявлять уязвимости, обусловленные различного рода инъекциями кода в запрос *(например, к веб-странице)* или связанные с некорректной конфигурацией *(самый простой пример — возможность аутентификации по пустому паролю)*. Ввиду ограниченного функционала, DAST не может быть сам по себе эталоном для оценки защищенности приложения, однако преимущества делают его хорошим дополнением к общей картине, включающей SAST и SCA. Так, DAST не привязан к языкам программирования, для анализа не требуется исходный код, а также происходит незначительное количество ложноположительных срабатываний или они отсутствуют вовсе.

Кроме того, стоит добавить, что DAST может быть интегрирован в CI/CD-pipeline для автоматического запуска сканирования.

Эксплуатация приложения

WAF. Web Application Firewall — межсетевой экран прикладного уровня, основной задачей которого является защита приложений, доступных онлайн. Сперва может показаться, что это очень «ограниченное» решение, направленное на защиту одного класса приложений. Однако практически каждый слышал о переходе в digital, одним из аспектов которого является предоставление сервисов клиентам по всем возможным каналам в любое время, в том числе и через веб.

Задача WAF — контроль http/https-трафика между пользователем и веб-приложением. Он позволяет идентифицировать и защищать приложения от наиболее известных атак, информация о которых регулярно публикуется OWASP (Open Web Application Security Project), например:

- инъекции, они же «внедрение кода»;
- некорректная аутентификация;
- ошибки в настройке;

КОНТЕЙНЕРЫ ПОСТЕПЕННО СТАНОВЯТСЯ НЕОТЪЕМЛЕМОЙ ЧАСТЬЮ ЖИЗНИ КАЖДОГО ПРОГРАММИСТА: ОНИ УДОБНЫЕ, БЫСТРЫЕ, «ЛЕГКИЕ», ПОЗВОЛЯЮТ РЕАЛИЗОВАТЬ КОНЦЕПЦИЮ МИКРОСЕРВИСНОЙ АРХИТЕКТУРЫ. НО ДЛЯ ИБ-СПЕЦИАЛИСТОВ СРЕДЫ КОНТЕЙНЕРНОЙ ВИРТУАЛИЗАЦИИ СОЗДАЮТ НОВЫЕ ВЫЗОВЫ – ПОТОМУ ЧТО, НАПРИМЕР, В КОНТЕЙНЕР НЕЛЬЗЯ ПОСТАВИТЬ АНТИВИРУС, ПРОСКАНИРОВАТЬ ЕГО ПРИ ПОМОЩИ ПРИВЫЧНОГО СКАНЕРА УЯЗВИМОСТЕЙ, УСТАНОВИТЬ МЕЖСЕТЕВОЙ ЭКРАН МЕЖДУ НОДАМИ КЛАСТЕРА ИЛИ МЕЖДУ КОНТЕЙНЕРАМИ.

- межсайтовый скриптинг *(XSS)*;
- подделка межсайтовых запросов *(CSRF)*;
- использование компонентов с известными уязвимостями;
- недостаточные логирование и мониторинг.

WAF выступает в роли щита между веб-приложением и пользователем, что позволяет перехватывать http/https-трафик и реализовывать действия согласно настроенным политикам — например, блокировать трафик, если была идентифицирована попытка SQL-инъекции. В таком случае трафик не дойдет до конечного потребителя *(веб-приложения)* и работоспособность сервиса не нарушится или не будет совершена кража конфиденциальных данных компании. В другом сценарии WAF разрешает только «доверенный» трафик, который был заранее определен *(whitelisting-подход)*.

Возможен альтернативный вариант использования WAF — виртуальный патчинг (грубо говоря, использование настроек WAF для создания видимости установки несуществующего обновления, которое выполняет необходимый функционал). Допустим, существует скрипт, который некорректно проверяет входные данные, что создает возможность внедрения произвольного SQL-кода. Есть несколько вариантов решения проблемы:

- **«Классический» патчинг.** Скорректировать скрипт, переписав логику его работы, и добавить фильтрацию данных, получаемых извне.
- **«Виртуальный» патчинг.** Настроить WAF таким образом, чтобы он проверял передаваемую в скрипт нагрузку *(payload)* на наличие запрещенных элементов.

Первый вариант возможен, но занимает гораздо больше времени. На практике применяется гибридный подход: «виртуальный» патч ставится на время, необходимое команде разработки для создания полноценного обновления, устраняющего уязвимость. Как только такое обновление будет передано в промышленную эксплуатацию, потребность в «виртуальном» патче отпадет. Но он сделает свое дело: выиграет необходимое количество времени и обеспечит защиту веб-сервиса.

В статье мы описали значимые инструменты, используемые для обеспечения безопасности приложений, однако упомянули далеко не все. Например, есть решения для автоматизации fuzzing-тестирования, которые пытаются передать на вход приложения всевозможные комбинации потенциально вредоносной нагрузки для анализа ответной реакции. Распределение инструментов можно адаптировать по мере потребности, мы лишь показали один из возможных вариантов, который не создаст лишней нагрузки ни на технику, ни на специалистов. Помимо инструментов, рекомендуемых к применению на определенных этапах *(например, для реализации концепции Shift Left, о которой мы говорили вначале)*, есть инструменты, которые подойдут на многих этапах, и о них не стоит забывать.

Container Security. Контейнеры постепенно становятся неотъемлемой частью жизни каждого программиста: они удобные, быстрые, «легкие», позволяют реализовать концепцию микросервисной архитектуры. ИТ-специалисты могут быстро создавать масштабируемые и отказоустойчивые кластеры. Но для специалистов по информационной безопасности среды контейнерной виртуализации создают новые вызовы — потому что, например, в контейнер нельзя поставить антивирус, просканировать его при помощи привычного сканера уязвимостей либо поставить межсетевой экран между нодами кластера или между контейнерами. Как выстроить полноценную модель информационной безопасности в среде контейнерной виртуализации? Мы рекомендуем обратить внимание на следующие аспекты.

- **Безопасность кластера.** Эта часть мало чем отличается от «классической» информационной безопасности. Задача — защитить ноды *(серверы, хосты)* кластера, используемые для функционирования среды контейнеризации. Для этого стоит обращать внимание:

- *на использование встроенных механизмов хостов для повышения уровня ИБ (hardening);*
- *управление сетевыми потоками между нодами кластера;*
- *сканирование хостов на уязвимости.*

Особое внимание следует уделить ETCD *(базе данных, в которой хранится конфигурация кластера).*

/ **Безопасность оркестратора.** Среды оркестрации *(например, на базе Kubernetes)* обладают встроенным функционалом, который можно использовать в интересах информационной безопасности:

- *управление namespaces, включая распределение контейнеров по нодам в зависимости от их значимости для компании (например, все контейнеры, которые входят в скоуп PCI DSS, должны «подниматься» только на специально отведенном сервере);*
- *управление pod security policy (политиками безопасности, которые определяют возможности и ограничения контейнеров);*
- *управление ограничениями запускаемых контейнеров (управление квотами на использование ресурсов, применение функционала AppArmor, SELinux, cgroups);*
- *обеспечение сетевой безопасности при взаимодействии контейнеров (как между собой, так и с внешними ресурсами).*

/ **Безопасность образов.** Контейнеры создаются из образов *(аналог template виртуальных машин)*, которые могут быть получены из внешних или внутренних реестров либо создаваться разработчиками в рамках CI/CD-pipeline. Обеспечить безопасность образов рекомендуется на всех этапах.

- *удаление «лишнего» (например, в образе контейнера в момент разработки требовался уязвимый curl, а впоследствии потребность в нем пропала, поэтому проще удалить ненужный уязвимый компонент, чем пытаться его обновить);*
- *«подпись» образов, гарантирующая, что контейнер запускается только из образов, целостность которых контролируется;*
- *встраивание проверок образов в CI/CD-pipeline для автоматизации сканирования на наличие уязвимостей и compliance-несоответствий (например, запуск контейнера из-под привилегированной учетной записи, незащищенные системные файловые каталоги, завышенные права системных пользователей, включенные ненужные системные службы и т.д.);*
- *сканирование образов в частных и публичных реестрах, используемых компанией;*
- *управление контролем доступа к реестрам.*

/ **Безопасность контейнеров.** Даже если контейнер был создан из образа, не обладающего уязвимостями и иными дефектами, это еще не означает, что среда контейнерной виртуализации полностью защищена. Необходимо контролировать то, что происходит с контейнерами в их режиме run-time:

- *настройка политик безопасности, в которых указывается, например, перечень разрешенных команд, системных вызовов, сетевых взаимодействий;*
- *поведенческая аналитика: создание «модели» контейнера путем профилирования для последующей идентификации отклонений от «нормы» (например, изменение конфигурационных файлов, запись в сторонние хранилища, попытка установления несанкционированных сетевых соединений, запуск вредоносных файлов и т.д.).*

/ **Управление доступом и секретами.** На каждом из «уровней» — от ноды до контейнера — присутствует множество разных сущностей, взаимодействующих между собой. Для них необходимо выполнить следующее:

- *разработать ролевую модель, описывающую, кто и с какими правами имеет доступ, например, к оркестратору, реестру с образами контейнеров, к конкретному namespace и т.д.;*
- *управлять секретами — паролями пользователей, сервисными учетными записями, токенами для аутентификации в сторонних сервисах, выстроить корректное управление инфраструктурой открытых ключей.*

/ **Мониторинг и аудит ИБ.** Для того чтобы было проще идентифицировать инциденты ИБ и анализировать, насколько требования в области ИБ исполняются в реальной жизни, а не просто «на бумаге», рекомендуется:

- *реализовать управление событиями для передачи данных, например, в SIEM-системы для идентификации инцидентов ИБ;*
- *особое внимание уделять анализу действий администраторов;*
- *периодически проверять выполнение требований в области ИБ (например, требований к hardening кластера, который описывался в пункте «Безопасность кластера»).*

Для того чтобы реализовать перечисленные меры, применяется «смешанный» подход: часть выполняется при помощи встроенных механизмов *(то, что относится к hardening-активностям)*, часть — при помощи навесных средств. Например, организовать защиту контейнеров в режиме run-time без них не представляется возможным. На рынке представлены специализированные решения, которые обладают обширным функционалом и позволяют охватить сразу несколько областей: безопасность образов, безопасность контейнеров, мониторинг и аудит ИБ, частичные активности других разделов *(например, проверка того, что hardening нод кластера реализован)*. Кроме «корпоративных» решений, можно использовать open source *(который представлен в достаточной степени)* для сборки собственного «комбайна» для защиты среды контейнеризации. Большинство решений интегрируются в CI/CD-pipeline, для некоторых разработаны специализированные надстройки, что упрощает процесс внедрения и настройки.

Secret Management. При разработке ПО, особенно если задействовано множество различных сервисов *(git-системы, контейнерные среды, облачные ресурсы, реестры артефактов и т.д.)*, можно столкнуться с тем, что потребуется выстроить управление такими сущностями, как:

/ API-токены;

/ SSH-ключи;

/ технологические учетные записи;

/ данные аутентификации облачных сервисов;

/ x.509-сертификаты и другие чувствительные данные *(например, пароли)*.

Все вместе это можно назвать одним словом — секрет. Если их немного, управление можно осуществлять вручную. Ситуация меняется, когда число таких сервисов превышает десяток. При этом в отношении секретов требования в области ИБ могут быть различными. Самый простой пример: пароли пользователей и пароли технологических учетных записей. Именно для этих целей применяются решения класса Secret Management — централизованные хранилища, предназначенные для безопасного создания, управления *(доступ и распределение)* и хранения различных секретов.

Помимо централизованного управления секретами, подобные сервисы позволяют в большей степени контролировать доступ. Например, если раньше для взаимодействия трех сервисов использовалась одна технологическая учетная запись, то с функцией динамического предоставления секретов можно создать отдельную учетную запись для взаимодействия «сервис — сервис» без повышения загрузки администратора: выдача, смена и отзыв указанной записи могут происходить автоматически, с использованием функционала решения.

Для взаимодействия приложений между собой или приложений и БД требуются учетные данные, иногда привилегированные. Один из самых простых способов, который иногда применяют на практике, заключается в том, что учетные данные вписывают *(hardcode)* в исходный код, который может быть доступен лицам, не обладающим соответствующими правами. Это повышает вероятность компрометации данных или может привести к недоступности сервиса *(если кто-нибудь, даже по ошибке, сможет изменить данные аутентификации)*. Такие недостатки можно устранить при помощи решения Secret Management: код вызывает функцию, предоставляющую ему секрет, необходимый для установки соединения. Схожий функционал есть, например, у git-систем. Важно не забывать, что мы рассматриваем ситуацию, в которой необходимо централизованно управлять большим количеством секретов разного типа.

www.gartner.com/en/documents/3762274

РЕШЕНИЯ BAS НЕ СПОСОБНЫ ПОЛНОЦЕННО ЗАМЕНИТЬ СПЕЦИАЛИСТА ПО ТЕСТИРОВАНИЮ НА ПРОНИКНОВЕНИЕ, НО МОГУТ НАГЛЯДНО ПОКАЗАТЬ ПРОБЛЕМЫ В ОБЛАСТИ ИБ НА ВСЕХ ЭТАПАХ KILL-CHAIN (УНИВЕРСАЛЬНОГО СЦЕНАРИЯ, ОПИСЫВАЮЩЕГО ДЕЙСТВИЯ ЗЛОУМЫШЛЕННИКА).

Некоторые решения, представленные на рынке, обладают дополнительным функционалом: создание удостоверяющего центра, шифрование данных. Как и большинство приведенных в статье классов решений, системы Secret Management могут быть интегрированы *(использоваться)* в CI/CD-pipeline, где их помощь просто неоценима — ИБ-специалисты вряд ли смогут вручную менять большое количество секретов, используемых при автоматизированных сборках приложений.

BAS. Breach and Attack Simulation — термин, впервые введенный компанией Gartner в 2017 г. BAS — класс решений, которые используются для имитации действий реального злоумышленника при атаках на компанию. Можно сказать, что решения частично позволяют автоматизировать функционал тестирования на проникновение для идентификации потенциальных уязвимостей и для анализа корректности работы средств защиты информации. Решения BAS не способны полноценно заменить специалиста по тестированию на проникновение, но могут наглядно показать проблемы компании в области ИБ на всех этапах kill-chain *(универсального сценария, описывающего действия злоумышленника)*. Для этого специалисты компаний-производителей формируют playbooks *(сценарии действий)*, основанные на активностях реальных хакерских групп, таких как Fancy Bear, Lazarus Group, Dragon Fly 2, или разрабатываемые с учетом готовых фреймворков — MITRE ATT&CK.

- **Разведка и вооружение (Reconnaissance and Weaponization).** Задача BAS — идентифицировать возможные пути проникновения внутрь периметра компании. В качестве его анализа может быть реализована проверка корректности настройки WAF — сделаны попытки реализации SQL-инъекций, XSS, выполнения удаленных файлов на стороне сервера и т.д.
- **Доставка (Delivery).** Многие BAS-решения позволяют имитировать атаки типа «социальная инженерия» путем рассылки email, содержащих вредоносные файлы или ссылки на веб-ресурсы, переходы по которым могут привести к компрометации пользовательских учетных данных. Альтернативный под-

ход — попытки эксплуатации уязвимостей веб-ресурса компании *(данные о которых были получены на предыдущем этапе)* для продвижения атаки «вглубь».

- **Заражение (Exploitation)**. Проверка корректности настроек средств защиты конечных точек. Для этого BAS позволяет эмулировать различные атаки: вирусное заражение, установка троянов и червей, запуск вирусов-шифровальщиков и т.д. Вредоносный код может находиться в содержащем макросы файле MS Word, который был передан в рамках phishing-рассылки на предыдущем этапе. Помимо попыток заражения, на данном этапе BAS-решения могут попытаться собрать дополнительную информацию, пригодную для расширения поверхности атаки *(attack surface)*: о запущенных процессах, доступных портах, сетевых папках *(network share)* и т.д. При каждой попытке атаки решение анализирует, смогли ли системы защиты конечных точек — антивирусы, EDR-системы, системы контроля целостности и т.д. — идентифицировать или заблокировать действия потенциального злоумышленника.
- **Инсталляция (Installation)**. После заражения предпринимаются попытки расширения зоны присутствия за счет анализа сети и оценки возможностей латерального движения *(lateral movement)*, что позволяет оценить, насколько злоумышленник сможет продвинуться и до каких данных добраться. BAS-решение собирает необходимую информацию: данные об операционных системах, используемых службах и портах *(RDP: 3389, SMB: 445 и т.д.)*. Следующий шаг — попытка получить учетные данные *(пароли, токены, kerberos-тикеты)* из оперативной памяти. Для этого может быть использована специальная утилита mimikatz. Получив сведения об окружении и восстановив пароли, BAS пытается получить максимально возможный доступ при помощи техник, которые детально описаны в MITRE ATT&CK framework: pass the password, pass the ticket, pass the hash, kerberoasting и т.д. На протяжении атак BAS анализирует срабатывания межсетевых экранов, IPS- и SIEM-систем. По результатам сканирования формируется отчет о реализованных атаках и о реакции систем безопасности.
- **Управление и действия (Command&-Control and Actions)**. Решение имитирует попытки передачи конфиденциальной информации *(например, данных платежных карт)* за пределы компании, одновременно фиксируя ответную реакцию DLP-систем: была ли предпринята попытка блокировки передачи данных на личный email или нет? Эмуляция передачи может осуществляться по разным векторам: email, облачные сервисы, съемные носители и т.д.

Как организовать имитацию, максимально приближенную к реальным сценариям, без причинения ущерба вычислительным мощностям компании? Можно разместить виртуальные машины в необходимых сетевых сегментах, например, для проверки сетевой доступности. Еще один вариант — установить на вычислительные мощности компании агенты, необходимые для синхронизации с облаком производителя *(многие BAS-решения представляют собой SaaS-платформы)*.

На основании результатов тестирования формируется отчет, содержащий статистическую информацию о том, какие атаки получилось реализовать. Производители некоторых решений, представ-

ИСПОЛЬЗОВАНИЕ ИНСТРУМЕНТОВ ДЛЯ ЗАЩИТЫ ПРИЛОЖЕНИЙ НА ВСЕХ СТАДИЯХ ИХ ЖИЗНЕННОГО ЦИКЛА, КОНЕЧНО, УВЕЛИЧИТ TIME-TO-MARKET. НО КОРРЕКТНАЯ АВТОМАТИЗАЦИЯ СДЕЛАЕТ ЭТО УВЕЛИЧЕНИЕ НЕ СТОЛЬ ЗНАЧИТЕЛЬНЫМ В СРАВНЕНИИ С ПЛЮСАМИ, КОТОРЫЕ МОЖНО ПОЛУЧИТЬ В ЧАСТИ БЕЗОПАСНОСТИ.

ленных на рынке, дают рекомендации по настройке средств защиты информации, выполнение которых не позволит реализовать имитируемую атаку.

Однако и это еще не всё! Рассмотренные примеры решений по автоматизации безопасности касались в большей степени разработки и защиты кода. Но не стоит забывать, что классическая безопасность с межсетевыми экранами, антивирусами, системами мониторинга и корреляции событий ИБ остается. Она необходима в том числе для защиты рабочих станций и серверов, которыми пользуются разработчики для грамотного распределения сетевого доступа между DEV-, TEST- и PROD-сегментами, и для многого другого. Здесь мы не будем подробно останавливаться на этом аспекте, ведь в ограниченном объеме статьи рассмотреть вопросы построения контура безопасной разработки можно лишь поверхностно, а если захватывать еще и «классический» уровень, то уложиться точно не получится. В результате наш первоначальный вариант pipeline может приобрести, например, такой вид (см. рис. 4).

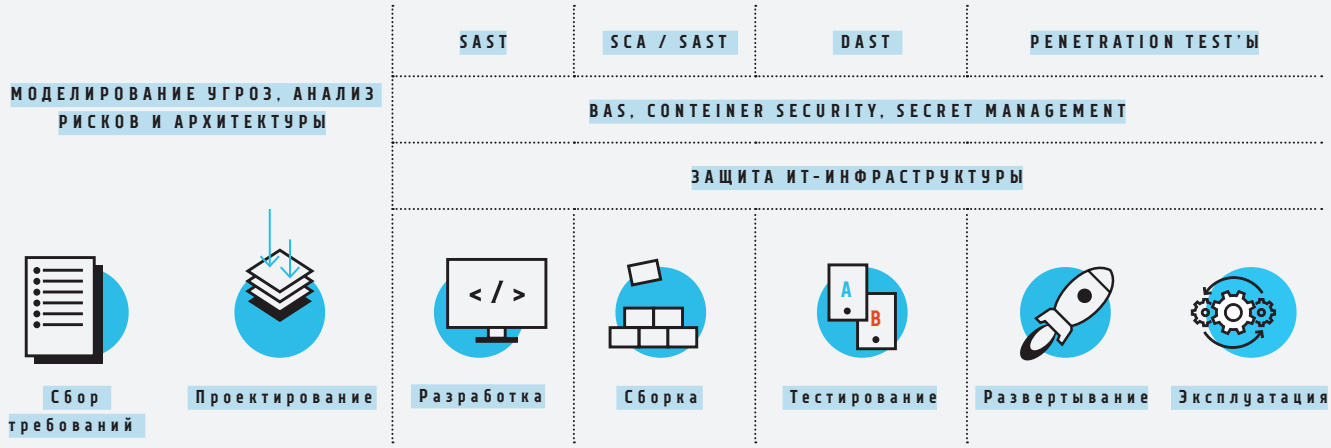
Так на что же следует обращать внимание при выборе инструментария для автоматизации процесса безопасной разработки? Согласно лучшим практикам:

- решения должны обладать возможностью доступа по API, Command Line и/или использовать специализированную надстройку *(для встраивания в CI/CD-pipeline)*;
- решение в виде контейнеров в значительной степени упрощает возможность его применения;
- у решения должны быть минимальные лицензионные ограничения *(например, на параллельное выполнение задач)*;
- итогом работы решения должен быть легко «разбираемый» результат *(parsing)*, например xml и/или json;
- необходимо реализовать возможность подсчета false positive / false negative.

Большое количество инструментов может напугать или привести в некоторое замешательство: «Неужели всё это нужно?». Да, всё. Но не сразу. И не всем. Компании бывают разные: разные уровни зрелости, бизнес-модели. Кто-то разрабатывает ПО для внутренних нужд, кто-то — на продажу клиентам. Соответственно, возникает потребность в различных уровнях защиты ПО. Одной компании хватит SAST, а другой потребуется «полный набор» и еще несколько технологий, которые не были указаны в нашей статье. Главное — выбрать то, что требуется, и приступить

i.blackhat.com/asia-19/Thu-March-28/bh-asia-Shrivastava-DevSecOps.pdf

Рисунок 4. **Общий вид жизненного цикла процесса разработки ПО с ИБ-решениями** *(security pipeline)*



6 ВАЖНЫХ МОМЕНТОВ ПРИ АВТОМАТИЗАЦИИ ПРОВЕРОК ИБ

01

Процессы первичны. Начинайте автоматизацию в соответствии с определенной процессной картой, тогда получится «вдохнуть жизнь» в решение и оно начнет работать. «Поставил и забыл» — это не та стратегия, на которую стоит ориентироваться.

02

Определите наиболее подходящие инструменты. Возможно, вам подойдет open source. А может быть, вы нацелены на корпоративные решения. Или вам нужен гибридный вариант. Инструментов достаточно, главное — найти тот, что подойдет именно вам. Например, не все SAST-решения поддерживают одинаковое количество языков. Некоторые решения Container Security сфокусированы на защите «конечных точек», представленных в виде контейнеров, а некоторые — на обеспечении безопасности сети сред контейнерной виртуализации.

03

Используйте существующее. Вероятно, в компании есть некоторые решения, позволяющие реализовать часть ИБ-требований, а выстраивание процессов позволит повысить эффективность использования внедренных ИБ-решений.

04

Дайте доступ разработчикам к средствам защиты. Практически все средства защиты, используемые при обеспечении ИБ разработки, обладают встроенной ролью для разработчиков, с тем чтобы они могли проводить необходимую аналитику. После внедрения средства защиты проведите семинар для команд, расскажите, что делает система и как ей пользоваться, на что нажимать и как получить необходимую информацию.

05

Используйте метрики. Начать можно, например, с CI/CD, которые наглядно показывают изменение времени сборки приложения с использованием ИБ-решений и без них, что может стать начальной точкой для анализа и ответа на вопрос «Всё ли мы делаем правильно?». Или, например, с сокращения количества false positive в SAST из-за настройки решения по результатам обратной связи от команд разработки. Метрики особенно актуальны, когда в компании есть несколько команд: они помогают понять, где идет «просадка» показателей и как их можно улучшить.

06

Автоматизируйте всё. Использование многочисленных инструментов для защиты приложений на всех стадиях жизненного цикла, конечно, увеличит time-to-market. Но корректная автоматизация сделает это увеличение не столь значительным в сравнении с плюсами, которые можно получить в части безопасности. Это применимо и к ИТ-инфраструктуре: например, целесообразно использовать технологии, позволяющие автоматически разворачивать инфраструктуру и конфигурировать серверы с помощью скриптов, выполнять различные тесты, включая ИБ-тестирование.

к реализации намеченного плана. Необходимо внедрить SAST не просто как технологию. Нужен инструмент для решения поставленных задач с учетом потребностей разработчиков, ИТ- и ИБ-специалистов, и при этом с грамотным выстраиванием процессов. Такое внедрение требует немало времени.

БОЛЬШОЕ КОЛИЧЕСТВО ИНСТРУМЕНТОВ ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССА БЕЗОПАСНОЙ РАЗРАБОТКИ МОЖЕТ НАПУГАТЬ ИЛИ ПРИВЕСТИ В ЗАМЕШАТЕЛЬСТВО: «НЕУЖЕЛИ ВСЁ ЭТО НУЖНО?». ДА, ВСЁ. НО НЕ СРАЗУ. И НЕ ВСЕМ. КОМПАНИИ БЫВАЮТ РАЗНЫЕ: РАЗНЫЕ УРОВНИ ЗРЕЛОСТИ, БИЗНЕС-МОДЕЛИ. КТО-ТО РАЗРАБАТЫВАЕТ ПО ДЛЯ ВНУТРЕННИХ НУЖД, КТО-ТО – НА ПРОДАЖУ КЛИЕНТАМ. СООТВЕТСТВЕННО, ВОЗНИКАЕТ ПОТРЕБНОСТЬ В РАЗЛИЧНЫХ УРОВНЯХ ЗАЩИТЫ ПО. ОДНОЙ КОМПАНИИ ХВАТИТ SAST, А ДРУГОЙ ПОТРЕБУЕТСЯ «ПОЛНЫЙ НАБОР» И ЕЩЕ НЕСКОЛЬКО ТЕХНОЛОГИЙ, КОТОРЫЕ НЕ БЫЛИ УКАЗАНЫ В НАШЕЙ СТАТЬЕ.

ЗАКЛЮЧЕНИЕ

ВОЗМОЖНО, ПОСЛЕ ПРОЧТЕНИЯ СТАТЬИ У ВАС ВОЗНИКНУТ ВОПРОСЫ.

КАКИЕ ПРОЦЕССЫ МНЕ НЕОБХОДИМО РЕАЛИЗОВАТЬ В ПЕРВУЮ ОЧЕРЕДЬ?

У МЕНЯ СТОЛЬКО КОМАНД РАЗРАБОТКИ! МНЕ ИДТИ КО ВСЕМ И СРАЗУ С ЦЕЛЬЮ НАЙТИ SECURITY CHAMPION?

СТОЛЬКО РЕШЕНИЙ ДЛЯ АВТОМАТИЗАЦИИ! ЧТО ВНЕДРИТЬ?

МЫ РЕКОМЕНДУЕМ ПОГРУЖАТЬСЯ В МИР БЕЗОПАСНОЙ РАЗРАБОТКИ ПОСТЕПЕННО, СОЗДАВАЯ «КОНТУР» — СВОЕОБРАЗНУЮ «ВИРТУАЛЬНУЮ ПЛАТФОРМУ», КОТОРАЯ ДОЛЖНА ВКЛЮЧАТЬ В СЕБЯ:

- перечень технологий *(сервисов)*, предоставляемых информационной безопасностью командам;

ГЛАВНОЕ ПРИ ПОСТРОЕНИИ МОДЕЛИ БЕЗОПАСНОЙ РАЗРАБОТКИ – НЕ БРАТЬСЯ ЗА ВСЕ И СРАЗУ. НУЖНО ИДТИ ПОСТЕПЕННО И ВЫБИРАТЬ ТО, ЧТО НЕОБХОДИМО ИМЕННО ВАМ И ИМЕННО СЕЙЧАС ПО ТРЕМ НАПРАВЛЕНИЯМ: ПРОЦЕССЫ, ЛЮДИ И ТЕХНОЛОГИИ.

- описанные процессы и инструкции, отвечающие на вопрос «Что и как делать?», доступные всем участникам процесса;
- ответственных ИБ-специалистов, к которым можно обратиться за советом.

ЧТО ЭТО ЗНАЧИТ? ДОПУСТИМ, НАШ КОНТУР СОСТОИТ ИЗ СТАТИЧЕСКОГО АНАЛИЗАТОРА ИСХОДНОГО КОДА *(Static Application Security Testing)*, ЗАДОКУМЕНТИРОВАННОГО ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ *(отвечает на вопросы, кто запускает сканирование, у кого есть доступ к результатам, кто должен устранить уязвимости, что делать, если уязвимость не может быть устранена, и т.д.)* И ПЕРЕЧНЯ ИБ-СОТРУДНИКОВ, КОТОРЫЕ ОТВЕЧАЮТ ЗА АДМИНИСТРИРОВАНИЕ SAST И ПРОЦЕСС УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ.

ОТЛИЧНО! НАШЛАСЬ КОМАНДА, КОТОРУЮ НЕОБХОДИМО ПОДКЛЮЧИТЬ К НАШЕМУ ВООБРАЖАЕМОМУ КОНТУРУ. ДЛЯ ЭТОГО МЫ ИНТЕГРИРУЕМ ЕЕ GIT-РЕПОЗИТОРИЙ ИСХОДНОГО КОДА ДЛЯ АНАЛИЗА ПРИ ПОМОЩИ SAST, ЯВНО ОПРЕДЕЛЯЕМ ОТВЕТСТВЕННЫХ ЗА РЕАЛИЗАЦИЮ ЭТАПОВ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ, ПРОВОДИМ ВВОДНЫЕ СЕМИНАРЫ. У КОМАНДЫ ДОЛЖНЫ БЫТЬ КОНТАКТЫ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ЧТОБЫ В СЛУЧАЕ НЕОБХОДИМОСТИ БЫЛО К КОМУ ОБРАТИТЬСЯ С ВОПРОСАМИ. И ПРОДОЛЖАЕМ ПРОЦЕСС С КОМАНДАМИ, КОТОРЫЕ ОСТАЛИСЬ «ВНЕ КОНТУРА». НА ДЕЛЕ ВСЕ ЭТО ОБСТОИТ НЕСКОЛЬКО ИНАЧЕ *(сложнее и длительнее)*, НО КОНЦЕПТ ОСТАЕТСЯ ТАКИМ ЖЕ.

ЧТО ВКЛЮЧАТЬ В ЭТОТ КОНТУР НА ПЕРВЫХ ЭТАПАХ? УВЫ, УНИВЕРСАЛЬНОГО ОТВЕТА НЕ СУЩЕСТВУЕТ. В КАЖДОЙ СИТУАЦИИ НУЖЕН ИНДИВИДУАЛЬНЫЙ ПОДХОД. РЕШЕНИЕ ЗАВИСИТ ОТ МНОЖЕСТВА АСПЕКТОВ — НАЧИНАЯ ОТ ОРГАНИЗАЦИОННОЙ СТРУКТУРЫ КОМПАНИИ, ПРИМЕНЯЕМЫХ МЕТОДОВ РАЗРАБОТКИ ПО, ИСПОЛЬЗУЕМЫХ ТЕХНОЛОГИЙ И ЗАКАНЧИВАЯ ОГРАНИЧЕНИЯМИ, К КОТОРЫМ МОЖНО ОТНЕСТИ И КОНКРЕТНУЮ ЦИФРУ ВЫДЕЛЕННОГО БЮДЖЕТА, И ТРЕБОВАНИЯ РЕГУЛЯТОРНЫХ ОРГАНОВ, И НАЛИЧИЕ/ОТСУТСТВИЕ ПОСТАВЩИКОВ РЕШЕНИЙ НА РОССИЙСКОМ РЫНКЕ ИБ.

НАДЕЕМСЯ, ЧТО СТАТЬЯ ПОМОГЛА ВАМ СФОРМИРОВАТЬ ПРЕДСТАВЛЕНИЕ О ТОМ, ЧТО ТАКОЕ БЕЗОПАСНАЯ РАЗРАБОТКА, И ВЫ СМОЖЕТЕ НАЙТИ ПОДХОД К ЕЕ СОЗДАНИЮ И РЕАЛИЗАЦИИ НА ПРАКТИКЕ. ГЛАВНОЕ — НЕ БРАТЬСЯ ЗА ВСЕ И СРАЗУ. НУЖНО ИДТИ ПОСТЕПЕННО И ВЫБИРАТЬ ТО, ЧТО НЕОБХОДИМО ИМЕННО ВАМ И ИМЕННО СЕЙЧАС ПО ТРЕМ НАПРАВЛЕНИЯМ: ПРОЦЕССЫ, ЛЮДИ И ТЕХНОЛОГИИ.

О КОМПАНИИ

РОСБАНК

Руководство компании:
Председатель правления
Илья Андреевич Поляков

Отрасль
Банковская

Год основания
1993

Количество сотрудников
10 000

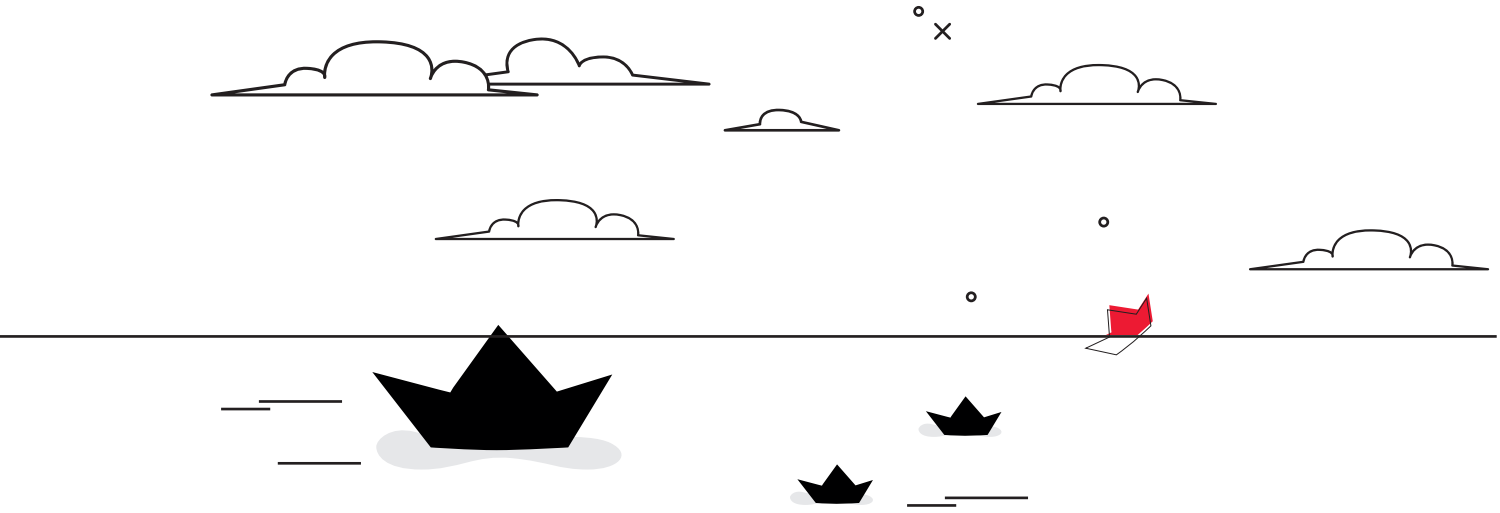
Сайт
www.rosbank.ru

ПРОТИВОДЕЙСТВИЕ ОРГАНИЗОВАННОЙ КИБЕРПРЕСТУПНОСТИ, КАДРОВЫЙ ГОЛОД И ДРУГИЕ ИБ-ВОПРОСЫ. ОПЫТ РОСБАНКА

АВТОР
Михаил Иванов,
директор департамента информационной безопасности «Росбанка»

ОБЪЕМ СТР.

РОСБАНК



/ КАКОВЫ ОСНОВНЫЕ ИБ-ТРЕНДЫ В БАНКОВСКОЙ ИНДУСТРИИ

/ В ЧЕМ ЗАКЛЮЧАЕТСЯ ГЛАВНАЯ СЛОЖНОСТЬ ИСПОЛЬЗОВАНИЯ DEVSECOPS-ПОДХОДА

/ ЧТО РАЗУМНО ОТДАВАТЬ НА АУТСОРСИНГ

МИХАИЛ ИВАНОВ

ПОРТИРОВАТЬ НЕЛЬЗЯ ИЗОЛИРОВАТЬ

Что вы вкладываете в понятие «развитие ИТ»? На ваш взгляд, в последние несколько лет технологии развиваются стремительнее, чем раньше?

Для меня развитие ИТ — это промышленное использование новых технологий, которые ранее применялись в тестовом режиме или для решения узких академических задач. Например, ML, Big Data, контейнеризация и блокчейн уже стали окружающей нас действительностью.

Какие основные ИБ-тренды в банковской индустрии можно отметить в 2019 г.?

Ужесточилось регулирование сферы безопасности: появились новые нормативные акты в области ИБ. Требования ИБ изменились не только количественно, но и качественно, в результате банковская отрасль стала еще более зарегулированной.

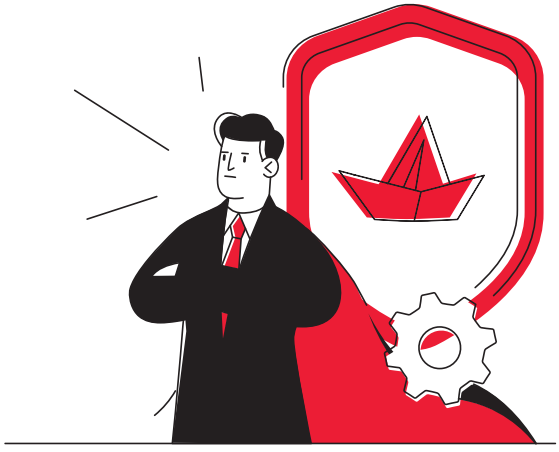
ДЛЯ БАНКОВ АКТУАЛЬНЫ ТРИ ТИПА УГРОЗ: ПРЕРЫВАНИЕ БИЗНЕС-ПРОЦЕССОВ, УТЕЧКА ДАННЫХ И ПРЯМАЯ КРАЖА ДЕНЕГ.

Последние примеры: выпуск нового ГОСТ Р 57580.1-2017, появление нормативной базы по работе с Единой биометрической системой, внесение поправок в Положение Банка России № 382-П.

Я ПРЕДПОЧИТАЮ BSIMM-ПОДХОД (FRAMEWORK DEVSECOPS) И DESCRIPTIVE-КОНЦЕПЦИЮ. ОНИ ПОЗВОЛЯЮТ ПО-НАСТОЯЩЕМУ ПОГРУЖАТЬСЯ В ПРОДУКТЫ И СЕРВИСЫ СВОЕЙ КОМПАНИИ.

Обозначьте наиболее актуальные для банков ИБ-угрозы.

Прерывание бизнес-процессов, утечка данных и прямая кража денег. Остальные угрозы — по сути, варианты реализации этих основных рисков. Например, в 2019 г. была зафиксирована масштабная атака на клиентов крупнейших российских банков, злоумышленники использовали методы социальной инженерии. Анализ атаки выявил новые ИБ-угрозы, связанные с двусторонней аутентификацией банк-клиент и клиент-банк. Это означает, что нам нужно разрабатывать релевантные способы защиты.



Одна из проблем информационной безопасности, о которой регулярно говорят ИБ-директора на профильных конференциях, — использование старого оборудования. Актуально ли это для банковской сферы?

Это актуально для любой компании, которая работает на рынке более 7–10 лет, в том числе для банков. У многих есть legacy-оборудование, которое до сих пор выполняет свои функции, — сетевое железо или рабочие станции на Windows XP, для которых не выпускаются обновления безопасности. Ребята с темной стороны продолжают заниматься «ресерчем» и находят в них все новые и новые уязвимости.

Следующий вопрос проистекает из предыдущего. Существует мнение, что самый простой способ отвечать на новые вызовы в сфере ИБ — регулярно закупать и использовать новейшее специализированное оборудование. Так ли это?

Важно соблюдать баланс между затратами на новое оборудование и ожидаемой выгодой. Для устаревшего оборудования мы разрабатываем и применяем компенсирующие меры. Это дешевле его замены, при этом риски нивелируются. Также необходимо понимать, что существующий в компании бизнес-процесс не всегда подразумевает возможность замены оборудования. Некоторый старый софт может работать только на устаревших версиях операционных систем *(например, на Windows XP)*, и портировать его на новую версию гораздо сложнее, чем просто изолировать этот хост в сети.

Зачастую крупный российский бизнес сливает в корпоративный data lake данные сотрудников, клиентов компании и другую критически важную информацию. При этом доступ к нему имеют большое количество подразделений и отдельных сотрудников, то есть защиту по периметру не так просто построить. Как Росбанк защищает большие данные?

Росбанк активно использует технологии Big Data. Цифровизация, накопление данных и аналитика на больших объемах — неотъемлемая часть современного бизнеса. Для нас вопрос защиты хранилища стоит остро на всех уровнях: инфраструктурном, на уровне взаимодействия с системами-источниками, при подключении пользователей и администраторов, на уровне прикладного ПО. Мы ориентируемся на рекомендации производителей, используем встроенные средства и строим комплексный контур безопасности больших данных.

ПРИНЦИП ЛЕБЕДЯ, РАКА И ЩУКИ

Сейчас есть достаточно много перспективных технологий защиты (Breach and Attack Simulation, SOAR/IRP, защита контейнеризации и т.д.). Каким образом вы определяете целесообразность новых ИБ-инструментов?

Мы идем от конкретных проблем: проводим анализ рисков, оцениваем степень их актуальности. Производители действительно выпускают много новых решений, но зачастую их работоспособность подтверждена только маркетинговыми исследованиями. Нужно смотреть, какие конкретные задачи будет «закрывать» та или иная технология, вовлекать в процесс отбора ИТ-шников, поскольку новый ИБ-инструментарий не должен мешать их процессам. Некоторые риски можно уменьшить с помощью простых мер *(настройки харденинга, введение регламентов и т.д.)*. Экономическую целесообразность никто не отменял.

Как ИБ может доказать бизнесу, что необходимо регулярно выделять бюджеты на обеспечение безопасности? Формализован ли этот процесс в вашем банке?

Как и в любом крупном enterprise, у нас формализован процесс бюджетирования потребностей ИБ. К сожалению или к счастью, финансовые организации, с одной стороны, достаточно зарегулированы с точки зрения ИБ, а с другой — часто атакуемы. Поэтому доказывать бизнесу крупного технологического банка необходимость повышения безопасности не нужно, он все прекрасно понимает и готов к тратам. Другой вопрос, что каждая отдельная трата должна быть обоснована.

Поговорим о DevSecOps. Это относительно новое явление для российского рынка. Как к этому подходу относятся в Росбанке? Внедряете ли вы DevSecOps? С какими сложностями приходится сталкиваться?

Суть DevSecOps в том, что разработчики, инфраструктурщики и ИБ-специалисты вместе делают безопасный продукт. Сама идея не нова, мы и без подобных ярких ярлыков всегда стремились к ней. Поэтому к подходу относимся положи-

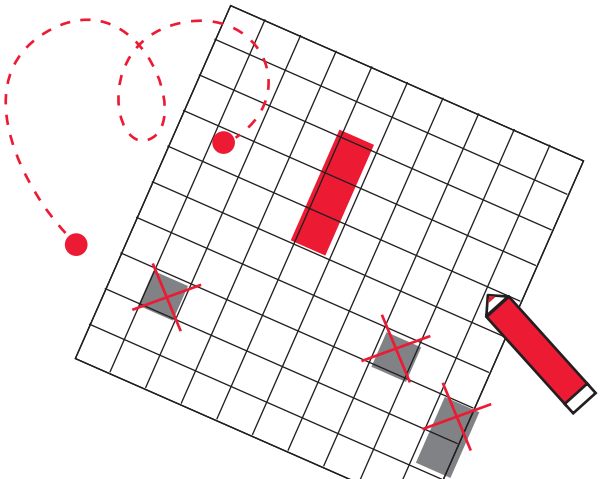
СЕЙЧАС ПРОИСХОДИТ ПЕРЕОСМЫСЛЕНИЕ РОЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В CI/CD, ПОЭТОМУ КОМПАНИИ НАЧИНАЮТ ПРИВЛЕКАТЬ SATELLITE, ИЛИ SECURITY CHAMPIONS.

МЫ НЕ ГОТОВЫ ОТДАВАТЬ НА АУТСОРСИНГ ВОПРОСЫ, СВЯЗАННЫЕ С ДОСТУПОМ К ДАННЫМ НАШИХ КЛИЕНТОВ, ВНУТРЕННЕЙ ПЕРЕПИСКОЙ И СОПРОВОЖДЕНИЕМ DLP-СИСТЕМЫ.

тельно и внедряем его. Безопасность должна закладываться в продукты еще на этапе их создания и контролироваться на протяжении всего жизненного цикла ПО. Основная сложность здесь — коммуникативная. Понятно, где и какие уязвимости могут возникнуть, гораздо труднее выстроить сотрудничество большого количества стейкхолдеров с разными KPI. Они могут взаимодействовать друг с другом по принципу лебедя, рака и щуки из известной басни — проще говоря, ставить во главу угла свои цели, а не желаемый общий результат.

По вашему мнению, DevSecOps — это обязательный подход к разработке ПО? Или он актуален только для отдельных отраслей (ритейла, например)?

Я бы не стал делить по отраслям, в каждом сегменте рынка есть компании, которые строят свой бизнес на максимальной автоматизации, самостоятельной разработке и использовании собственных ноу-хау. Для них DevSecOps актуален. В то же время у этих компаний могут быть прямые конкуренты, которые пользуются коммерческим софтом и у них нет разработки. Им DevSecOps не нужен.



Насколько при реализации DevSecOps принципиально наличие в ИБ-команде Security Champion?

На мой взгляд, сейчас происходит переосмысление роли ИБ в CI/CD, поэтому компании и начинают привлекать satellite, или Security Champions. Это разработчики, специалисты по тестированию, архитекторы, не являющиеся ИБ-экспертами, но заинтересованные в выпуске безопасного и качественного бизнес-продукта.

ИБ и Time-to-Market в банковской сфере — как обеспечить эффективность этого тандема?

Основная задача ИБ — оказывать для бизнеса и ИТ сервис соответствующего уровня с необходимой скоростью. ИБ в вопросах разработки и TTM, создания новых банковских услуг является функцией вспомогательной и контрольной. Система должна быть выстроена таким образом, чтобы результаты контрольной функции не тормозили процесс. Наша задача — предоставлять бизнесу информацию о возможных рисках и путях их оперативного устранения. А бизнес уже решает, готов ли он в каком-то моменте поступиться безопасностью ради скорости вывода продукта на рынок.

ИБ-КАДРЫ И ОРГАНИЗОВАННАЯ КИБЕРПРЕСТУПНОСТЬ

Кадровый вопрос: где брать компетентных ИБ-шников в условиях, когда все стремительно меняется и это стало новой рыночной реальностью? Какой подход вам ближе: растить специалистов самим из вчерашних студентов, переучивать имеющихся сотрудников или перекупать их на рынке?

Мы крупный банк, наша потребность в ИБ-кадрах исчисляется десятками человек, и их крайне сложно найти на рынке. Мы ведем десятки ИБ-проектов, среди

последних и крупных: присоединение банка «ДельтаКредит» в 2019 г. и создание in-house SOC. Так что нам приходится комбинировать все упомянутые подходы. Нельзя набрать только студентов и растить их — мы сразу просядем в квалификации. Перекупить всех необходимых специалистов мы тоже не сможем — слишком дорого. Нужно нанимать квалифицированные кадры, набирать под них студентов-стажеров, где-то переучивать наших ИТ-шников и программистов, которые хотят заниматься ИБ, вовлекать смежные подразделения.

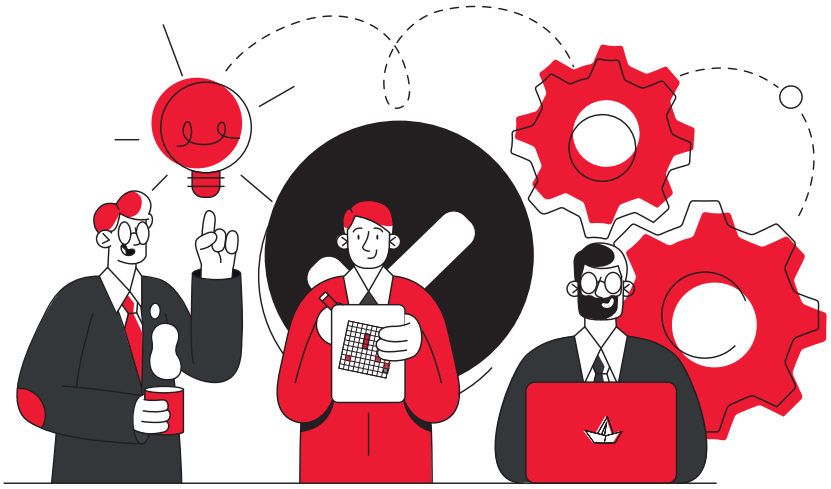
За счет разделения труда у киберпреступников, их квалификация и опыт постоянно растут. Как можно бороться с этим? Как успевать наращивать свои компетенции с такой же скоростью?

Опыт последних лет показывает, что киберпреступники интенсивно прокачивают свои скиллы, атаки становятся все интенсивнее, а методы — изощреннее. Это настоящая организованная преступность, которая хочет заработать денег, а не поприкалываться, как это было какое-то время назад.

В то же время у ИБ-специалистов существует проблема с ростом квалификации. У команды, работающей на определенном участке, замыливается глаз, она может с головой уйти в операционную деятельность и перестать развивать свои компетенции, поскольку нет постоянного прессинга и тренировки на реальных кейсах. Чтобы не попасть в такую ситуацию, мы применяем целый комплекс мер. Это постоянное обучение и повышение квалификации наших ИБ-специалистов, поиск новых кадров, которые могут привнести что-то новое в подходы и методики защиты. Очень важна работа с нашими партнерами. Мы можем сделать один проект по определенной теме за год, а партнер — 20 подобных проектов. Естественно, он приобретает уникальный опыт. Поэтому один из самых действенных способов наращивания компетенций — общение с индустрией, рынком, партнерами и использование их аутсорсинговых услуг там, где это возможно. При этом мы не стараемся всё отдавать на аутсорсинг, используем гибридный подход. Нашей целевой моделью является развитие собственных компетенций и сервисов, при этом мы понимаем, что определенные вещи просто необходимо отдавать на аутсорсинг.

ОРГАНИЗОВАННАЯ КИБЕРПРЕСТУПНОСТЬ СЕГОДНЯ ПРОКАЧИВАЕТ СВОИ СКИЛЛЫ И ХОЧЕТ ЗАРАБОТАТЬ ДЕНЕГ, А НЕ ПОПРИКАЛЫВАТЬСЯ, КАК ЭТО БЫЛО КАКОЕ-ТО ВРЕМЯ НАЗАД.

Мы подключаем партнеров по вопросам, связанным со сложной системной интеграцией и консалтингом, — например, регулярно проводим внешние аудиты. Используем их квалификацию и опыт для реализации ИБ-проектов, но затем стараемся перенять это и поддерживать системы самостоятельно.



ДЛЯ МЕНЯ ГЛАВНЫЙ КРИТЕРИЙ ОТБОРА СОТРУДНИКОВ — ИХ ЧЕСТНОСТЬ

О КОМПАНИИ

КОРПОРАЦИЯ МСП

Руководство компании
Генеральный директор Александр Арнольдович Браверман

Отрасль
Государственный сектор

Год основания
2015

Сайт
www.corpmsp.ru

АВТОР
Сергей Фомиченко,
начальник отдела информационной безопасности Корпорации МСП, MBA

- / КАК УБЕДИТЬ БИЗНЕС В ВАЖНОСТИ ИБ
- / МОЖНО ЛИ ПЕРЕДАВАТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ АУТСОРСЕРАМ
- / КАКИМ ОБРАЗОМ АУТСОРСИНГ РЕШАЕТ ПРОБЛЕМУ КАДРОВОГО ГОЛОДА

ОБЪЕМ СТР.

Корпорация МСП

У НАС ЕСТЬ ТРИ РЫЧАГА УБЕЖДЕНИЯ БИЗНЕСА: ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА, ЭКСПЕРТНЫЕ МНЕНИЯ И ЛУЧШИЕ ПРАКТИКИ. Я НЕ ВИЖУ СМЫСЛА В «ПУГАЛКАХ». ДАЖЕ ЕСЛИ ЭТО СРАБОТАЕТ И ТЫ ПОЛУЧИШЬ НУЖНЫЕ СРЕДСТВА ЗАЩИТЫ, УЖЕ ЗАВТРА ОНИ УСТАРЕЮТ, ПОТОМУ ЧТО ПОЯВЯТСЯ НОВЫЕ УЯЗВИМОСТИ. И ЧТО ТОГДА? СНОВА ПУГАТЬ? КРОМЕ ТОГО, ПРИ ТАКОЙ КОНЦЕПЦИИ РАБОТЫ ФОРМИРУЕТСЯ НЕГАТИВНОЕ ОТНОШЕНИЕ К ОТДЕЛУ ИБ. ГОРАЗДО ВЫГОДНЕЕ РАЗВИВАТЬСЯ ВМЕСТЕ С БИЗНЕСОМ, ПРЕДОСТАВЛЯЯ ЕМУ ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ.

Главная особенность ИБ-ландшафта Корпорации МСП — разделение на внутренние и внешние системы. Первые в основном обеспечивают операционную деятельность компании. Вторые — это публичные системы, предназначенные для пользователей наших веб-сервисов. Например, портал «Бизнес-навигатор МСП» — бесплатный информационный ресурс для предпринимателей, которые хотят открыть или расширить свой бизнес.

HTTPS://SMBN.RU/

Все внешние системы Корпорации МСП должны быть доступны в режиме 24/7. Мы оказываем поддержку субъектам МСП по всей России, это 11 часовых поясов. Так, в региональных лизинговых компаниях, созданных с нашим участием, одна из систем выполняет функцию ядра, обеспечивающего учет сделок. Если она будет недоступна, оператор не сможет оформить сделку.

Мы передали защиту наших ИТ-систем на аутсорсинг «Ростелекому». У нас высокие требования с точки зрения информационной безопасности, потому что такие системы содержат сведения конфиденциального характера и имеют высокую социальную значимость.

Утечка данных может нанести ущерб и нам, и нашим клиентам. Сведения о субъектах МСП включают в себя персональные данные, значит, мы должны обеспечить их защиту в соответствии с законом № 152-ФЗ. Утрата конфиденциальности таких сведений для нас недопустима и гораздо страшнее временной недоступности какого-либо сервиса.

ИБ — это сервисная функция. Информационная безопасность не должна мешать компании достигать поставленных целей, ее задача — помогать бизнесу развиваться, защищая его.

У нас есть три рычага убеждения бизнеса: требования законодательства, экспертные мнения и лучшие практики. Я не вижу смысла в «пугалках». Даже если это сработает и ты получишь нужные средства защиты, уже завтра они устареют, потому что появятся новые уязвимости. И что тогда? Снова пугать? Кроме того, при такой концепции работы формируется негативное отношение к отделу ИБ. Гораздо выгоднее развиваться вместе с бизнесом, предоставляя ему дополнительные возможности.

Нужно объяснять бизнесу стратегическую важность того или иного ИБ-решения, рассказывать, как оно увеличивает ценность продуктов и положительно влияет на репутацию компании.

ПАРАДИГМА «ВСЕ СВОЕ» — В ПРОШЛОМ

Casio делает часы, в которых нет практически ничего «своего», кроме бренда. Они говорят: «Сердце оставьте себе, а все остальное отдайте на аутсорсинг».

Аутсорсинг необходим: он позволяет компаниям быстро меняться в зависимости от динамично меняющихся требований рынка. Если компания не успевает за рынком, она обречена на провал. Допустим, вам резко понадобилось увеличить объем облака, чтобы провести тесты или установить новые средства защиты. Классическая схема с CAPEX не позволяет оперативно реагировать на такие запросы.

Непрерывность сервисов для МСП обеспечивают наши партнеры. Если мы попробуем обойтись своими силами, придется организовать смены, обучить людей, заложить деньги в CAPEX. В итоге выйдет огромная сумма.

Нужно оставить позади парадигму рынка «все свое». Она формировалась в то время, когда технологии для выхода на сервисные модели бизнеса просто отсутствовали. Конечно, вы можете сами построить ЦОД, в котором будет определенное количество серверов, дисковых мощностей, а также ноль возможностей для масштабирования. И быстро останетесь в прошлом.

Не все стоит отдавать на аутсорсинг с точки зрения ИБ. ИТ- и ИБ-инфраструктуру для публичных информационных систем, обрабатывающих персональные данные, мы получаем по сервисной модели от внешнего провайдера. Требования по защите персональных данных формализованы в законе № 152-ФЗ и руководящих документах ФСТЭК России. Какая разница, кто именно будет их выполнять? Если ЦОД сервис-провайдера располагается на территории России, имеет сертифицированные средства защиты, нужные аттестаты и работает в рамках вменяемых SLA и NDA, вас не должно ничего останавливать. Регуляторы не запрещают такого взаимодействия.

Не следует отдавать на аутсорсинг внутренние службы — можно передать только техническую поддержку и обновление некоторых сервисов. Иногда у нас выходят внутренние распоряжения, которые нужно выполнить в течение дня. Если сроки не коррелируют с утвержденными SLA, аутсорсинг только помешает вашей работе.

Есть мнение, что безопасники боятся доверить партнеру инфраструктуру. «Если собственники увидят, что аутсорсинг работает хорошо, то уволят ИБ-отдел». Это миф. Без профильного отдела вы неправильно поставите задачу, не проконтролируете ее выполнение, не сможете адекватно оценить обратную связь и внести изменения в исполняемые задачи при необходимости. Мы берем к себе ИБ-экспертов, которые также способны квалифицированно отслеживать рабо-

№ 152-ФЗ ОТ 27.07.2006

ФЕДЕРАЛЬНЫЙ ЗАКОН О ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящим Федеральным законом регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее — государственные органы), органами местного самоуправления, иными муниципальными органами (далее — муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

ЧАСТЬ 1 В РЕД. ФЕДЕРАЛЬНОГО ЗАКОНА ОТ 25.07.2011 N 261-ФЗ

CONSULTANT.RU/DOCUMENT/CONS_DOC_LAW_61801

ту подрядчиков. Если у вас нет человека с нужными компетенциями, то это будет делать сотрудник, не обладающий глубокими знаниями в информационной безопасности.

КАДРОВОЕ НАПРЯЖЕНИЕ

Специалистов на рынке много, но опытных — мало. Я полгода искал для аттестации информационных систем эксперта, который знает нюансы законодательства и умеет работать с требованиями Федеральной службы по техническому и экспортному контролю. У большинства либо было ничтожно мало опыта, либо не было вообще.

Нам нужны опытные сотрудники, способные «с порога» решать сложные задачи. Мы не готовы брать людей, не понимая, какие специалисты из них получатся. Системы Корпорации динамично развиваются, и ИБ-подразделение не должно быть слабым звеном, замедляющим этот процесс или не обеспечивающим должного уровня безопасности ИТ-решений. Объем и динамика развития систем в нашей компании дают возможность получить богатый опыт, равный которому есть только у ИБ-интеграторов.

Мы поощряем тех, кто хочет учиться новому. Узнать такого человека несложно — достаточно посмотреть на наличие у него подобного опыта. Это может быть дополнительное образование, курсы или сертификаты о повышении квалификации. Сейчас основные критерии успеха — обучаемость, адаптивность и умение восстанавливать энергию. Без последнего можно быстро выгореть на работе.

Аутсорсинг помогает снять кадровое напряжение. У сервис-провайдеров много сильных экспертов, мы столько нанять не сможем — слишком дорого. Нам достаточно взять несколько классных специалистов, способных контролировать сервис-провайдеров.

Мои сотрудники должны обладать навыками проджект-менеджеров. Если говорить в терминологии проектного управления, у нас есть внутренние и внешние заказчики — стейкхолдеры. Внутренние стейкхолдеры — это не только ИТ-департамент, но и другие функциональные подразделения, развивающие информационные системы.

ПРИ ВЫБОРЕ НОВЫХ СОТРУДНИКОВ Я ПРИДАЮ ОГРОМНОЕ ЗНАЧЕНИЕ ИХ ЧЕСТНОСТИ. ДЛЯ МЕНЯ ЭТО ФУНДАМЕНТ БУДУЩИХ ОТНОШЕНИЙ. ЕСЛИ ВЫ НЕ ДОВЕРЯЕТЕ ЧЕЛОВЕКУ, КАК ВЫ ПЛАНИРУЕТЕ С НИМ РАБОТАТЬ? КАК НАДЕЛИТЕ ЕГО ПОЛНОМОЧИЯМИ? НИКАК. ЗНАЧИТ, ЕГО РАБОТУ ПРИДЕТСЯ ДЕЛАТЬ ВАМ. ЗАЧЕМ ТОГДА БРАТЬ ЕГО В КОМАНДУ?

Внешние — это сервис-провайдеры, ИБ-интеграторы: в каждой организации непосредственные исполнители находятся на своем уровне *(руководители проектов, технические специалисты и т.д.)*. Мы должны работать в связке со всеми, и безопасники выполняют в ней роль менеджеров проектов.

При выборе новых сотрудников я придаю огромное значение их честности. Для меня это фундамент будущих отношений. Если вы не доверяете человеку, как вы планируете с ним работать? Как наделите его полномочиями? Никак. Значит, его работу придется делать вам. Зачем тогда брать его в команду?

Раздел II

Оценка ИБ-рисков vs киберпреступность

DLP

- Почему системы DLP недостаточно для предотвращения потерь конфиденциальных данных
- Как выстроить процесс управления данными в компании

Оценка ИБ-рисков

- Как часто нужно проводить и пересматривать оценку рисков
- Какой софт используется для таких проектов

Защита объектов КИИ

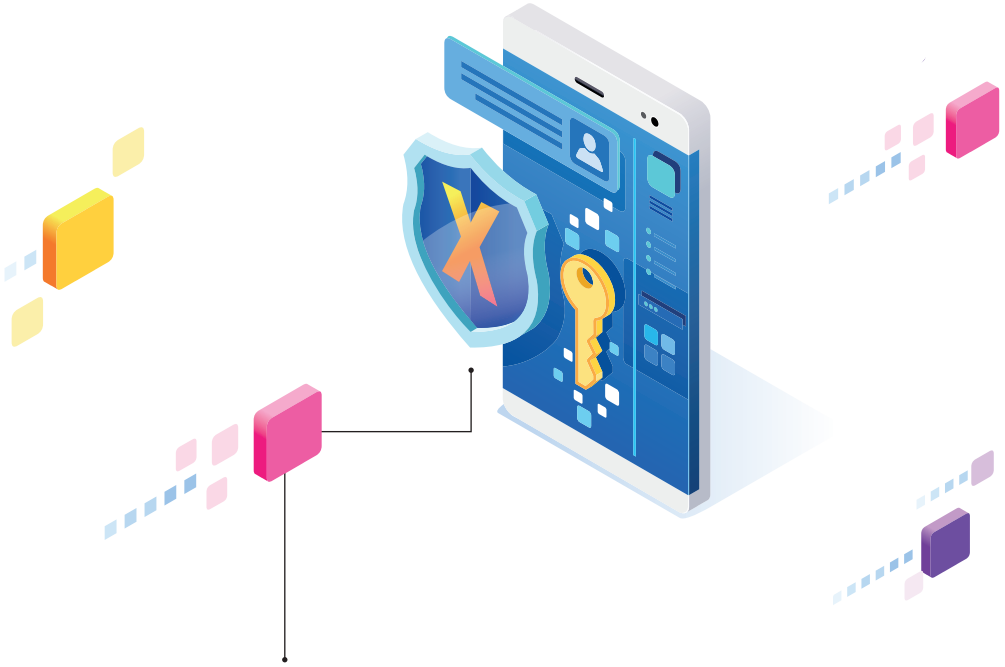
- Как создать систему безопасности значимых объектов КИИ
- Кто и как должен взаимодействовать с объектами КИИ

Рынок киберпреступности

- Топ-10 тенденций из отчета «Hi-Tech Crime Trends 2019/2020» Group-IB
- Масштаб ущерба от киберпреступности. Инфографика

«Многие с удовольствием потратят 10 млн руб. на новую систему, но не выделят и 100 тыс., чтобы научить людей с ней работать. В результате компания будет использовать всего 20% потенциала нового решения, потому что инженеры просто не умеют им пользоваться. Это смешно, ведь стоимость обучения ничтожно мала по сравнению с расходами на инструментарий».

Всеслав Соленик,
директор Центра экспертизы R-Vision



X неизвестных в защите критической информационной инфраструктуры

АВТОР
Виталий Сиянов,
руководитель направления защиты АСУ ТП Центра информационной безопасности компании «Инфосистемы Джет»

ОБЪЕМ СТР.

/ КАК СОЗДАТЬ СИСТЕМУ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КИИ

/ КТО И КАК ДОЛЖЕН ВЗАИМОДЕЙСТВОВАТЬ С ОБЪЕКТАМИ КИИ

/ ЧТО ВКЛЮЧАЕТ В СЕБЯ ПЛАН ОРГАНИЗАЦИИ СЛУЖБЫ БЕЗОПАСНОСТИ ДЛЯ ЗНАЧИМЫХ ОБЪЕКТОВ

ВИТАЛИЙ СИЯНОВ

Прошло уже более 2 лет с момента вступления в силу Федерального закона № 187-ФЗ. Периодически я встречаюсь с представителями компаний — владельцев значимых объектов КИИ по всей стране. И по-прежнему вижу, что лишь немногие из них имеют четкое представление о том, для чего проводится категорирование и какие шаги следует предпринять после него. Чаще всего меня спрашивают: сколько будет стоить «сделать КИИ» под ключ? Мы даем оценку, разъясняя при этом, что можно реализовать «бумажную» безопасность, но лучше воспользоваться шансом и выполнить работу, которую стоило сделать уже давно. Например, ФСТЭК России своим Приказом № 31 от 14 марта 2014 г. уже предписал провести эти работы, но они воспринимались не как обязательные, а скорее как рекомендательные. Тем, кто в свое время реализовал требования Приказа, осталось сделать лишь «косметическое» редактирование, дополнить организационно-распорядительную документацию *(ОРД)* и назначить лиц, ответственных за безопасность значимых объектов.

В статье мы даем свое видение — как выполнить рекомендации закона № 187-ФЗ.

Работы по категорированию можно разделить на 2 части: собственно присвоение категории и создание системы безопасности значимых объектов КИИ. Отметим, что хотя эта система создается в первую очередь для защиты значимых объектов *(то есть имеющих категорию)*, об остальных активах забывать не стоит. Например, если у субъекта есть АСУ ТП, не имеющая категории, но подпадающая под определение «критически важный объект» из Приказа № 31 ФСТЭК, она тоже подлежит защите.

Если с первой частью все более-менее понятно, то создание системы безопасности вызывает недоумение у многих субъектов. Ниже мы разберемся, как ее построить: уточним важные моменты, связанные с реализацией мер защиты, и укажем, на что стоит обратить особое внимание.

Система безопасности должна включать 3 блока: силы *(под этим термином регулятор имеет в виду людей, далее по статье для упрощения понимания мы будем обозначать их именно так)*, организационно-распорядительную документацию и средства защиты информации *(СЗИ)*.

№ 187-ФЗ от 26.07.2017

О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 4. Принципами обеспечения безопасности критической информационной инфраструктуры являются:

1) законность;
2) непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры;
3) приоритет предотвращения компьютерных атак.

HTTP://WWW.CONSULTANT.RU/DOCUMENT/CONS_DOC_LAW_220885

ПРИКАЗ № 235 ФСТЭК РОССИИ

содержит информацию о том, как должна строиться система безопасности, что должно в нее входить, как нужно организовать работу по защите объектов КИИ и какие документы нужно разработать.

ПРИКАЗ № 239 ФСТЭК РОССИИ

Перечислены меры защиты, которые нужно применять исходя из присвоенной объекту категории.

ЛЮДИ

Главный элемент в системе безопасности — люди. Именно им предстоит организовать защиту, оформить документы, внедрить СЗИ и т.д. Сотрудники делятся на 4 сущности *(далее по статье — функциональные роли)*, у каждой свои задачи и ответственность. При этом только совместные действия всех людей, отвечающих за объект КИИ, помогут максимально эффективно предотвратить угрозы.

ЧАСТО МЕНЯ СПРАШИВАЮТ: СКОЛЬКО БУДЕТ СТОИТЬ «СДЕЛАТЬ КИИ» ПОД КЛЮЧ? МЫ ДАЕМ ОЦЕНКУ, НО РАЗЪЯСНЯЕМ ПРИ ЭТОМ, ЧТО МОЖНО, КОНЕЧНО, РЕАЛИЗОВАТЬ «БУМАЖНУЮ» БЕЗОПАСНОСТЬ, НО ЛУЧШЕ ВОСПОЛЬЗОВАТЬСЯ ШАНСОМ И ВЫПОЛНИТЬ РАБОТУ, КОТОРУЮ СТОИЛО СДЕЛАТЬ УЖЕ ДАВНО.

Первая функциональная роль — руководитель или назначенное им уполномоченное лицо. Этот человек обязан создать систему безопасности, контролировать ее функционирование и следить за тем, чтобы она постоянно функционировала. Именно он несет ответственность за ее отсутствие или неработоспособность.

Его главные задачи — назначить ответственных за 3 другие сущности и убедиться в выполнении требований закона. Если в значимом объекте КИИ или структурных подразделениях произойдут изменения, руководитель также будет отвечать за внесение корректировок в систему безопасности.

Вторая функциональная роль — служба безопасности (СБ)*. Ее формирует руководитель предприятия. ФСТЭК России отмечает, что это должно быть специально выделенное подразделение, занимающееся организацией безопасности объектов КИИ. Создать фиктивную СБ, состоящую из ИТ-администратора и бухгалтера, вряд ли удастся. При этом руководитель может возложить эти обязанности на уже существующую службу безопасности.

Основные задачи СБ объектов КИИ — формирование и актуализация организационно-распорядительной документации по реализации мер защиты для остальных категорий сотрудников. Это подразделение определяет, как защищаться от актуальных угроз и какие СЗИ применять.

Но самое важное — реагирование на компьютерные инциденты. При выявлении такого случая СБ должна сообщить о нем в НКЦКИ в течение суток с момента его обнаружения и принять меры по локализации и нейтрализации угрозы, а также минимизации ущерба. Она же будет нести ответственность за попытки замалчивания инцидентов.

Третья роль — подразделения, эксплуатирующие значимые объекты КИИ. Это сотрудники, которые непосредственно взаимодействуют со значимым объектом. На них возлагается обязанность по обеспечению безопасности на основании организационно-распорядительных документов,

*Здесь и далее по тексту под сокращением «СБ» понимается именно служба безопасности.

Рисунок 1. **Сотрудники, взаимодействующие с объектом КИИ, и их задачи**

разработанных СБ. То есть служба безопасности передает функции реализации непосредственно подразделениям и специалистам, которые работают со значимым объектом. При возникновении инцидента они должны первыми реагировать, руководствуясь ОРД, и сообщать о произошедшем в СБ.

Четвертая роль — сотрудники, обеспечивающие функционирование значимых объектов КИИ. Они взаимодействуют с объектом только для реализации определенных функций. Это могут быть ИТ-специалисты, обслуживающие информационные системы. Для них, так же как и для подразделений, обеспечивающих эксплуатацию, служба безопасности разрабатывает ОРД, включающую информацию по работе с объектом КИИ.

Резюме

Субъект должен выделить у себя 4 перечисленные категории, назначить ответственных, сформировать подразделения. Основная задача — создание службы безопасности значимых объектов. Именно она будет выстраивать систему безопасности. Важно обратить внимание на требования, которые регулятор предъявляет к квалификации ИБ-специалистов, и выполнить их заранее.

Без совместной работы всех участников процесса построить рабочую систему безопасности не получится. Эксплуатирующие и поддерживающие ее функционирование подразделения должны активно участвовать в подготовке ОРД. Ведь именно им предстоит выполнять сформированные правила по взаимодействию со значимыми объектами.

ГЛАВНЫЙ ЭЛЕМЕНТ В СИСТЕМЕ БЕЗОПАСНОСТИ – ЛЮДИ. ИМЕННО ИМ ПРЕДСТОИТ ОРГАНИЗОВАТЬ ЗАЩИТУ, ОФОРМИТЬ ДОКУМЕНТЫ, ВНЕДРИТЬ СРЕДСТВА ЗАЩИТЫ.

На заметку

Если у субъекта еще нет службы безопасности, ее необходимо создать в виде отдельного подразделения, а если она уже есть, нужно наделить ее соответствующими полномочиями. В 2021 г. начнут действовать новые требования для персонала ИБ-подразделений объектов КИИ. Так, руководитель по безопасности, не имеющий профильного образования и как минимум 3-летнего стажа работы в сфере ИБ, должен будет пройти курс профессиональной переподготовки (не менее 360 часов). Рядовым специалистам при отсутствии профильного образования будет необходимо пройти курс повышения квалификации (не менее 72 часов). Следует заранее позаботиться о том, чтобы сотрудники, не имеющие нужной квалификации, приобрели ее к указанному сроку, и документально зафиксировать этот факт.

ДОКУМЕНТЫ

После того как субъект выделит людей, работающих со значимыми объектами, ему следует определиться с ОРД. Если посмотреть на таблицу из Приказа № 239 ФСТЭК России, то мы увидим, что каждая группа требований начинается с нулевого пункта. Например, группа «VI. Антивирусная защита» содержит меру «АВ3.0 — Регламентация правил и процедур антивирусной защиты». Следовательно, если для владельца значимого объекта положения этой группы применимы, ему стоит позаботиться о принятии документа, регламентирующего требования к антивирусной защите, соответствующие мероприятия и т.д.

Таблица из Приказа № 239 разбита на 17 групп, к каждой из них нужно разработать новые или актуализировать действующие регламенты. Либо нужно создать документ «Политика ИБ значимых объектов КИИ» и добавить в него соответствующие разделы. Надо отметить, что 17 групп применимы только к объектам 1-й и 2-й категорий значимости. Для 3-й категории исключаются группы III «Ограничение программной среды» и VII «Средство обнаружения вторжения». Но остальные 15 групп необходимо рассмотреть, выделить те, что применимы к объекту КИИ и соответствуют вашим моделям угроз и нарушителей, и приступить к их разработке.

Иерархическая структура необходимых документов представлена в **табл. 1.**

В качестве примера в **табл. 2** представлен минимальный набор регламентов, которые мы готовим для заказчиков в рамках построения системы безопасности для объектов 3-й категории значимости.

СИСТЕМА БЕЗОПАСНОСТИ ДОЛЖНА ВКЛЮЧАТЬ 3 БЛОКА: СИЛЫ (РЕГУЛЯТОР ИМЕЕТ В ВИДУ ЛЮДЕЙ), ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНУЮ ДОКУМЕНТАЦИЮ И СРЕДСТВА ЗАЩИТЫ.

Таблица 1. Иерархия организационно-распорядительной документации значимых объектов КИИ

Документ	Что описывает
Политика информационной безопасности значимых объектов критической информационной инфраструктуры	• Цели и задачи информационной безопасности • Модель нарушителя • Модель угроз • Структура системы безопасности субъекта • Проводимые мероприятия и т.д.
Регламенты и положения	• Функции участников и распределение зон ответственности • Реализация мер информационной безопасности • Порядок реагирования • Информирование и обучение персонала
Журналы, реестры, инструкции	• Правила и процедуры работы со значимым объектом КИИ • Действия при компьютерных инцидентах

Таблица 2. **Пример организационно-распорядительной документации для ЗОКИИ 3-й категории**

№ п/п	Документ	Требования
1	**Политика информационной безопасности значимых объектов критической информационной инфраструктуры**	17 групп Приказа № 239 ФСТЭК Требования Приказа № 235 ФСТЭК
2	**Регламент по защите ОКИИ**	Требования Приказа № 235 ФСТЭК: планирование, реализация, аудит, развитие Требования Приказа № 239 ФСТЭК: I. Идентификация и аутентификация (ИАФ) II. Управление доступом (УПД) XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС) XIV. Управление обновлениями программного обеспечения (ОПО) XV. Планирование мероприятий по обеспечению безопасности (ПЛН)
3	**Регламент учета машинных носителей информации и правил их использования**	XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)
4	**Регламент физического доступа в серверные помещения**	IV. Защита машинных носителей информации (ЗНИ) X. Защита технических средств и систем (ЗТС)
5	**Регламент по антивирусной защите**	VI. Антивирусная защита (АВЗ)
6	**Регламент по обеспечению сетевой безопасности**	XV. Планирование мероприятий по обеспечению безопасности (ПЛН)
7	**Регламент по внутренним проверкам ИБ**	V. Аудит безопасности (АУД)
8	**Регламент резервного копирования**	IX. Обеспечение доступности (ОДТ)
9	**Регламент управления инцидентами ИБ**	XII. Реагирование на компьютерные инциденты (ИНЦ)
10	**Регламент по управлению уязвимостями**	XII. Реагирование на компьютерные инциденты (ИНЦ)
11	**Регламент по управлению изменениями конфигураций ИС**	VIII. Обеспечение целостности (ОЦЛ) XIII. Управление конфигурацией (УКФ)
12	**Политика осведомленности и обучения персонала в области ИБ**	XVII. Информирование и обучение персонала (ИПО)
13	**Политика обеспечения действий в нештатных ситуациях**	XVI. Обеспечение действий в нештатных ситуациях (ДНС)

Указанные в таблице документы в большинстве случаев уже есть в компаниях. Задача тех, кто создает систему безопасности, — проверить, все ли требования регулятора они охватывают. То есть нужно провести аудит документации и добавить недостающие положения.

В НАШИХ ПРОЕКТАХ МЫ ВСЕГДА ПРОВОДИМ АУДИТ И ОБЩАЕМСЯ С ТЕМИ, КОМУ ПРЕДСТОИТ ВЫПОЛНЯТЬ ПРАВИЛА ИЗ ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНОЙ ДОКУМЕНТАЦИИ.

К этому этапу стоит отнестись так же серьезно, как и к выделению людей, ответственных за реализацию ИБ. В наших проектах мы всегда проводим аудит и общаемся с теми, кому предстоит выполнять правила из сформированной документации. Крайне важно грамотно распределить ответственность между подразделениями.

Именно сотрудники, отвечающие за эксплуатацию и поддержание функционирования объектов КИИ, становятся звеном, от которого зависит безопасность. Ведь они непосредственно работают с объектом и могут воздействовать на него. Они со своей стороны должны детально проработать организационно-распорядительную документацию. Ведь после того, как служба безопасности все подготовит, отвечать за инциденты будут именно вышеозначенные подразделения. И скорее всего, именно в этой части возникнут самые большие сложности, так как люди, отвечающие за функционирование объекта, должны будут дополнительно выполнять работу по информационной безопасности, которую им поручит СБ. Мы считаем, что подробное распределение зон ответственности и описание требований к сотрудникам в политиках и регламентах будут способствовать пониманию задач всеми экспертами, участвующими в обеспечении ИБ.

Резюме

ОРД — ответственный этап построения системы безопасности. Именно от того, как составлены документы, зависит, кто и как будет минимизировать последствия при компьютерных атаках. Очень важно правильно сформировать подразделения, отвечающие за эксплуатацию и поддержание функциональности значимых объектов КИИ, снабдить их регламентами и инструкциями, а также периодически проводить учения для выявления пробелов в знаниях.

Что касается структуры документов: в начале описывается политика информационной безопасности *(ее общие положения)*, затем идут регламенты и положения, а на нижнем уровне — журналы, реестры и инструкции. Все документы должны быть утверждены руководителем субъекта и актуализироваться службой безопасности.

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ (СЗИ)

Чаще всего у нас спрашивают: нужно ли использовать только те средства защиты, которые прошли сертификацию во ФСТЭК? Пункт 28 Приказа № 239 говорит о том, что вы можете применять инструменты ИБ, сертифицированные регулятором, но не обязательно только их. Для использования средств защиты, не прошедших сертификацию, необходимо провести их испытания и приемку. Они должны доказать, что, например, антивирус выполняет заявленный функционал и соответствует требованиям Приказа № 239. Для объектов 3-й категории должны быть проведены следующие приемо-сдаточные испытания: «АВЗ.2 – Антивирусная защита электронной почты и иных сервисов», «АВЗ.4 – Обновление базы данных признаков вредоносных компьютерных программ *(вирусов)*», «АВЗ.1 – Реализация антивирусной защиты».

Проблема с несертифицированным антивирусом особенно актуальна для промышленных предприятий, использующих импортное оборудование. Зачастую его производители крайне негативно относятся к применению СЗИ, не прошедших испытания в их лабораториях,

и рекомендуют только одобренные ими продукты. При исполнении гарантийных обязательств в случае неисправности оборудования они в первую очередь проверяют, не вмешивался ли эксплуатант в его работу и не устанавливал ли он нерекомендуемое ПО. При выявлении попыток вмешательства вендор АСУ ТП просто снимает оборудование с гарантии. Поэтому мы постоянно видим на промышленных предприятиях несертифицированные регулятором средства защиты.

Также субъектов волнует, какие именно средства защиты нужно внедрить для выполнения требований регулятора. Ответить однозначно не сможет никто. Во-первых, категорируются 3 разные сущности: информационные системы, информационно-телекоммуникационные сети и АСУ ТП. Для каждой из них есть свои рекомендованные СЗИ. Во-вторых, выполнение более половины требований Приказа № 239 обеспечивается встроенными возможностями. В-третьих, всегда нужно всесторонне оценивать существующие средства защиты, особенно для АСУ ТП.

В качестве примера рассмотрим субъект с АСУ ТП, которая ранее не защищалась, а сейчас ей присвоена 3-я категория значимости. Мы предлагаем обратить внимание на средства защиты из **табл. 3**. Мы всегда предоставляем на выбор решения нескольких вендоров, а если возможно, то и несколько вариантов от выбранного производителя. Например, если субъект хочет установить межсетевой экран, мы предложим продукты как минимум 3 производителей, а затем варианты из модельного ряда, представленного в России.

Таблица 3. **Производители и средства защиты АСУ ТП 3-й категории ЗОКИИ**

Контроль доступа	Dallas Lock	Secret Net, ПАК «Соболь				
Межсетевое экранирование	USG		FortiGate			ARMA
Анализ защищенности	MaxPatrol 8, XSpider	Nexpose		Nessus		
Антивирусная защита					KICS for Nodes, KES	
Мониторинг безопасности	FortiSIEM	MaxPatrol SIEM	ArcSight	QRadar SIEM		
Реализация защищенного удаленного доступа	ViPNet	«Квазар»	«АПКШ Континент», «TLS Континент»			
Централизованное управление ИБ	Resilient Incident Response Platform		SOC 3D			

Перед приобретением средств защиты мы рекомендуем провести аудит ИБ субъекта *(или непосредственно значимого объекта)*. Необходимо проанализировать имеющиеся СЗИ и определить, какие требования Приказа № 239 будут выполняться встроенными средствами защиты, а для каких потребуется приобретение дополнительных.

ГЛАВНАЯ МЫСЛЬ, ПРОХОДЯЩАЯ КРАСНОЙ НИТЬЮ ПО ВСЕМУ ПРИКАЗУ № 239: КАТЕГОРИРОВАНИЕ И СОЗДАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ – ЭТО НЕ РАЗОВЫЙ ПРОЕКТ, А ПРОЦЕСС.

Также стоит отметить требование регулятора к наличию гарантийной и *(или)* технической поддержки установленных средств защиты *(пункт 31 Приказа № 239)*. Мы же часто видим АСУ ТП, которые были внедрены более 15 или даже 20 лет назад, и зачастую на автоматизированных рабочих местах либо вообще не установлены средства защиты, либо установлены старые версии ОС — Windows Vista или XP, которые не поддерживаются даже производителями антивирусов.

Резюме

При построении системы безопасности необходимо уделить большое внимание выбору СЗИ. При этом не стоит забывать о том, что большинство требований, представленных в Приказе № 239, можно выполнить, применяя встроенные возможности и используя ОРД. Конечно, не обойтись без антивируса, защиты удаленного доступа и других средств, но вопрос приобретения необходимого ПО и оборудования должен решаться уже после реализации 2 предыдущих этапов — выделения сил *(ответственных сотрудников)* и актуализации ОРД.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ — ЭТО ПРОЦЕСС

Главная мысль регулятора, проходящая красной нитью по всему тексту Приказа № 239, заключается в том, что категорирование и создание системы безопасности — это не разовый проект, а процесс. Он не может прекратиться. Этот процесс цикличен, мероприятия повторяются из года в год. У каких-то из них будет 3-летний цикл *(например, проверки, проводимые комиссией)*.

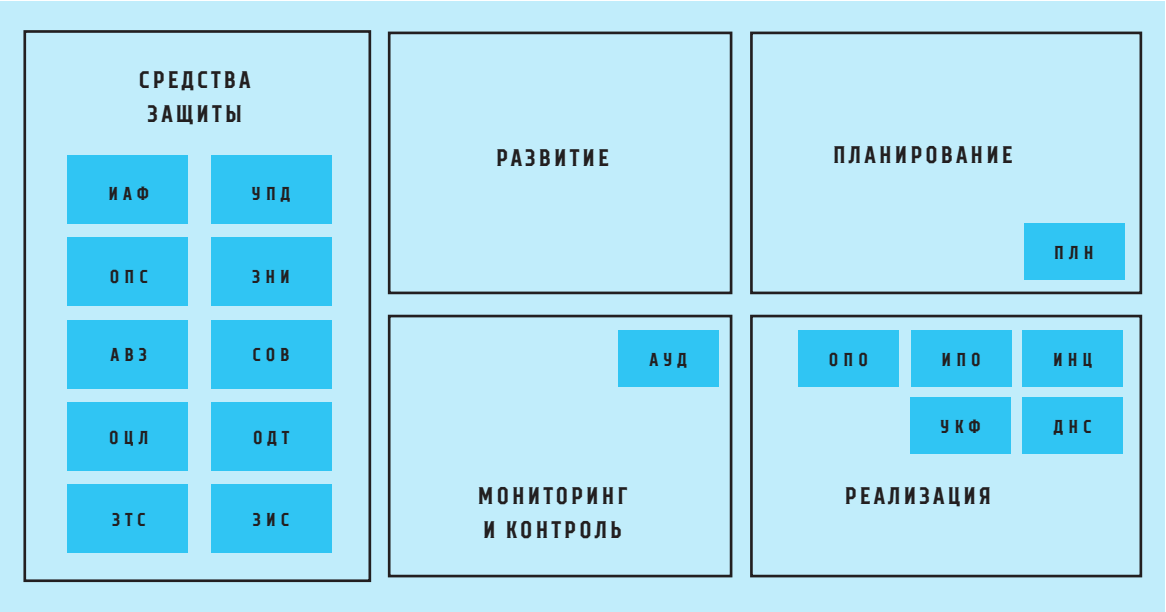
Если субъект считает, что, закупив средства защиты и создав на бумаге систему безопасности, сможет продемонстрировать выполнение требований регулятора во время проверки ФСТЭК, то он глубоко заблуждается. Мало организовать и провести комплекс мероприятий — все функции защиты нужно поддерживать в актуальном состоянии, проводить обучение персонала, обновлять СЗИ и т.д.

Если проиллюстрировать требования 2 основных Приказов, у нас получится 2 блока работ: 1) процесс построения системы безопасности; 2) внедрение ОРД и средств защиты. Процесс всегда будет выглядеть одинаково и состоять из 4 элементов: планирование, реализация, мониторинг и контроль *(аудит)*, развитие *(совершенствование)* **[см. рис. 2]**.

Часть этих требований содержится в обоих приказах. Например, **планирование** является одной из групп Приказа № 239 *(XV. Планирование мероприятий по обеспечению безопасности)*, а в Приказе № 235 *(п. 29)* уточняется: «В рамках планирования мероприятий... осуществляются разработка и утверждение ежегодного плана мероприятий».

Под **реализацией** стоит понимать внедрение средств защиты и действия сотрудников. В качестве примера можно привести группу «XII. Реагирование на компьютерные инциденты *(ИНЦ)*». Рассматривая содержащиеся в ней меры, мы видим, что они начинаются с выявления

Рисунок 2. Система безопасности субъекта



компьютерных инцидентов и заканчиваются предотвращением повторных случаев. Таким образом, служба безопасности объектов КИИ на основе модели нарушителя должна предусмотреть действия злоумышленников и определить, как должны реагировать на это эксплуатирующие подразделения.

Вместо «**мониторинга**» регулятор использует 2 слова: контроль и аудит. Контроль — прерогатива службы безопасности, которая должна следить за действиями подразделений, связанных со значимыми объектами. Также на СБ возложена ответственность за выполнение запланированных мероприятий. При этом Приказ № 235 возлагает контроль за состоянием ИБ субъекта на комиссию, включающую представителей всех подразделений, участвующих в системе безопасности, — от службы безопасности до структур, обеспечивающих функционирование значимых объектов. Для более качественной оценки можно заменить проверку внутренней комиссией на внешний аудит. Выявленные недостатки в любом случае должны быть устранены.

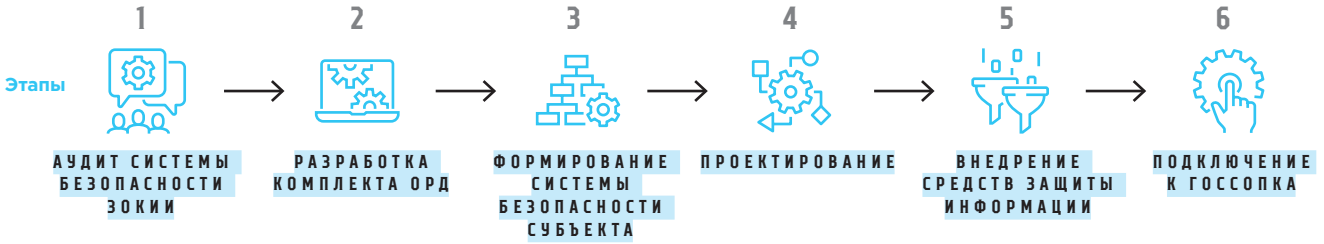
МАЛО ОРГАНИЗОВАТЬ И ПРОВЕСТИ КОМПЛЕКС МЕРОПРИЯТИЙ – ВСЕ ФУНКЦИИ ЗАЩИТЫ НУЖНО ПОДДЕРЖИВАТЬ В АКТУАЛЬНОМ СОСТОЯНИИ, ОБУЧАТЬ ПЕРСОНАЛ, ОБНОВЛЯТЬ СЗИ.

Эта обязанность ложится на плечи службы безопасности. Она должна запустить новый цикл — планирование мероприятий, реализация и контроль исполнения — на основе полученных замечаний.

По замыслу ФСТЭК, эта последовательность мероприятий может быть прекращена только после вывода значимого объекта из эксплуатации. Поэтому мы настоятельно советуем серьезно отнестись к положениям Закона № 187-ФЗ и реализовать его требования.

Для упрощения выполнения этой масштабной задачи мы публикуем план создания службы безопасности для значимых объектов КИИ (см. табл. 4).

Таблица 4. **План организации СБ для значимых объектов КИИ**



1. АУДИТ СИСТЕМЫ БЕЗОПАСНОСТИ ЗОКИИ

СОСТАВ РАБОТ

/ Изучение формы категорирования *(Приказ № 236 ФСТЭК)*, поданной регулятору
/ Составление опросных листов и их заполнение ответственными лицами *(сотрудники, отвечающие за информационную и физическую безопасность, подразделения, эксплуатирующие и поддерживающие функционирование объектов КИИ)*
/ Проверка данных из опросных листов
/ Анализ ОРД по информационной безопасности: политика ИБ, регламенты, инструкции
/ Формирование структуры объектов КИИ
/ Анализ и корректировка модели угроз и модели нарушителя

- Приказ ФСТЭК России № 235, п. 36
- Приказ ФСТЭК России № 239
- № 239, V. Аудит безопасности (АУД)

РЕЗУЛЬТАТ РАБОТ

/ Уточнение модели угроз и модели нарушителя
/ Схемы и описания значимых объектов КИИ с указанием существенных характеристик безопасности, внешних и внутренних информационных потоков значимых объектов КИИ, необходимых для построения системы безопасности
/ Схемы и описание существующей системы защиты информации значимых объектов КИИ
/ Состав и существенные для решения задач проекта характеристики встроенных в значимые объекты КИИ механизмов защиты
/ Состав реализованных организационных мер защиты информации в соответствии с требованиями Приказов ФСТЭК России № 239 и № 235
/ Состав и существенные для решения задач проекта характеристики дополнительных средств защиты информации, используемых на значимых объектах КИИ

2. РАЗРАБОТКА КОМПЛЕКТА ОРД

СОСТАВ РАБОТ

/ Корректировка и *(или)* разработка ОРД

РЕЗУЛЬТАТ РАБОТ

Комплект проектов внутренних нормативных документов в составе:
/ Политика ИБ
/ Регламент управления доступом
/ Положение о защите объектов КИИ *(включающее ограничение программной среды, аудит безопасности, планирование мероприятий по обеспечению защиты информации)*
/ Регламент учета машинных носителей информации и правил их использования
/ Регламент физического доступа в серверные помещения
/ Политика антивирусной защиты
/ Положение по обеспечению сетевой безопасности
/ Положение о внутренних проверках ИБ
/ Регламент резервного копирования
/ Регламент управления инцидентами ИБ

- Приказы ФСТЭК России № 239 (требования к ОРД) и № 235 (требования к системе безопасности)

/ Регламент по управлению уязвимостями
/ Положение об управлении изменениями конфигураций ИС
/ Политика осведомленности и обучения персонала в области ИБ
/ Политика обеспечения действий в нештатных ситуациях

3. ФОРМИРОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ СУБЪЕКТА

СОСТАВ РАБОТ

/ Выделение ответственных *(руководитель, служба безопасности, эксплуатирующие подразделения, подразделения, обеспечивающие функционирование ЗОКИИ)*

- Приказ ФСТЭК России № 235 (требования к организации СБ для ЗОКИИ)

РЕЗУЛЬТАТ РАБОТ

/ Приказ *(распоряжение)* о внедрении организационных мер по обеспечению безопасности значимого объекта КИИ
/ Регламент функционирования системы безопасности субъекта
/ Приказы о выделении сотрудников, ответственных за эксплуатацию и поддержание функционирования значимого объекта КИИ

4. ПРОЕКТИРОВАНИЕ

СОСТАВ РАБОТ

/ *Составление технического проекта и технического задания системы безопасности*

РЕЗУЛЬТАТ РАБОТ

/ Техническое задание на создание системы безопасности
/ **Технический проект системы безопасности:**
- Пояснительная записка к техническому проекту
- Структурная схема
- Ведомость покупных изделий
- Описание настроек средств защиты информации
- Программа и методика испытаний

/ Технико-экономическое обоснование

5. ВНЕДРЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

СОСТАВ РАБОТ

/ *Закупка СрЗИ*
/ *Внедрение и настройка СрЗИ*
/ *Приемо-сдаточные испытания СрЗИ*

- Приказ ФСТЭК России № 239 (требования по СрЗИ)

РЕЗУЛЬТАТ РАБОТ

/ Акт сдачи-приемки оборудования в монтаж
/ Протокол предварительных испытаний
/ Акт о вводе системы в опытную эксплуатацию
/ Журнал опытной эксплуатации
/ Протокол приемочных испытаний

6. ПОДКЛЮЧЕНИЕ К ГОССОПКА

СОСТАВ РАБОТ

/ *Определение необходимых организационных и технических мер для подключения к ГосСОПКА*
/ *Определение подразделений и должностных лиц, ответственных за взаимодействие с НКЦКИ*
/ *Проектирование и внедрение необходимых средств ГосСОПКА*
/ *Разработка ОРД и регламентов*
/ *Подключение к технической инфраструктуре НКЦКИ*
/ *Выполнение функций мониторинга и реагирования на инциденты ИБ*
/ *Выполнение функций по информационному взаимодействию с НКЦКИ (предоставление информации об инцидентах, о защищенности ИС, обработка сообщений от главного центра ГосСОПКА)*

- Закон № 187-ФЗ, ст. 9, п. 2

АНАЛИЗ ИБ-УЯЗВИМОСТЕЙ С ПОМОЩЬЮ ГРАФОВ

/ КАКИЕ ОГРАНИЧЕНИЯ ИМЕЕТ ШКАЛА CVSS, ТРАДИЦИОННО ПРИМЕНЯЕМАЯ ДЛЯ РАНЖИРОВАНИЯ ИБ-УГРОЗ

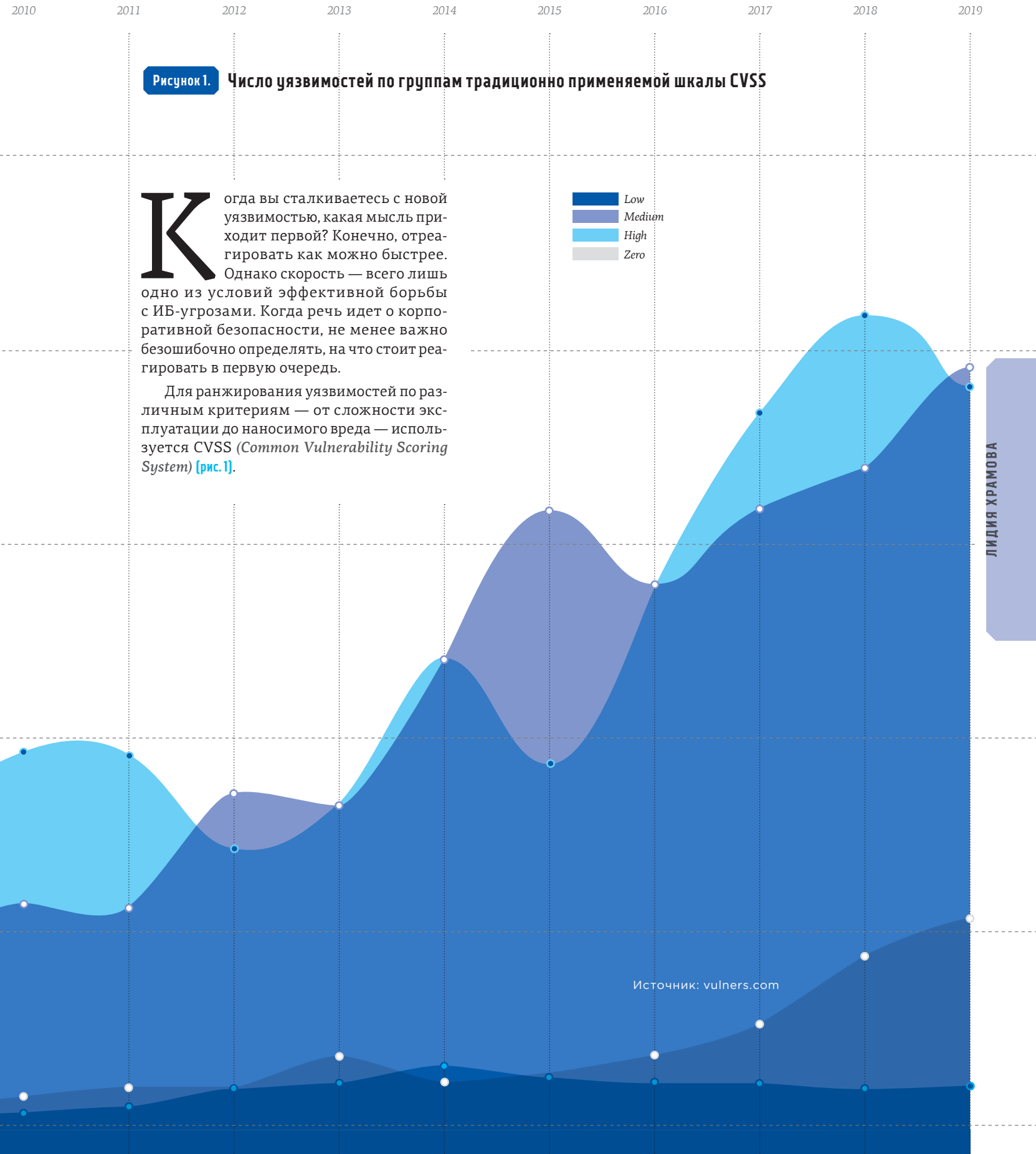
/ ЧЕМ DATA SCIENTISTS МОГУТ ПОМОЧЬ СПЕЦИАЛИСТАМ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

/ КАК ГРАФ СВЯЗАННОЙ ИНФОРМАЦИИ ПОМОГАЕТ КЛАССИФИЦИРОВАТЬ УЯЗВИМОСТИ

АВТОР
Лидия Храмова,
менеджер группы бизнес-моделирования компании QIWI

ЛИДИЯ ХРАМОВА

Рисунок 1. Число уязвимостей по группам традиционно применяемой шкалы CVSS



Когда вы сталкиваетесь с новой уязвимостью, какая мысль приходит первой? Конечно, отреагировать как можно быстрее. Однако скорость — всего лишь одно из условий эффективной борьбы с ИБ-угрозами. Когда речь идет о корпоративной безопасности, не менее важно безошибочно определять, на что стоит реагировать в первую очередь.

Для ранжирования уязвимостей по различным критериям — от сложности эксплуатации до наносимого вреда — используется CVSS *(Common Vulnerability Scoring System)* (рис. 1).

На заметку

Почему именно графы? Они давно применяются для анализа социальных сетей и СМИ — от оценки распространения контента в новостном потоке и влияния топовых авторов на мнение читателей до кластеризации соцсети по интересам. Любая уязвимость может быть представлена как граф, содержащий данные (новости об изменениях в software или hardware и вызванных ими эффектах).

Но у CVSS есть слабое место: она строится на экспертных оценках, не подкрепленных реальной статистикой. Гораздо эффективнее было бы предлагать экспертам уже отобранные по определенным количественным критериям кейсы, чтобы решения принимались на основании проверенных данных. Где их взять и как верно интерпретировать? Это нетривиальная задача для датасаентиста. Именно этот вызов вдохновил команду QIWI совместно с проектом Vulners создать новую концепцию оценки и классификации уязвимостей на основе графа связанной информации.

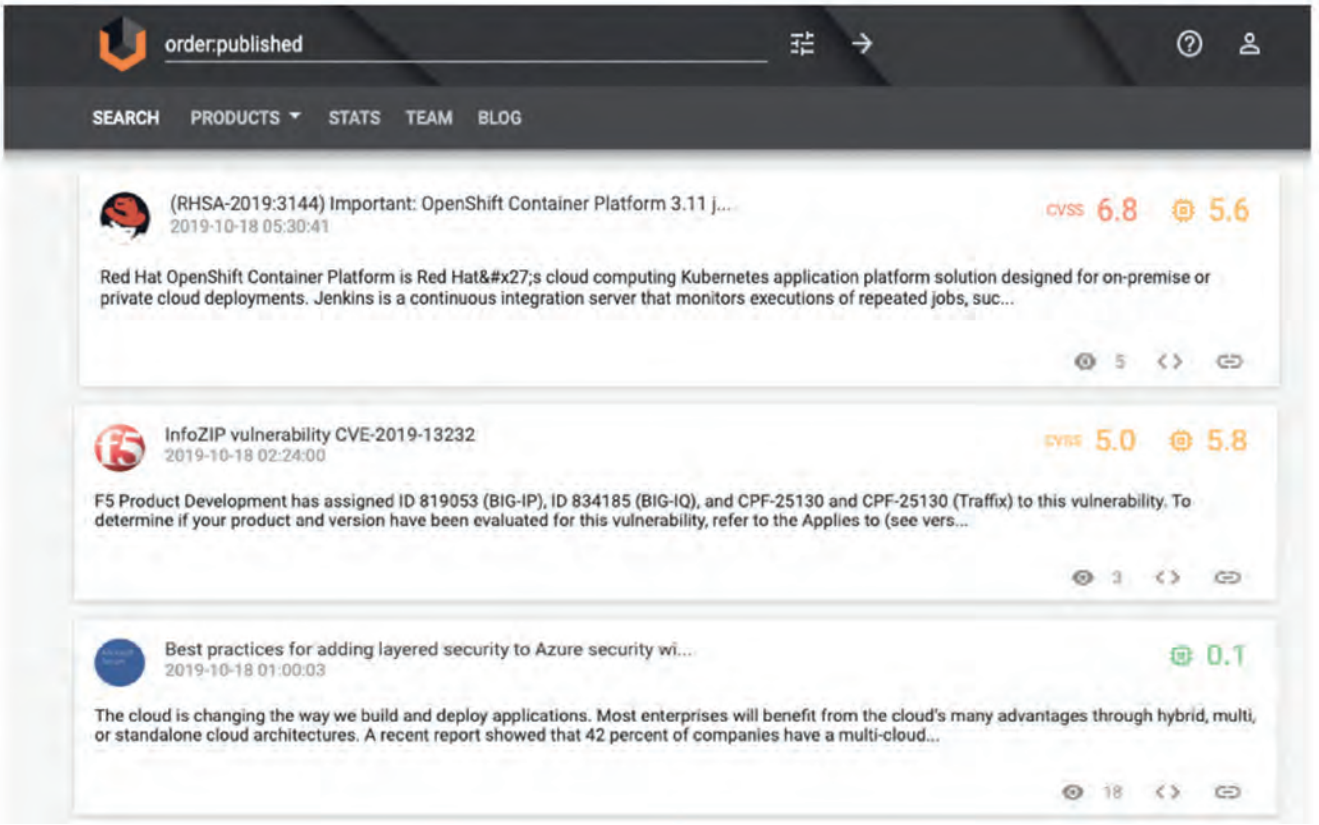
О ДАННЫХ

Нам не пришлось вручную собирать новости об угрозах ИБ, все необходимые тексты содержала открытая база vulners.com (рис. 2).

Каждая уязвимость в базе, помимо названия, даты публикации и описания, имеет присвоенные ей тип *(CVE, nessus и др.)*, семейство *(NVD, scanner, exploit и др.)*, оценку CVSS *(здесь и далее используется CVSS V2.0)*. Также указаны ссылки на связанные новости.

Если представить эти связи в виде графа, то каждая уязвимость будет выглядеть следующим образом (рис. 3): оранжевый кружок обозначает исходную, или родительскую, публикацию, черные кружки — новости, на которые можно кликнуть, находясь на родительской страничке, а серые — связанные новости, до которых можно добраться, только пройдя по публикациям, обозначенным черными кружками. Каждый цвет — это новый уровень графа связанной информации: от нулевого *(исходной уязвимости)* до первого, второго и т.д.

Рисунок 2. Примеры новостей на vulners.com



Конечно, при просмотре одной новости нам известны только нулевой и первый уровень. Поэтому для получения всех данных мы использовали метод обхода графа в глубину, позволяющий распутать клубок новостей от начала до самых последних связанных узлов *(далее — нод графа)*. Как выглядят графовые данные? На **рис. 4** мы представили граф известной, но не очень опасной уязвимости Heartbleed *(5 из 10 баллов по шкале CVSS V2.0)*.

Глядя на этот пышный «букет» из связанных новостей и эксплойтов, где красная точка — исходная уязвимость, мы понимаем, что Heartbleed был существенно недооценен. Этот пример показывает, что графовые метрики качественно оценивают системность, продолжительность и другие параметры уязвимости. Ниже мы приведем несколько кейсов из нашего исследования, которые послужили базой для разработки альтернативной классификации:

- **число нод в графе** отвечает за «широту» уязвимости и показывает, насколько большой след она оставила в различных системах;
- **число подграфов** *(крупных скоплений новостей)* отвечает за гранулярность проблемы или наличие крупных проблемных зон для ИБ-специалистов внутри уязвимости;
- **число связанных эксплойтов и патчей** говорит о взрывоопасности уязвимости и о том, сколько раз ее приходилось «лечить»;
- **количество типов и семейств новостей в графе** — о системности, то есть числе

Рисунок 3. Графовый вид исходных данных

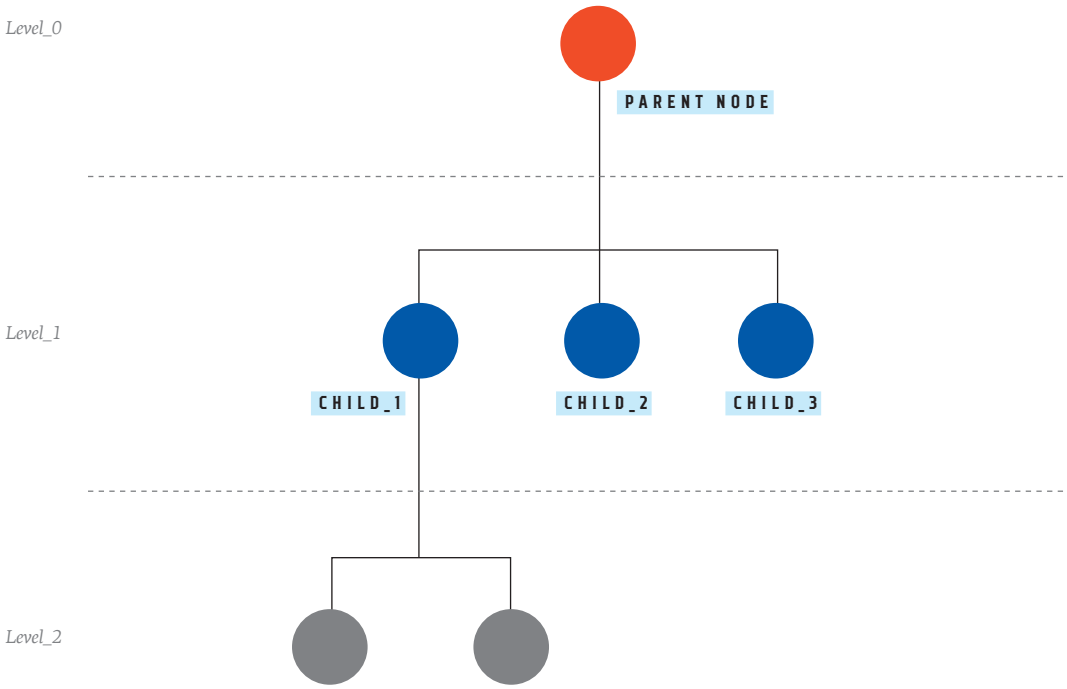
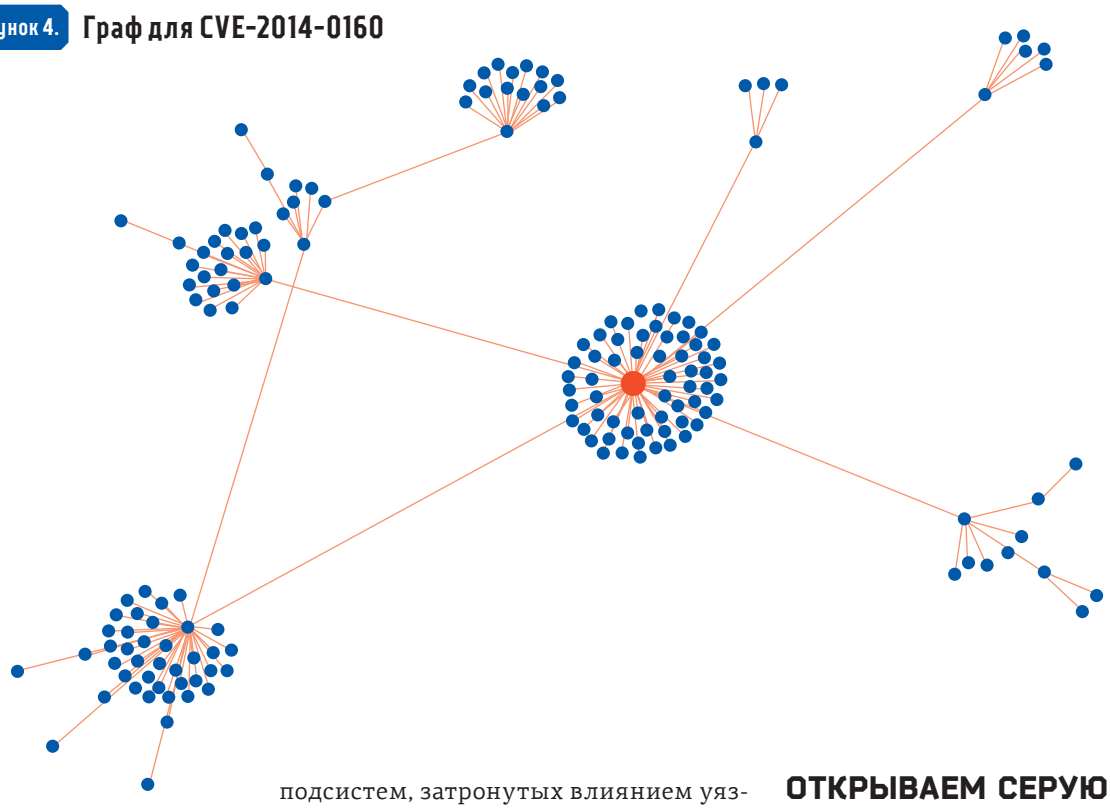


Рисунок 4. Граф для CVE-2014-0160



подсистем, затронутых влиянием уязвимости;

- **время от первой публикации до первого эксплойта и до последней связанной новости** — о темпоральной природе уязвимости, тянется ли она с большим «хвостом» последствий или быстро развивается и затухает.

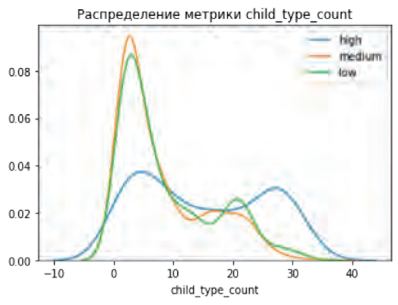
Конечно, это не все наши метрики, «под капотом» исследования сейчас порядка 30 показателей, дополняющих базовый набор критериев CVSS V2.0.

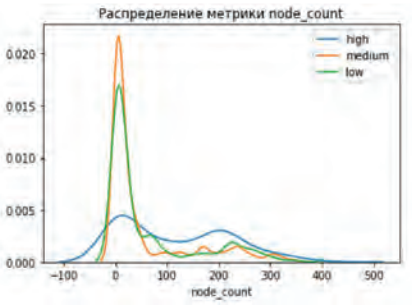
ОТКРЫВАЕМ СЕРУЮ ЗОНУ

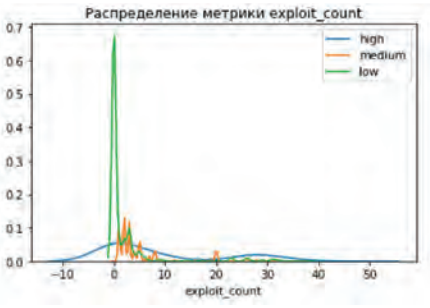
А теперь немного Data Science и статистики, ведь гипотезы нужно подтверждать на данных. Для эксперимента с альтернативной шкалой и новыми метриками мы отобрали новости, опубликованные в январе 2019 г. (2403 бюллетеня и более 150 тысяч строк в графе новостей). Все исходные уязвимости были разделены на 3 группы по CVSS:

- High — от 8 баллов включительно;
- Medium — от 6 *(включительно)* до 8 баллов;
- Low — менее 6 баллов.

Рисунок 5. Графовые метрики для групп CVSS V2.0







Для начала мы проверили, как CVSS-балл коррелирует с числом и типом связанных новостей в графе, а также с числом эксплойтов (рис. 5). В идеале мы должны были увидеть четкое разделение метрик на 3 кластера, однако этого не произошло. Это указало на возможное наличие серой зоны, которую CVSS не определяет.

Затем мы провели кластеризацию уязвимостей, сгруппировав их в однородные группы, и построили новую шкалу. Для первой итерации был выбран метрический классификатор и получена новая матрица оценок: по оси X — класс уязвимостей, где 2 — максимально крупные по нашим метрикам, 1 — новые уязвимости, 0 — самые маленькие; по оси У — исходные баллы *(High, Medium, Low)* (рис. 6).

На рис. 6 зона, помеченная овалом *(класс 2 с первоначальными оценками low & medium)*, — потенциально недооцененные уязвимости. Разделение на новые классы выглядит более четким по сравнению с CVSS, чего мы и добивались (рис. 7).

Рисунок 6. Кластеризация уязвимостей

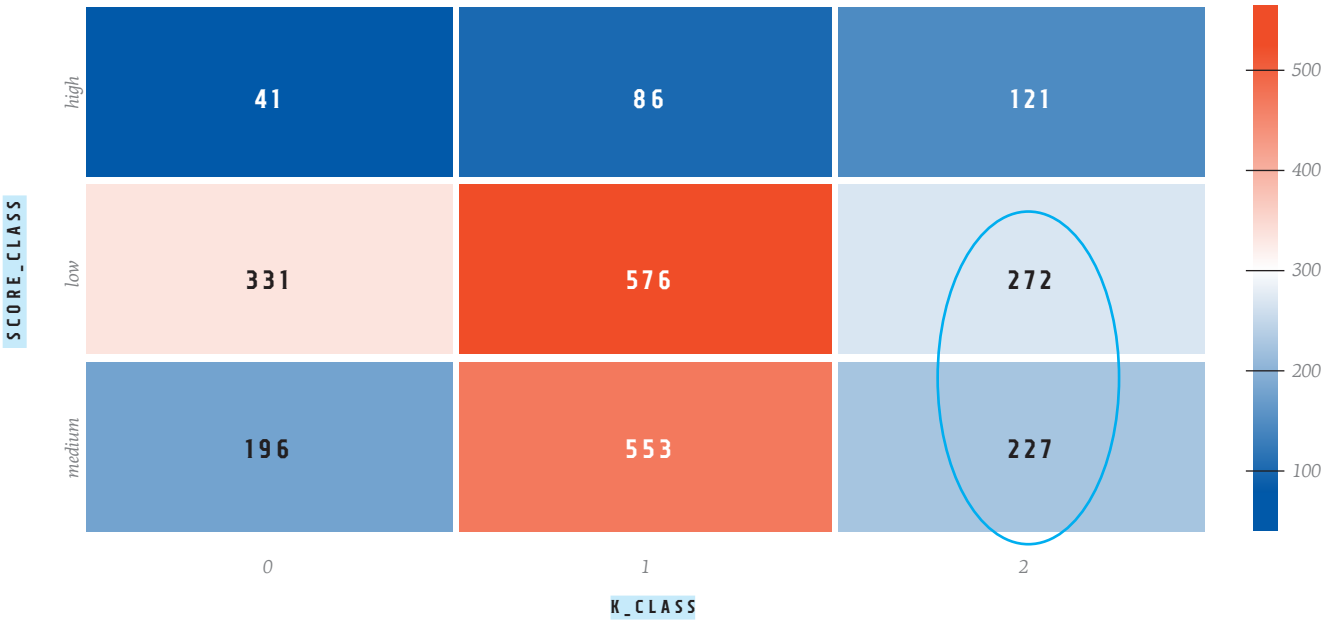
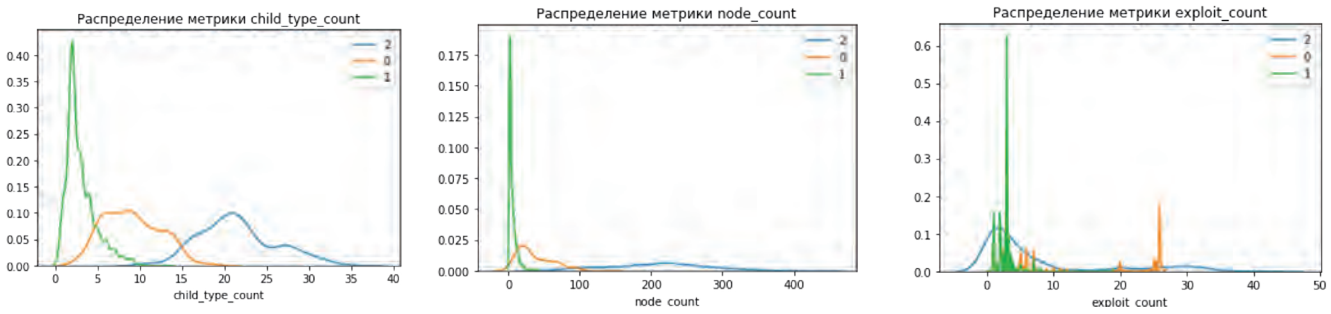


Рисунок 7. Графовые метрики для альтернативной классификации



Однако просто доверять модели — плохая идея. Мы точечно проверили ее, взяв несколько уязвимостей для детального анализа. На **рис. 8–11** представлены яркие образцы из серой зоны. Они имеют низкий балл CVSS, но высокий графовый балл, а значит, потенциально требуют другого приоритета работы с ними.

Концепция была подтверждена статистикой и точечной проверкой. В ближайшем

Рисунок 8. **CVE-2019-0555** *(балл CVSS — 4,4, графовый класс 2 — high)*

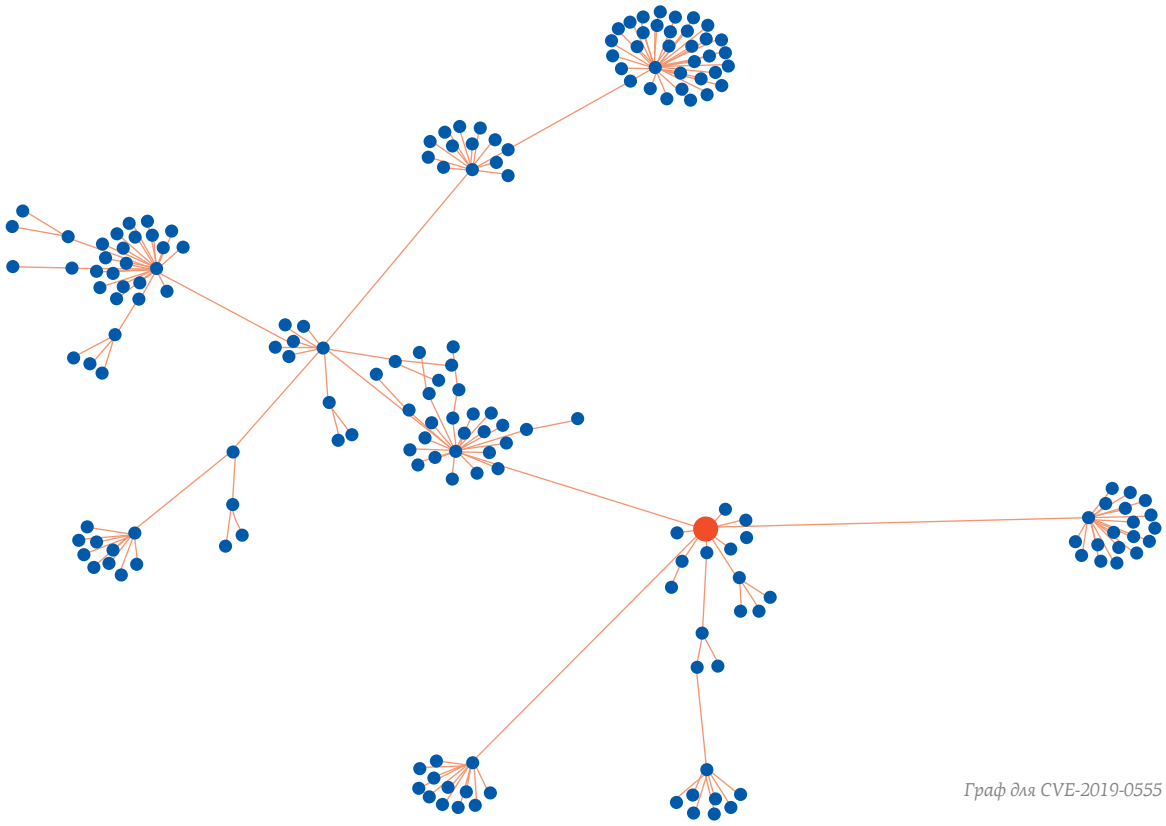
CVE-2019-0555
2019-01-08 21:29:00

CVSS 4.4
5.4

ID CVE-2019-0555
Type cve
Reporter cve@mitre.org
Modified 2019-02-26 20:53:00

Description

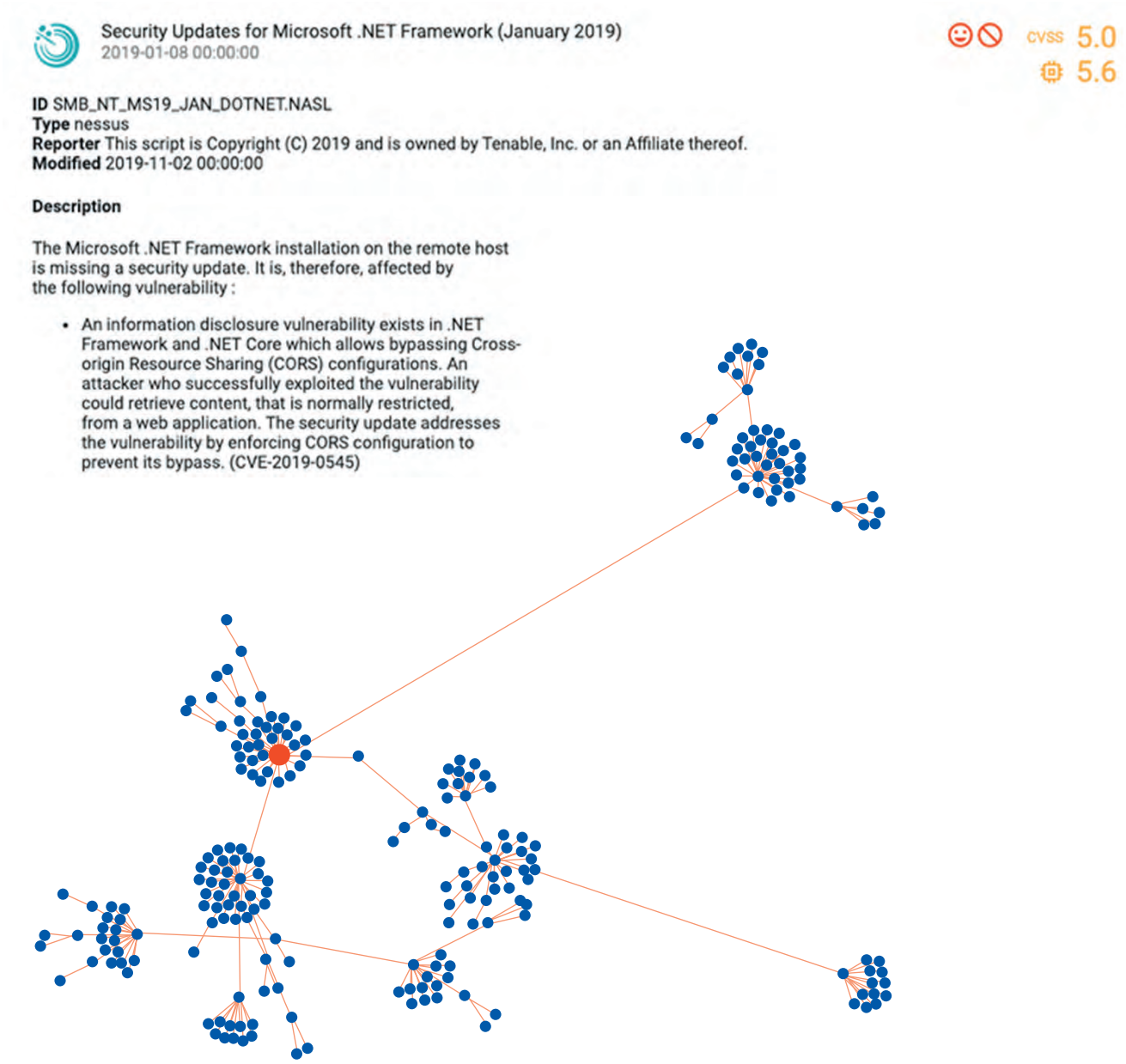
An elevation of privilege vulnerability exists in the Microsoft XmlDocument class that could allow an attacker to escape from the AppContainer sandbox in the browser, aka "Microsoft XmlDocument Elevation of Privilege Vulnerability." This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers.



Граф для CVE-2019-0555

будущем мы планируем автоматизировать сбор графовых метрик, а также реализовать production-версию нашего классификатора, чтобы команда ИБ использовала его в работе с уязвимостями. На этом пути еще много вызовов — от сбора огромного числа новых графов по не охваченным в исследовании месяцам до оптимизации модели.

Рисунок 9. **SMB_NT_MS19_JAN_DOTNET.NASL** *(балл CVSS — 5,0, графовый класс 2 — high)*



Граф для SMB_NT_MS19_JAN_DOTNET.NASL

Рисунок 10. **CVE-2019-1653** *(балл CVSS — 5,0, графовый класс 2 — high)*

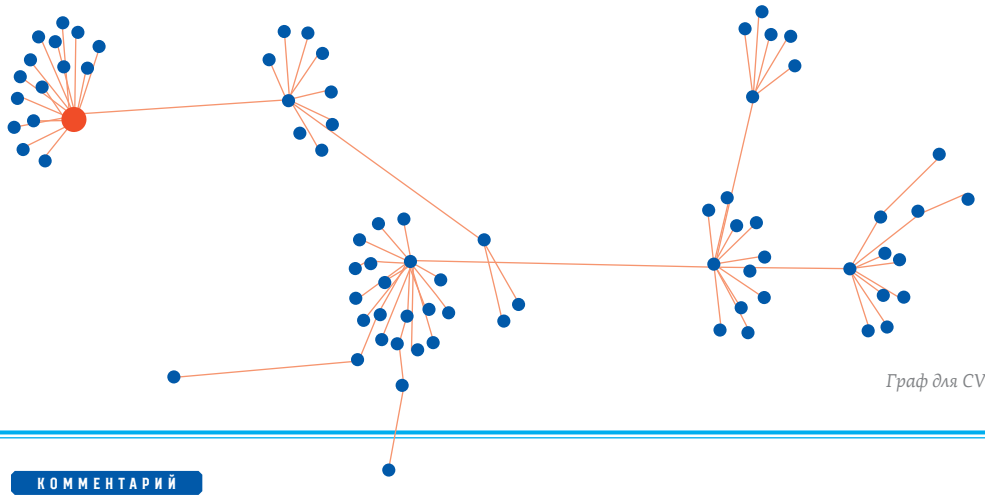
CVE-2019-1653
2019-01-24 16:29:00

CVSS 5.0
3.8

ID CVE-2019-1653
Type cve
Reporter cve@mitre.org
Modified 2019-04-08 20:29:00

Description

A vulnerability in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an unauthenticated, remote attacker to retrieve sensitive information. The vulnerability is due to improper access controls for URLs. An attacker could exploit this vulnerability by connecting to an affected device via HTTP or HTTPS and requesting specific URLs. A successful exploit could allow the attacker to download the router configuration or detailed diagnostic information. Cisco has released firmware updates that address this vulnerability.



Граф для CVE-2019-1653

КОММЕНТАРИЙ

Павел Волчков,

заместитель директора Центра информационной безопасности компании «Инфосистемы Джет»

Этот кейс будет интересен крупным компаниям, уделяющим внимание теме Vulnerability Management. Именно крупным, потому что одна из основных проблем ИБ-специалистов связана с приоритизацией уязвимостей. Что вообще нужно устранять? Что из этого — в первую очередь? Где и в какой срок необходимо закрыть самые критичные уязвимости? Ответы на эти вопросы невозможно найти, применяя шаблонные методики Vulnerability Management «в лоб». Использование кастомных наработок, подобных той, что была реализована в QIWI, дает прямую экономическую выгоду за счет сокращения времени, затрачиваемого на исправление уязвимостей, которые по факту таковыми не являются. Сама идея выглядит свежей и интересной. Вопрос, как это часто бывает, — в полноте ее реализации, а также в том, все ли значимые исходные параметры были учтены. На мой взгляд, для того чтобы использовать этот инструмент в повседневной деятельности ИБ-подразделения, его необходимо доработать.

Рисунок 11. **RHSA-2019:0130** *(балл CVSS — 5,0, графовый класс 2 — high)*

CVSS 5.0
6.9

(RHSA-2019:0130) Moderate: Red Hat JBoss Web Server 3.1 Service Pack 6 security and bug fix update
2019-01-22 18:28:08

ID RHSA-2019:0130
Type redhat
Reporter RedHat
Modified 2019-01-22 18:28:31

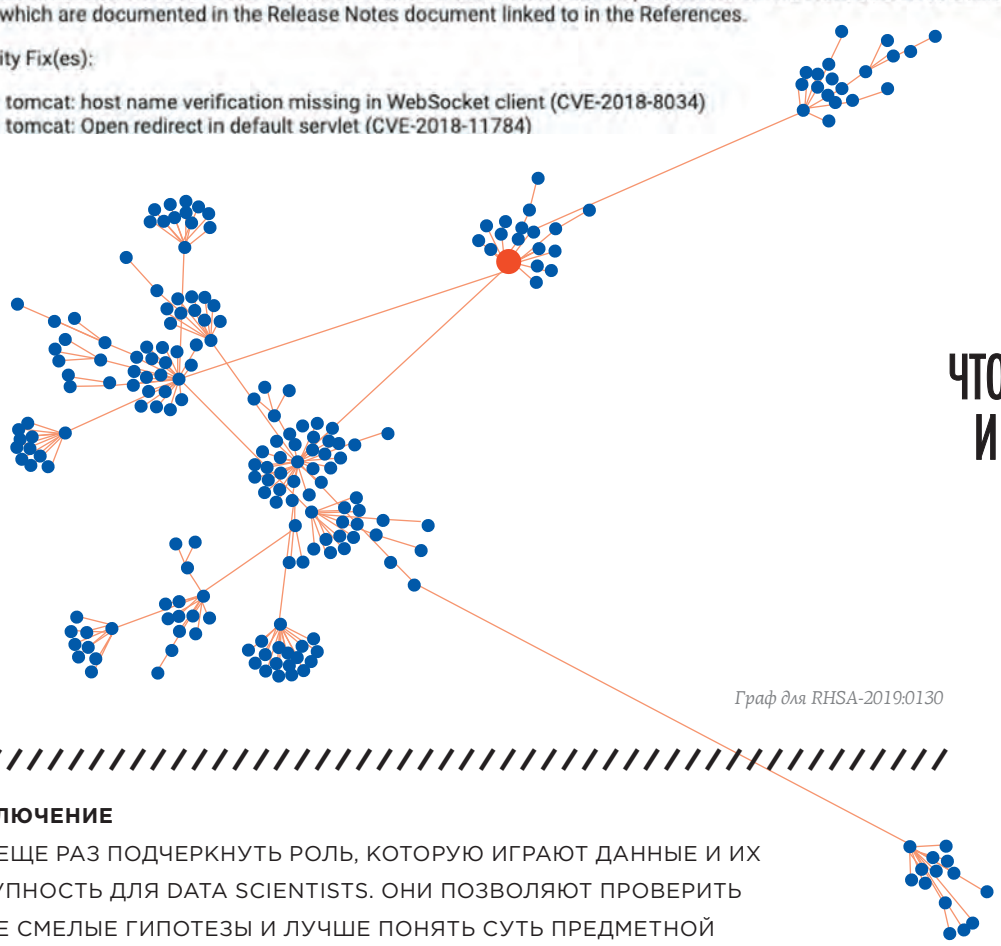
Description

Red Hat JBoss Web Server is a fully integrated and certified set of components for hosting Java web applications. It is comprised of the Apache HTTP Server, the Apache Tomcat Servlet container, Apache Tomcat Connector (mod_jk), JBoss HTTP Connector (mod_cluster), Hibernate, and the Tomcat Native library.

This release of Red Hat JBoss Web Server 3.1 Service Pack 6 serves as a replacement for Red Hat JBoss Web Server 3.1, and includes bug fixes, which are documented in the Release Notes document linked to in the References.

Security Fix(es):

- tomcat: host name verification missing in WebSocket client (CVE-2018-8034)
- tomcat: Open redirect in default servlet (CVE-2018-11784)



Граф для RHSA-2019:0130

НАШ КЕЙС ПОКАЗЫВАЕТ, ЧТО DATA DRIVEN И INFORMATION SECURITY ОТЛИЧНО ДОПОЛНЯЮТ ДРУГ ДРУГА.

В ЗАКЛЮЧЕНИЕ

ХОЧУ ЕЩЕ РАЗ ПОДЧЕРКНУТЬ РОЛЬ, КОТОРУЮ ИГРАЮТ ДАННЫЕ И ИХ ДОСТУПНОСТЬ ДЛЯ DATA SCIENTISTS. ОНИ ПОЗВОЛЯЮТ ПРОВЕРИТЬ САМЫЕ СМЕЛЫЕ ГИПОТЕЗЫ И ЛУЧШЕ ПОНЯТЬ СУТЬ ПРЕДМЕТНОЙ ОБЛАСТИ. ГЛАВНОЕ — НЕ ОГРАНИЧИВАТЬСЯ ОБЩЕПРИНЯТЫМИ РАМКАМИ. ПОЭТОМУ, ЕСЛИ ВЫ ЕЩЕ НЕ СОБИРАЕТЕ ИЛИ УДАЛЯЕТЕ «НЕНУЖНЫЕ» ДАННЫЕ, ЗАДУМАЙТЕСЬ: КАЖДЫЙ БАЙТ МОЖНО ИСПОЛЬЗОВАТЬ ЭФФЕКТИВНО.

ОЦЕНКА РИСКОВ КАК MUST HAVE,

ИЛИ ПЕРЕСТАНЬТЕ ТЫКАТЬ ПАЛЬЦЕМ В НЕБО

АВТОР
Всеслав Соленик,
директор Центра экспертизы R-Vision

/ КАК ЧАСТО НУЖНО ПРОВОДИТЬ ОЦЕНКУ РИСКОВ

/ КАКОЙ СОФТ ЦЕЛЕСООБРАЗНО ИСПОЛЬЗОВАТЬ ДЛЯ ТАКИХ ПРОЕКТОВ

/ ПО КАКИМ ПРИЧИНАМ СНИЖАЕТСЯ ПРОДУКТИВНОСТЬ ИБ-СПЕЦИАЛИСТОВ

ОБЪЕМ СТР.

— Какие угрозы кибербезопасности сегодня наиболее актуальны?

— Зависит от профиля компании. Каждая организация с помощью оценки рисков должна выявить наиболее актуальные для себя угрозы. Если этого не сделать, то их актуальность будет определяться по принципу «пальцем в небо». Например, систему ДБО банка с высокой долей вероятности будут атаковать хакеры, чтобы украсть деньги.

То, что у вас нет инцидентов, не значит, что угрозы неактуальны. Это может означать, что вы их не выявили и не знаете о них.

Если брать весь рынок, то ситуация с глобальными угрозами не меняется. Может быть, только Интернет вещей выстрелил некоторое время назад: прошла волна крупных DDoS-атак с использованием гигантского количества утюгов и пылесосов. В целом же можно повторить слова многих спикеров о том, что «количество угроз ИБ растет, все плохо, надо покупать средства защиты и т.д.».

При управлении рисками угрозы ранжируют исходя из актуальной модели нарушителя, предпосылок и потенциального ущерба, который может наступить при их реализации. Проще говоря, если угроза может повлечь за собой 6 млн руб. ущерба,

ЛИЦА, ПРИНИМАЮЩИЕ РЕШЕНИЯ (ЛПР), СЧИТАЮТ ДЕНЬГИ И ХОТЯТ ВИДЕТЬ, ГДЕ БЕЗОПАСНОСТЬ ЗАРАБАТЫВАЕТ ИЛИ ЭКОНОМИТ. УЗНАТЬ ЭТО МОЖНО ТОЛЬКО ОДНИМ СПОСОБОМ – ОЦЕНИТЬ РИСКИ. ПОЗДНО ОЦЕНИВАТЬ УЩЕРБ, КОГДА ОН УЖЕ НАСТУПИЛ, А ДЕНЬГИ УТЕКЛИ.

то она актуальнее той, что оценивается в 200 тыс. Так их и надо ранжировать.

О РИСКАХ ИБ

— Как часто нужно проводить и пересматривать оценку рисков?

— С периодичностью от года до трех лет. При соблюдении регуляторных требований, серьезном изменении инфраструктуры, процессов и продуктов в компании моделирование угроз должно быть непрерывным процессом. Нужен годичный цикл, в рамках которого будет проходить актуализация состояния конкретных систем или процессов.

В ряде крупных компаний оценка рисков происходит ежеквартально: группа стейкхолдеров берет предыдущую модель угроз и пересматривает ее, выявляет, что изменилось. Главное, чтобы это выполнялось не раз в несколько лет: при современной динамике за это время изменится как бизнес, так и ландшафт угроз.

Отмечу, что оценка рисков должна быть регулярной, но заниматься только ею нельзя. Для отдела ИБ это лишь одна из задач, поэтому надо найти приемлемый баланс: сколько времени и ресурсов вы готовы на нее тратить.

— Как найти тот же баланс между противоречивыми требованиями к киберзащите: и чтобы затраты на нее были низкими, и чтобы она обеспечивала высокую защищенность, функционировала прозрачно для пользователей, быстро и легко развертывалась?

— С помощью карты рисков. Она позволяет получить полную картину. Вы можете четко видеть угрозы, ущерб от них, а в сформированном плане мероприятий прописано, как снизить их до приемлемого уровня и сколько на это нужно будет потратить.

Другими словами, мы видим, какие риски генерируют реальный ущерб и во сколько обойдутся меры по их снижению. Карта рисков позволяет увидеть «дорогую» в плане ущерба угрозу с условно «дешевыми» мерами по ее нивелированию.

В целом нужно прокачать систему безопасности до определенного best-practice — базового уровня защищенности, а затем переходить к пентестам или формированию у себя Red/Blue Team. Когда вы всё реализовали по стандартам, достигли baseline, выполнили обязательную программу, тогда уже можно приглашать экспертов, которые помогут определить, где еще остались узкие места. И здесь нужны пентесты. Они покажут, над чем еще нужно работать. И это непрерывный, практически бесконечный процесс, поскольку совершенствоваться можно довольно долго. Если же система безопасности не выстроена, изначально дырявая, то пентесты бессмысленны: они за ваши деньги покажут то, что вы и так уже знаете, — кучу брешей и неработающие процессы.

— Что, по вашему мнению, первостепенно: высокий уровень защищенности или удобство сервисов для пользователей?

— У нас все еще наблюдается неклиентоориентированность ИБ, когда во главу угла ставится безопасность, а не удобство

пользователя. Это неправильно. Если компания зарабатывает деньги на предоставлении сервиса клиенту, а он уходит, то такая ИБ никому не нужна, потому что организация разорится. Безопасник обязательно должен думать об удобстве использования. Другой вопрос, что, как правило, это упирается в оптимизацию процессов. И здесь стоит работать над развитием компетенций ИБ-специалистов по этому направлению — BPM или Lean. В результате вы увидите, где слишком закручены гайки, на чем компания теряет ресурсы, что можно улучшить.

Наше общество сейчас — общество ленивых людей, которые привыкли к удобству сервисов. Естественно, в эту сторону развивается и информационная безопасность: инструменты становятся более удобными.

— Как это выражается в случае системы управления рисками?

— В идеальном мире решение, которое используется для оценки рисков, должно автоматически поддерживать ее пересмотр и актуализацию. Например, в нашей системе информация обо всех активах, инцидентах и уязвимостях обновляется в режиме онлайн. Мы идем к тому, чтобы при инвентаризации, добавлении данных о новом средстве защиты риски пересчитывались автоматически. Не во время кампании по актуализации угроз через год, а сразу.

При моделировании рисков в нашем решении настраиваются связи: например, отсутствие инцидентов определенного типа, связанного с конкретными угрозами, означает, что они неактуальны. Наличие от 1 до 3 инцидентов — угроза среднего уровня, более 5 инцидентов — высокого. При появлении инцидента система автоматически пересчитывает статус угрозы.

В результате, если открыть карту рисков, она будет актуальной: с учетом всех средств защиты, инцидентов и уязвимостей на текущий момент.

— Какой софт используется для оценки рисков?

Первый вариант — Excel. Это дешево, и его используют в 90% проектов по оценке рисков, даже представители «большой четверки». Обычно Excel применяется в сочетании с макросами и выглядит практически как интерфейс специальной программы. Но у такого подхода есть свои недостатки. На большом количестве данных система начинает тормозить, а чтобы отредактировать макрос, нужно найти его автора, что не всегда возможно. Зачастую вообще не получается разобраться, как именно Excel работает с макросом. Кроме того, в большинстве случаев у таких решений нет нормальной инструкции и методологии.

Второй вариант — GRC-системы — дорогой инструментарий для крупных компаний с высоким уровнем зрелости. Это конструкторы, с помощью которых можно создать собственный космос, свою систему, но это займет несколько лет и потребует много ресурсов. К тому же

ЛПР НУЖНО ПОКАЗЫВАТЬ КОНКРЕТНЫЕ КЕЙСЫ: ОБЪЯСНЯТЬ, ЧТО ЕСТЬ РИСК, КОТОРЫЙ СТОИТ 10 МЛН РУБ. В ГОД, МЫ МОЖЕМ СНИЗИТЬ ЕГО ДО 2 МЛН, НО ДЛЯ ЭТОГО НУЖНО ПОТРАТИТЬ 3 МЛН НА СРЕДСТВА ЗАЩИТЫ. ЭКОНОМИЯ – 5 МЛН РУБ. КОГДА К БИЗНЕСУ ПРИХОДЯТ С ФАКТУРОЙ: КОНКРЕТНЫМИ ЦИФРАМИ, АНАЛИЗОМ РЫНКА И КЕЙСОВ В КОМПАНИИ, – ЕМУ ГОРАЗДО ЛЕГЧЕ ПРИНЯТЬ РЕШЕНИЕ О ВЫДЕЛЕНИИ БЮДЖЕТА.

специалистов в этой области мало и стоят они дорого. Найти такого человека намного сложнее, чем того, кто напишет макрос. Из-за этого GRC не нашли широкого применения на рынке.

Также для оценки рисков ИБ можно использовать инструментарий Security GRC *(SGRC)*. Это не настолько масштабный конструктор, как полноценная GRC, — он дешевле и проще.

— Сколько времени занимает развертывание подобных решений?

Здесь работает принцип 80/20: 20% проекта идут быстро, потом нужно долго и тщательно работать. Волшебной таблетки, ускоряющей процесс, к сожалению, не существует. Наши решения тоже развертываются быстро, но затем начинается кропотливая работа по приведению системы в идеальное состояние.

Если уровень зрелости компании не очень высок, вы не сможете быстро выстроить правильную киберзащиту. Нужно сформировать стратегию развития направления хотя бы на 3 года и постепенно, год за годом, ее реализовывать. При этом важно минимизировать текучесть кадров — она может стать реальным стоппером проекта.

О КАДРАХ

— Какие средства защиты актуальны сегодня?

Сами по себе средства защиты не могут обеспечить кибербезопасность. Она строится на связке из технологий, людей и процессов. Помимо самой системы, нужны квалифицированные кадры, которые ее внедрят, будут использовать и поддерживать, нужен воспроизводимый, непрерывный и правильно

ПРАВИЛЬНО ПОСТРОЕННАЯ МАТРИЦА РИСКОВ, ГДЕ ОЦЕНЕНА СУММАРНАЯ СТОИМОСТЬ КАЖДОЙ МЕРЫ (ВКЛЮЧАЯ ВНЕДРЕНИЕ, ПОДДЕРЖКУ И ОРГАНИЗАЦИОННЫЕ СОСТАВЛЯЮЩИЕ), ПОЗВОЛЯЕТ ВЫБРАТЬ ТЕ ВАРИАНТЫ ЗАЩИТЫ, КОТОРЫЕ ДЕЙСТВИТЕЛЬНО АКТУАЛЬНЫ И ПРИНЕСУТ БОЛЬШЕ ПОЛЬЗЫ.

МНОГИЕ С УДОВОЛЬСТВИЕМ ПОТРАТЯТ 10 МЛН РУБ. НА НОВУЮ СИСТЕМУ, НО НЕ ВЫДЕЛЯТ И 100 ТЫС., ЧТОБЫ НАУЧИТЬ ЛЮДЕЙ С НЕЙ РАБОТАТЬ. В РЕЗУЛЬТАТЕ КОМПАНИЯ БУДЕТ ИСПОЛЬЗОВАТЬ ВСЕГО 20% ПОТЕНЦИАЛА НОВОГО РЕШЕНИЯ, ПОТОМУ ЧТО ИНЖЕНЕРЫ ПРОСТО НЕ УМЕЮТ ИМ ПОЛЬЗОВАТЬСЯ. ЭТО СМЕШНО, ВЕДЬ СТОИМОСТЬ ОБУЧЕНИЯ НИЧТОЖНО МАЛА ПО СРАВНЕНИЮ С РАСХОДАМИ НА ИНСТРУМЕНТАРИЙ.

задокументированный процесс. Без любого из этих элементов реальной безопасности в вашей компании не будет.

— Как вы решаете проблему недостатка квалифицированных кадров?

Лучше искать долго и придирчиво, но найти действительно классного специалиста, обладающего необходимым набором hard и soft skills. Как показывает опыт, личностные качества развивать сложнее, чем технические компетенции. Знания можно нарастить, а отношение к работе у человека меняется редко.

Готовых специалистов на рынке мало, к тому же такой сотрудник даже на новом месте будет стараться работать, используя уже знакомые ему подходы, и не факт, что его удастся переучить. Нужно не бояться подтягивать и выращивать экспертов. Это не всегда возможно, особенно если результат нужен «вчера» и человек, выходя на работу, должен сразу его показать. В остальных случаях стоит брать людей «на вырост» и давать им задачи чуть сложнее привычных, чтобы они развивались.

— Насколько важно вкладываться в обучение специалистов?

Будучи CISO, я всегда считал обучение важным. Оно играет огромную роль, когда в компании появляются новые системы или процессы, эффективность которых напрямую зависит от компетенций сотрудников. Некоторые считают, что хороший специалист обучится сам. Возможно, но он потратит существенно больше времени и наверняка что-то упустит. Есть приемы, позволяющие даже при отсутствии HR-бюджета закладывать расходы на обучение в проект, если руководитель в этом заинтересован. При этом узкие технические скиллы легко получить на курсах, а вот тренинги по процессам ИБ или оценке рисков на рынке представлены слабо. Бывает и такое, что желание обучить специалиста есть, а качественного курса нет.

— Как повышать продуктивность сотрудников?

Первая причина потери продуктивности — отсутствие порядка, того, что мы называем инвентаризацией. Когда есть четкое понимание того, что происходит с ИТ-активами компании и кто за них отвечает, любые вопросы решаются быстро. Яркий пример — задача обновления ПО. Ничего сложного в ней нет, но, если инвентаризация не проводится, ответственному сотруднику сначала придется долго разбираться, где что стоит и как используется. Это особенно актуально для больших компаний.

Второе, на чем теряется время сотрудников, — рутинные операции. Не надо бояться их автоматизировать: 5 раз выполнил задачу руками — на 6-й стоит задуматься и написать скрипт. Такие вещи сильно повышают продуктивность и мотивацию. Человек, который полдня занимается рутиной, гораздо менее «заряжен», чем тот, кто тратит на нее 20% времени.

DLP 2.0. КОМПЛЕКСНАЯ ЗАЩИТА АКТИВОВ

АВТОР

Дмитрий Ключников,

руководитель направлений DLP и DevSecOps Центра информационной безопасности компании «Инфосистемы Джет»

ОБЪЕМ СТР.

/ ПОЧЕМУ СИСТЕМЫ DLP НЕДОСТАТОЧНО ДЛЯ ПРЕДОТВРАЩЕНИЯ ПОТЕРЬ КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

/ КАК ВЫСТРОИТЬ ПРОЦЕСС УПРАВЛЕНИЯ ДАННЫМИ

/ КАКИЕ РЕШЕНИЯ ДОЛЖНЫ ВХОДИТЬ В КОМПЛЕКС УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ АКТИВАМИ

ДМИТРИЙ КЛЮЧНИКОВ

Системы DLP *(Data Leak Prevention)* на протяжении многих лет являются лидирующим классом продуктов по защите от утечек конфиденциальных данных в России. Раньше вендоры часто позиционировали их как решение всех проблем, связанных с потерей подобной информации. Такое представление у многих сохраняется и сегодня. Возможно, так и было 10–15 лет назад, когда внедрение DLP являлось, скорее, превентивной мерой, а утечки информации происходили по вполне понятным схемам. Но на сегодняшний день DLP-системы стали настолько популярными, что грамотные злоумышленники, внутренние или внешние, прекрасно осведомлены о возможностях таких решений и знают, что они «видят», а что нет.

Что же делать, когда бизнес потратил деньги на внедрение дорогой системы, но не избавился от утечек по, казалось бы, очевидным каналам? Кроме того, с этой проблемой напрямую связана переживающая сегодня трансформацию тема управления информационными активами, в том числе электронными данными.

УПРАВЛЕНИЕ АКТИВАМИ КАК ПРОЦЕСС

Бесконтрольность информационных активов может оказывать негативное влияние на деловую репутацию компании. Движение данных должно быть предсказуемым, упорядоченным и управляемым как внутри, так и за пределами периметра организации. Только так удастся выстроить защиту критичных данных на базе процесса управления информационными активами, чтобы обеспечить безопасность деловых операций и непрерывность бизнеса.

Как в любом эффективном подходе, в управлении активами первостепенным является процесс. Например, конфиденциальную информацию нужно грамотно проклассифицировать по уровням значимости и консолидировать по «владельцам», прежде чем передать на контроль системе DLP. К тому же в крупных организациях это можно сделать только с применением специализированных технических средств. Так как «Войну и мир» о процессах уместить в статье не удастся, сосредоточимся на контроле жизненного цикла информационных активов именно с точки зрения использования нестандартных каналов для DLP.

Внутри информационных систем данные в рамках жизненного цикла проходят несколько этапов. Они не линейны, но, как правило, включают в себя создание, перемещение, изменение, хранение и уничтожение.

Информация может быть наблюдаемой — например, находиться в виде файлов в хранилище. Или пребывать в неконтролируемом состоянии — в виде пакетов TCP во время передачи по сетям Ethernet или при записи в базу Oracle.

Существуют различные технические средства для отслеживания наблюдаемой информации на указанных выше этапах. Реализовать же в полной мере управление информацией, находящейся в неконтролируемом состоянии, не представляется возможным. Однако отслеживание можно вести в момент перехода информации из наблюдаемой в неконтролируемую или наоборот. Скажем, это можно сделать посредством контроля каналов связи или предсказуемой конечной точки формирования файла *(например, выгрузки из БД)*.

ИНТЕГРАЦИЯ DLP-СИСТЕМЫ С РЕШЕНИЕМ DATA CLASSIFICATION ПОЗВОЛИТ ЭФФЕКТИВНО ОТСЛЕЖИВАТЬ ПЕРЕМЕЩЕНИЕ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ.

КАКИЕ ТЕХНОЛОГИИ ПОМОГУТ В УПРАВЛЕНИИ АКТИВАМИ

Для того чтобы создать гибкую комплексную систему управления активами, необходимо использовать многоуровневый технический стек продуктов, работающих как единая экосистема по выстроенному процессу. Что же может входить в этот стек и как каждое техническое средство способно «усиливать» другие?

DLP. Было бы странно исключать из перечня средство, которое до сих пор часто воспринимается как решение всех проблем, тем более что оно действительно эффективно... в своей парадигме. Основная цель продукта — контроль утечек конфиденциальной информации посредством контентного анализа. Однако в рамках контроля жизненного цикла информационных активов системы данного класса могут и должны использоваться в качестве управляющего сервиса для других решений по управлению активами.

Data Classification. Тут можно выделить два варианта: техническую классификацию файлов, созданных пользователем *(например, путем проставления визуальных и «невидимых» меток на электронных документах)*, и классификацию выгрузок из БД. В первом варианте можно явно помечать, например, колонтитулы офисных файлов или — уже неявно — записывать определенные метаданные, допустим, в NTFS Property. Примитивно? Не торопитесь с выводами, средства могут оказаться куда полезнее. Большинство решений этого класса обладают функцией репортинга и позволяют отслеживать создание файла в момент его сохранения. Может быть создана политика, которая не позволит сохранить файл без его предварительной классификации, при этом в момент установки метки на консоли репорта будет появляться сообщение о создании.

Классификацию выгрузок из БД можно выполнять в пользовательском и автоматическом режимах. В первом случае, при наличии у формата выгрузок Property, с помощью политики можно задать обязательную классификацию файлов. Во втором случае, при выполнении выгрузок по расписанию, можно создать пользователя AD, от имени которого они будут осуществляться. При этом на все файлы будет автоматически ставиться определенная политикой метка.

Это уже больше похоже на «управление активами», но по-прежнему чего-то не хватает. Смотрим дальше.

Система контроля «нетиповых» каналов утечки. Название класса для таких систем еще не придумали, но о них уже часто можно слышать на различных конференциях при упоминании стеганографии. Суть в том, что, поупражнявшись различным образом с межстрочными и межбуквенными интервалами, можно выдавать пользователю не оригинал документа, а его уникальную копию. Соответственно, если произойдет утечка на бумажном носителе или через фото, при наличии переданного документа *(или даже его фрагмента)* можно будет определить, какой пользователь и в какой момент времени допустил утечку.

Системы распознавания голоса. Считается, что голос является абсолютно неконтролируемым каналом. Это не совсем так: существуют рабочие системы, которые

позволяют перевести голосовую информацию с корпоративной АТС в текст. Зачем? Порассуждаем далее.

Каждая из перечисленных технологий отлично справляется со своими задачами. Но любой процесс эффективнее, когда он учитывает все допущения, то есть является комплексным. Как же превратить наш разрозненный стек технологий в комплексную систему управления активами? Интегрировать и/или комбинировать различные продукты для усиления их возможностей. Приведем несколько примеров из реальной жизни.

КЕЙСЫ

Отслеживание системой DLP меток классификатора. DLP способна распознавать классификационные метки. Ее интеграция с решением Data Classification позволит не только повысить точность посредством корректного определения различных уровней важности информационного актива, но и эффективно отслеживать перемещение конфиденциальных документов. Кроме того, DLP может отслеживать корректность проставленной метки по контенту.

Интеграция системы контроля нетиповых каналов утечки в ЭДО. Все подобные системы создавались для интеграции с внедренными в организации решениями. Например, такие продукты можно встроить в существующий ЭДО таким образом, чтобы при каждом получении конечным пользователем конфиденциального документа на экран выводилась его копия. При этом можно будет отследить ее принадлежность конкретному человеку. Помимо технической составляющей, такая интеграция может повысить сознательность пользователей при работе с конфиденциальными данными. Например, оставить на принтере распечатанный финансовый отчет будет опасно, так как при его обнаружении сотрудник экономической безопасности легко определит беспечного пользователя.

Интеграция системы распознавания голоса с DLP. Зачем нужен голос, переведенный в текст? Текстовая информация подгружается в DLP-систему и анализируется по ее правилам. При достаточно точно составленном списке ключевых слов можно отследить, например, разглашение конфиденциальных данных. Так можно перекрыть изначально неконтролируемый системой вербальный канал.

МОЖНО ЛИ ЗАЩИТИТЬСЯ ОТ ВСЕХ НА СВЕТЕ УТЕЧЕК? ДУМАЮ, НЕТ. ЭТО КАК С УГОНОМ АВТОМОБИЛЯ: ЕСЛИ «УГОНЩИК» ДАННЫХ ЗАДАЛСЯ ЦЕЛЬЮ, ОН ЕЕ ДОСТИГНЕТ.

***

МОЖНО ЛИ ТАКИМ ОБРАЗОМ ЗАЩИТИТЬСЯ ОТ ВСЕХ НА СВЕТЕ УТЕЧЕК? ДУМАЮ, НЕТ. ЭТО КАК С УГОНОМ АВТОМОБИЛЯ: ЕСЛИ «УГОНЩИК» ДАННЫХ ЗАДАЛСЯ ЦЕЛЬЮ, ОН ЕЕ ДОСТИГНЕТ. СТОИТ ЛИ ОТКАЗЫВАТЬСЯ ИЗ-ЗА ЭТОГО ОТ ЗАЩИТЫ СВОИХ АКТИВОВ ВОВСЕ? Я БЫ НЕ СОВЕТОВАЛ. ШАНСЫ СОХРАНИТЬ КОНФИДЕНЦИАЛЬНОСТЬ АКТИВОВ НЕИЗМЕРИМО ВЫРАСТУТ ПРИ ИСПОЛЬЗОВАНИИ МЕР И СРЕДСТВ ЗАЩИТЫ, ОСОБЕННО КОМПЛЕКСНЫХ. НА СВОИ АВТОМОБИЛИ Я ВСЕГДА СТАВИЛ СИГНАЛИЗАЦИЮ И «СЕКРЕТКУ». СОВЕТУЮ И ВАМ НЕ ОГРАНИЧИВАТЬСЯ «ЦЕПОЧКОЙ НА КОЛЕСО», ИЛИ DLP, А ЗАДУМАТЬСЯ О ПОСТРОЕНИИ КОМПЛЕКСНОЙ СИСТЕМЫ УПРАВЛЕНИЯ АКТИВАМИ.

ВЫ СМОЖЕТЕ РЕШАТЬ СЕТЕВЫЕ ПРОБЛЕМЫ

ДО ТОГО, КАК ИХ ОБНАРУЖАТ ВАШИ ПОЛЬЗОВАТЕЛИ

ОБЪЕМ СТР.

/ КАКИМ КОМПАНИЯМ НУЖЕН ПРОАКТИВНЫЙ МОНИТОРИНГ СЕТИ

/ ЧЕМ ПРОПРИЕТАРНЫЕ СИСТЕМЫ МОНИТОРИНГА ОТЛИЧАЮТСЯ ОТ РЕШЕНИЙ OPEN SOURCE

/ КАК ВЫБРАТЬ РЕШЕНИЕ

АВТОР
Дмитрий Каросанидзе,
руководитель группы поддержки продаж сетевых решений компании «Инфосистемы Джет»

АВТОР
Иван Костин,
руководитель группы проектирования решений по передаче данных компании «Инфосистемы Джет»

ОТ САМОПИСНЫХ СИСТЕМ МОНИТОРИНГА К ПРОАКТИВНОМУ ПОДХОДУ

Потребность в мониторинге корпоративной сети возникает с момента, когда в ней начинают работать больше одного компьютера. 20 лет назад все обходились пингованием узлов. С его помощью специалисты узнавали о доступности хостов, времени задержки и размерах передаваемых пакетов. Но сети постоянно росли, количество узлов увеличивалось и пингования стало недостаточно для полноценного мониторинга сети.

Задачи ИТ-подразделений в компаниях стали расширяться. Появилась потребность не просто узнать, что узел находится в сети или что он отвечает на запросы, нужно было понимать, через сколько узлов проходит запрос, что влияет на скорость ответа и в каком месте возникают проблемы. Также было необходимо собирать информацию о настройках и маршрутах со всех устройств в сети и предоставлять данные в удобочитаемом графическом виде или в формате дашбордов. ИТ-специалисты начали создавать первые самописные системы мониторинга сетей, которые со временем становились все более сложными и продвинутыми *(многие из этих разработок стали полноценными коммерческими продуктами)*.

Чуть позже на рынке появились продукты open source — например, популярные до сих пор Nagios или Zabbix. Следом подтянулись вендоры с собственными решениями: Juniper, Cisco, Huawei, Extreme Networks и др.

Главный плюс проприетарных продуктов в том, что они закрывают задачу под ключ — это не наборы «Собери сам».

На заметку

Даже если вы узнали о проблеме в сети спустя какое-то время, ретроспективная аналитика позволит найти ее источник. Стандартная система мониторинга не справится с подобной задачей.

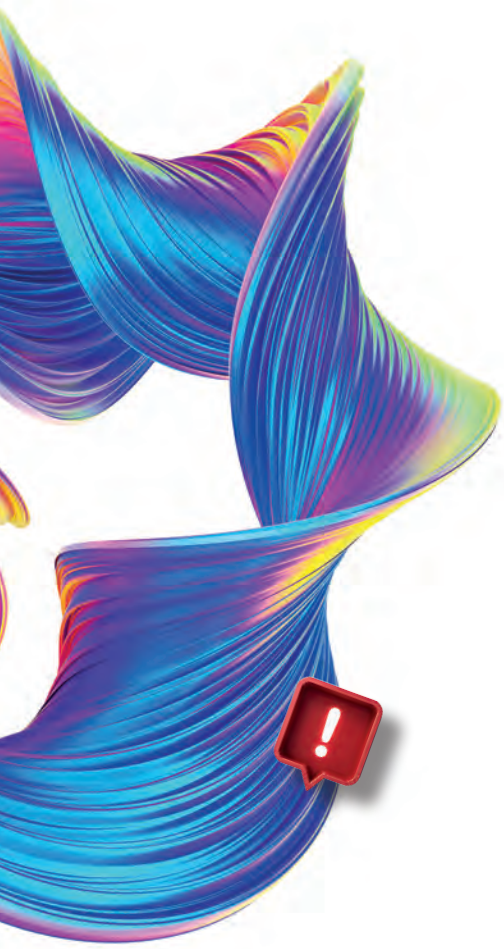
Вам не нужно руками добавлять оборудование, писать конфигурации, править сетевые схемы и настраивать все параметры для отображения, как в случае с решениями open source. Проблема открытого исходного кода — это зачастую отсутствие развития продукта, устаревшие интерфейсы и довольно скромный функционал, а также отсутствие системы резервирования. Проприетарные решения позволяют собирать намного больше информации с устройств и дают возможность не только мониторинга, но и полного управления системой, чего не может обеспечить open source. Но есть и минусы: они прилично стоят, и решение от конкретного производителя полноценно мониторит только его оборудование, а по остальному «железу» дает лишь общее представление. Если в рекламном проспекте написано обратное, это как минимум преувеличение. Да, система может отслеживать работоспособность и собирать минимальный набор конфигураций с чужого «железа», но глубоких настроек и детальной информации о работе сети вы не получите, как и возможности увидеть целостную картину ее состояния.

СЕГОДНЯ СЛЕДИТЬ ЗА СЕТЕВЫМ ОБОРУДОВАНИЕМ УЖЕ НЕДОСТАТОЧНО: ПРОБЛЕМЫ МОГУТ ВОЗНИКАТЬ КАК В КАНАЛАХ СВЯЗИ, ТАК И В СОЕДИНЕНИЯХ МЕЖДУ СЕРВЕРАМИ И БАЗАМИ ДАННЫХ ИЛИ ДАЖЕ УСТРОЙСТВАМИ КОНЕЧНЫХ ПОЛЬЗОВАТЕЛЕЙ.

Сегодня следить за сетевым оборудованием уже недостаточно: проблемы могут возникать как в каналах связи, так и в соединениях между серверами и базами данных или даже устройствами конечных пользователей. Допустим, после внедрения системы виртуальных рабочих столов *(VDI)* пользователи начинают жаловаться на тормозящий интерфейс. Если оборудование и софт в порядке, понять причину поможет система проактивного мониторинга. Она соберет не только информацию по протоколу SNMP, но и данные с коллекторов Netflow, с агентов, установленных у конечных пользователей, метрики пакетов. Затем решение агрегирует все в едином портале *(например, SteelCentral от компании Riverbed)* и покажет, что происходит не только внутри каналов или приложений, но и у пользователей, а также какие приложения или события в сети, на серверах или в ПО привели к появлению задержек. Система предложит варианты решений и в будущем будет заранее сигнализировать о возможных признаках критичных изменений.

В системах проактивного мониторинга есть функционал ретроспективной и предиктивной аналитики, что позволяет находить проблемы до того, как на них пожалуется пользователь. Также с их помощью можно проводить всеобъемлющую аналитику — смотреть, что происходило с сетью, в каком месте появилась проблема, как решались инциденты, какие действия привели к необходимому результату.

В проактивном мониторинге используются технологии искусственного интеллекта и Big Data. К примеру, решение HPE Aruba Mobility Master *(Aruba MM)* собирает информацию о сети Wi-Fi, а затем автоматически настраивает ее так, чтобы каждый пользователь получал максимум скорости. SteelCentral от Riverbed собирает данные от систем коллекторов и позволяет понять зависимости, определить производительность и мгновенно разобраться в каждом инциденте.



ОТРАСЛЕВАЯ СПЕЦИФИКА

Любому enterprise-бизнесу нужно анализировать свою сеть. Недавно мы развернули в крупной промышленной компании уже упомянутое Aruba MM со встроенной технологией Micro DPI и в первый же месяц отловили целую кучу ботнетов. Сейчас предприятия чаще атакуют изнутри, проактивный мониторинг позволяет оперативно анализировать трафик и своевременно закрывать уязвимости.

В России подобными системами в основном пользуются банки. Они уже более пяти лет осваивают эти решения и сейчас находятся на одном уровне с западными компаниями. Следом идут крупные страховые организации, а вот промышленность и ритейл сильно отстают.

Если несколько часов простоя сети не критичны для вашего бизнеса, скорее всего, сейчас вам не нужна система проактивного мониторинга. Например, для офлайнового ритейла временное выпадение нескольких магазинов из сети — не такая уж серьезная проблема. Задержки при торговле офлайн не так заметны: данные о ценах и складских остатках чаще всего передаются раз в день или в несколько дней. Но ситуация кардинально изменится, если

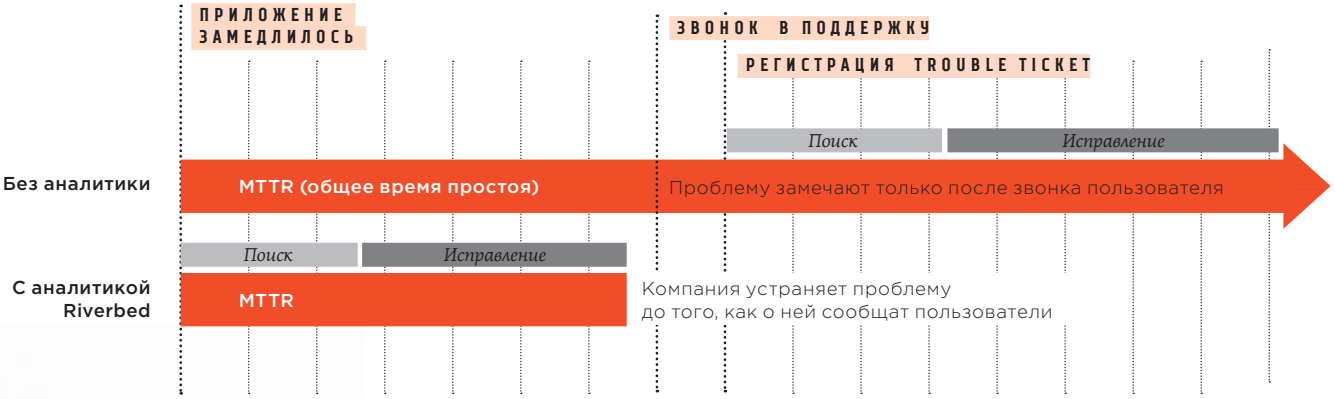
На заметку

Каким компаниям нужны системы проактивного мониторинга (по мере убывания потребности)

1. Банки (топ-50)
2. Страховые компании (топ-30)
3. Аэропорты
4. Транспорт
5. Телеком-операторы
6. Энергетика и нефтегазовый сектор

ЕСЛИ НЕСКОЛЬКО ЧАСОВ ПРОСТОЯ СЕТИ НЕ КРИТИЧНЫ ДЛЯ ВАШЕГО БИЗНЕСА, СКОРЕЕ ВСЕГО, СЕЙЧАС ВАМ НЕ НУЖНА СИСТЕМА ПРОАКТИВНОГО МОНИТОРИНГА.

Рисунок 1. **Обнаружение и устранение проблемы в сети без системы проактивного мониторинга и при ее наличии**



час простоя для них будет стоить столько же, сколько он сегодня стоит для банков. Для последних суммы измеряются в миллионах долларов, причем для топ-10 — в десятках и даже сотнях миллионов.

Без квалифицированных специалистов вы будете использовать только 30–40% возможностей проактивного мониторинга. Поскольку финансовые организации по очевидным причинам не пускают к себе сторонних сетевых инженеров, мы рекомендуем им отправлять сотрудников на соответствующее обучение или привлекать в штат специалистов с опытом внедрения систем мониторинга. Эти вложения однозначно окупаются.

ВЫБОР РЕШЕНИЯ

Если компании нужно просто получать информацию о доступности сетевого оборудования, мы рекомендуем использовать систему мониторинга того вендора, чье «железо» уже установлено. Это может быть система Huawei eSight, Cisco Prime Infrastructure, Extreme Networks Access Control и т.д. При наличии в компании «зоопарка вендоров» *(а это типичная ситуация для многих заказчиков)* самым верным вариантом будет определить превалирующего производителя, установить и настроить его систему мониторинга, а затем подключить к ней оборудование других вендоров. Таким образом вы

КЕЙС #1

ЗАКАЗЧИК

Крупное промышленное предприятие с филиальной структурой

ЗАДАЧА

Мониторинг оборудования сети в масштабах России для решения задач сетевого отдела и отдела информационной безопасности

РЕЗУЛЬТАТ

Создана адаптивная сервисная система ИБ для всей группы компаний. Запущен упреждающий мониторинг сети. Система мониторит более 4000 единиц оборудования в пяти регионах. Количество инцидентов ИБ, отслеживаемых в режиме реального времени, выросло в 10 раз. Работа по внедрению заняла около четырех месяцев.

КЕЙС #2

ЗАКАЗЧИК

Банк из топ-20

ЗАДАЧА

Запустить контроль метрик баз данных SQL, меток приложений, установить их корреляцию с бизнес-процессами в банке. ИТ-служба должна понимать, в какой момент наступает деградация процесса, чтобы принимать оперативные решения. Также нужно было запустить мониторинг мобильных приложений и контроль SLA.

РЕЗУЛЬТАТ

Отслеживается состояние бизнес-процессов на основании меток приложений, определены их узкие места. Сформирован список мер по предотвращению задержек в бизнес-процессах, оптимизирована работа приложений, выделены цели и участки для улучшений.

КЕЙС #3

ЗАКАЗЧИК

Страховая компания из топ-20

ЗАДАЧА

Поиск и устранение лагов в работе системы видео-конференц-связи: картинка постоянно «рассыпалась», а звук значительно отставал от нее. Системой пользовался топ-менеджмент компании, что поднимало приоритет задачи до бизнес-критичной. Стоимость потенциального решения проблемы «в лоб» — апгрейда всей сети — составляла около 900 000 долларов, работа по миграции заняла бы около двух месяцев.

РЕЗУЛЬТАТ

После внедрения системы проактивного мониторинга стало понятно, что проблема сети заключается не в загруженности каналов связи, а в неправильной настройке решения по приоритизации трафика. Также был необходим небольшой апгрейд нескольких узких мест на серверах с виртуальными контроллерами системы видео-конференц-связи. Совокупная стоимость решения составила около 81 000 долларов, ИТ-специалисты компании устранили проблему за 4 дня.

сможете контролировать и мониторить большую часть сети из одного места, а по остальным сегментам будете видеть общую информацию о доступности оборудования и его функционировании. Альтернативным вариантом могут быть решения open source, об их плюсах и минусах мы уже рассказывали раньше.

Для решения сложных задач подойдут продвинутые средства мониторинга: Riverbed, VIAVI или NetScout. Они позволяют проводить предиктивную и ретроспективную аналитику, а также собирать информацию со всех сегментов сети, включая приложения и инженерную инфраструктуру.

Продвинутые средства мониторинга также будут полезны, если за ИТ-инфраструктуру отвечают несколько подразделений. Когда в таких компаниях возникает проблема, чаще всего начинается пинг-понг: «Это у вас не работает! Нет, у вас!» Мониторинг поможет этого избежать: вы сможете точно определить, на чьей стороне инцидент, и разобраться с ним раньше, чем его заметят конечные пользователи. Системы типа Riverbed также подойдут для отслеживания состояния сети в региональных или зарубежных филиалах компании.

Продвинутый мониторинг позволяет прогнозировать, как перемены в ИТ-ландшафте скажутся на работоспособности сети. Например, если бизнес решил переехать в новый ЦОД, чтобы срезать косты или внедрить новое ПО, чтобы уменьшить время на тестирование, вы сможете заранее узнать, каких проблем стоит ожидать и как к ним подготовиться.

ТОП-10

ТЕНДЕНЦИЙ ИЗ ОТЧЕТА «HI-TECH CRIME TRENDS 2019/2020» GROUP-IB

ОБЪЕМ СТР.

GROUP-IB

КОНФЛИКТ МЕЖДУ ГОСУДАРСТВАМИ ПРИОБРЕЛ НОВЫЕ ФОРМЫ, И КИБЕРАКТИВНОСТЬ ИГРАЕТ ВЕДУЩУЮ РОЛЬ В ЭТОМ ПРОТИВОСТОЯНИИ. 2019 Г. СТАЛ ГОДОМ ОТКРЫТЫХ ВОЕННЫХ КИБЕРОПЕРАЦИЙ. ФОКУС ИССЛЕДОВАТЕЛЕЙ ВО ВСЕМ МИРЕ ПОСТЕПЕННО СМЕЩАЕТСЯ С ФИНАНСОВО МОТИВИРОВАННЫХ ХАКЕРСКИХ ГРУПП, ЗАРАБАТЫВАЮЩИХ ДЕНЬГИ ПУТЕМ ВЗЛОМА РАЗЛИЧНЫХ ОРГАНИЗАЦИЙ, В СТОРОНУ ПРОГОСУДАРСТВЕННЫХ АТАКУЮЩИХ. ПЕРЕХОД ОТ ОБОРОНИТЕЛЬНОЙ ПОЗИЦИИ К ОХОТЕ ЗА КИБЕРПРЕСТУПНИКАМИ – МАГИСТРАЛЬНЫЙ ТРЕНД РЫНКА ИБ. НУЖНО АБСТРАГИРОВАТЬСЯ ОТ ВРЕДОНОСНЫХ ПРОГРАММ И СОСРЕДОТОЧИТЬСЯ НА ИЗУЧЕНИИ ТОГО, КАК РАБОТАЮТ КИБЕРПРЕСТУПНИКИ И ХАКЕРСКИЕ ГРУППЫ. И В ЭТОМ НАМ ПОМОЖЕТ СВЕЖИЙ ОТЧЕТ НАШЕЙ КОМПАНИИ «HI-TECH CRIME TRENDS 2019/2020».

Дмитрий Волков,
сооснователь и технический директор
Group-IB

1 HUNT OR BE HUNTED

Предотвращение кибератак — одна из самых сложных задач для ИБ-специалистов. Основная магистральная тенденция в сфере информационной безопасности была сформулирована нами как «Hunt or be hunted» — охотиться, или охотиться будут за тобой. Ее идея в том, что продукты и технологии, используемые для обеспечения кибербезопасности, должны помогать в борьбе с киберпреступностью, а не в пассивной защите от нее. Вы должны заранее знать об актуальных угрозах и готовящихся атаках. Вашим аналитикам нужно иметь инструменты, позволяющие отследить связи *(например, сетевой граф)*, проанализировать подозрительную активность и выявить ранее неизвестные угрозы и инструменты. Новое исследование Group-IB «Hi-Tech Crime Trends» служит источником стратегических и тактических данных об актуальных киберугрозах в мире за период H2 2018 — H1 2019.

2 ОТКРЫТЫЕ ВОЕННЫЕ ОПЕРАЦИИ С ИСПОЛЬЗОВАНИЕМ КИБЕРОРУЖИЯ

Атаки на критическую инфраструктуру и целенаправленная дестабилизация сети Интернет в отдельных странах открывают новую эпоху проведения кибератак. Мы уверены в том, что мирное существование больше невозможно в отрыве от кибербезопасности.

За первые 6 месяцев 2019 г. стало известно о трех открытых военных операциях. В марте в результате атаки на ГЭС Венесуэлы большая часть страны осталась

Рисунок 1. Группы, атакующие энергетический сектор

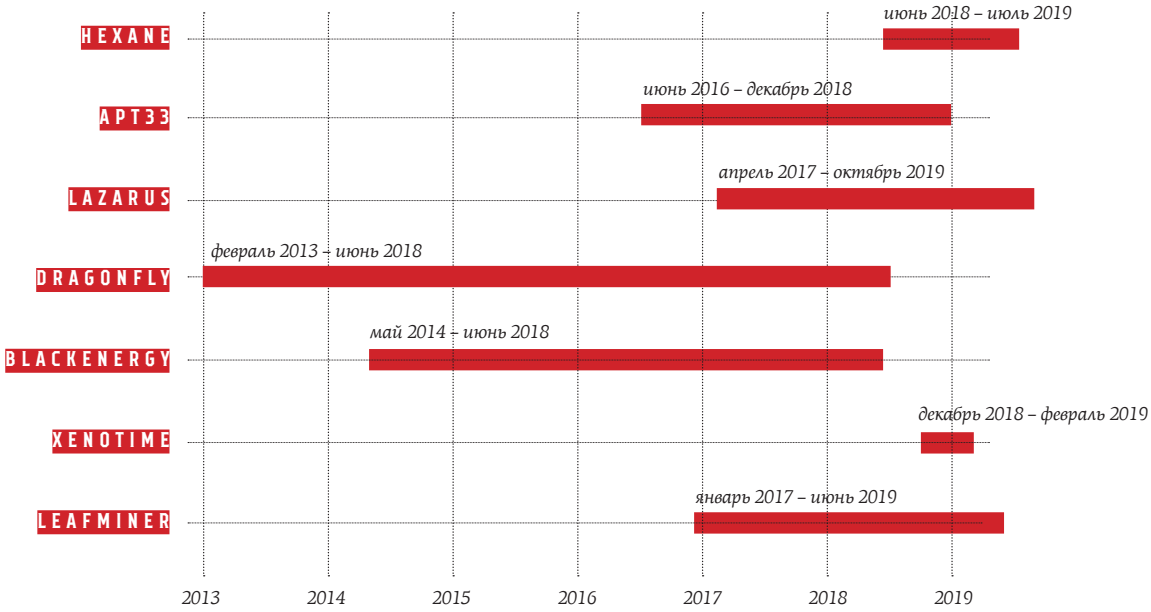


Рисунок 2. Группы, атакующие телекоммуникационный сектор

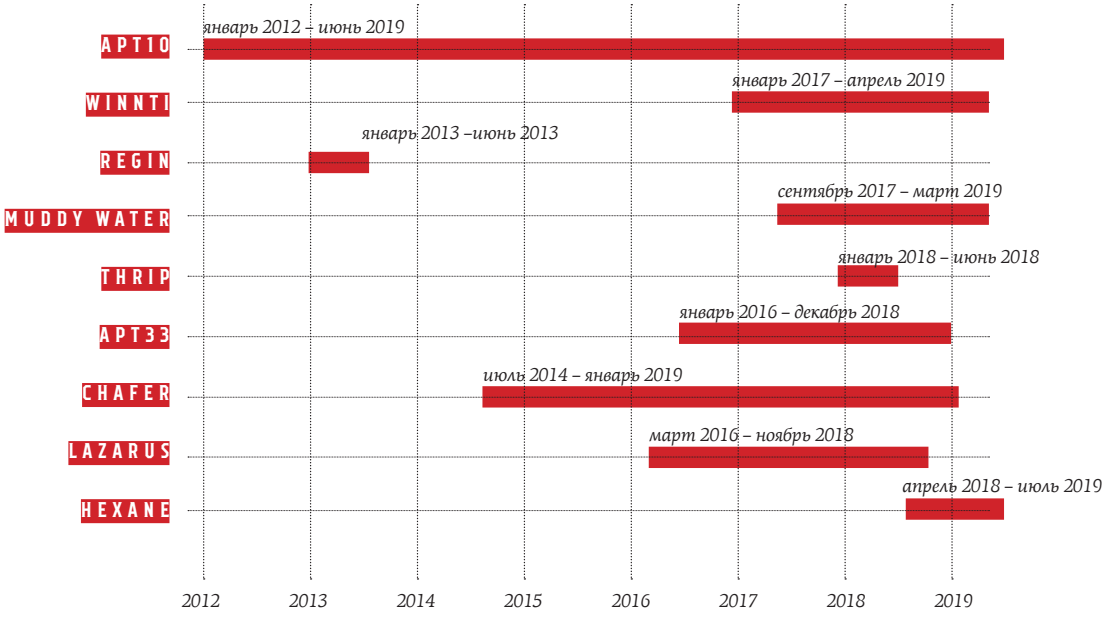


Рисунок 3. **География атак проправительственных группировок**

1

АТАКИ НА АМЕРИКУ

Россия: APT28, Turla, APT29, Xenotime

Пакистан: Gorgon Group

Иран: APT33, Charming Kitten

Северная Корея: Kimsuky, Lazarus, STOLEN PENCIL

Китай: APT40

Южная Америка: APT-C-36*

2

АТАКИ НА ЕВРОПУ

Россия: APT28, Turla, Gamaredon Group, APT29

Пакистан: Gorgon Group

Иран: APT33, MuddyWater

Северная Корея: DarkHotel, Lazarus

Китай: APT40, LEAD, APT10

Вьетнам: OceanLotus

Неизвестно: PowerPool, Inception, Gallmaker*

3

АТАКИ НА АЗИАТСКО-ТИХООКЕАНСКИЙ РЕГИОН

Северная Корея: APT37, Kimsuky, Lazarus, DarkHotel

Индия: Sidewinder, BITTER

Иран: Chafer, OilRig

Китай: APT10, Winnti, APT40

Россия: APT29, Turla, Xenotime

Вьетнам: OceanLotus

Неизвестно: APT-C-35 , BlueMushroom*, Whitefly*, неизвестная группа, TajMahal framework

4

АТАКИ НА БЛИЖНИЙ ВОСТОК И АФРИКУ

Ближний Восток: Bahamut, APT-C-27, HEXANE*

Турция: StrongPity

Газа: Gaza Cybergang

ОАЭ: FruityArmor

Иран: OilRig, MuddyWater, APT 33, Domestic Kitten, Chafer

Северная Корея: APT37, Lazarus

Китай: Emissary Panda

Неизвестно: APT-C-38, Windshift*, Gallmaker*

5

АТАКИ НА РОССИЮ И СНГ

Ближний Восток: HEXANE*

США: Equation Group

Пакистан: Gorgon Group

Иран: MuddyWater

Северная Корея: APT37, Lazarus

Россия: Gamaredon Group, Buthtrap, APT28

Китай: Winnti

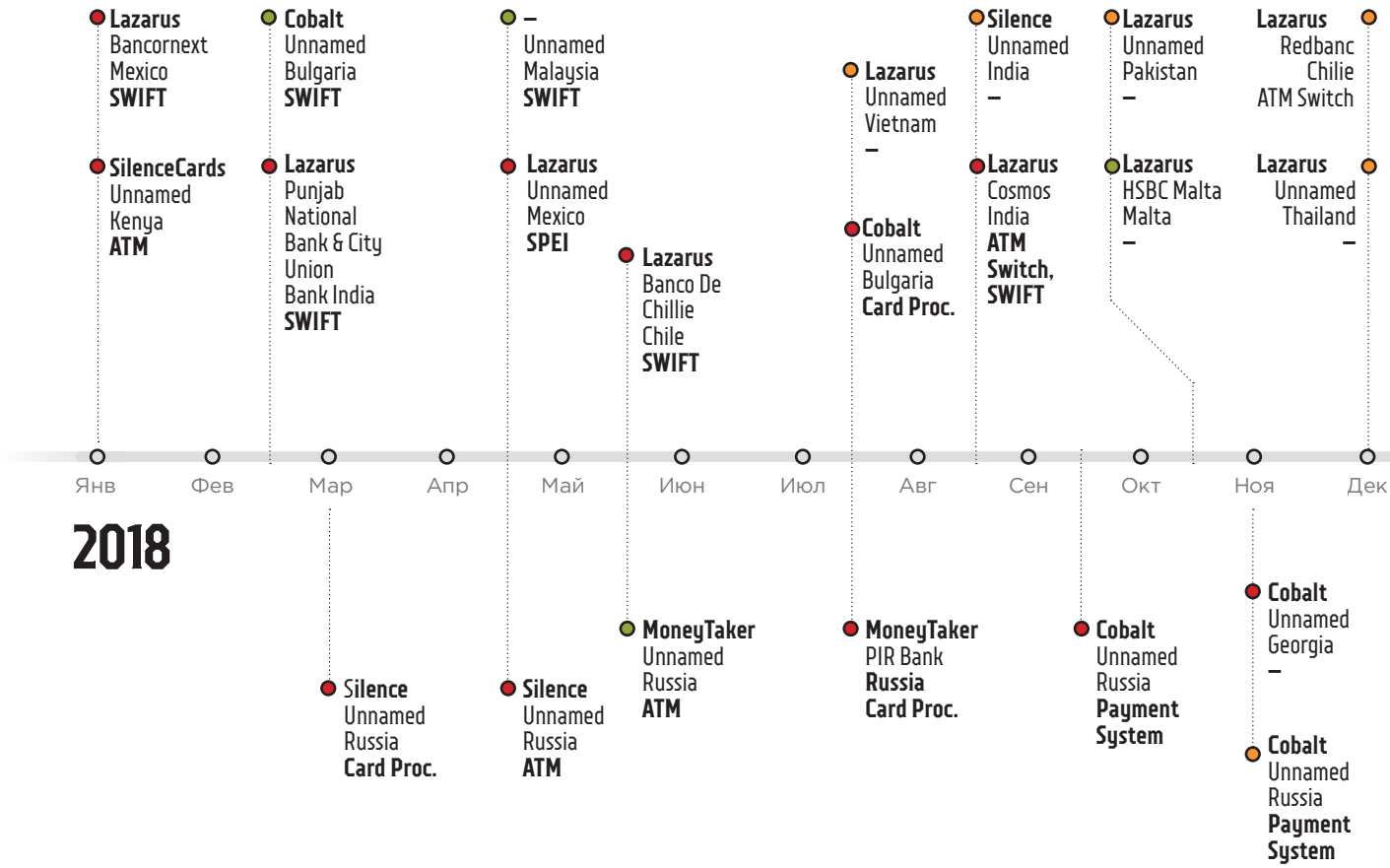
Неизвестно: PowerPool, Whitefly*

* Новые группы.

без электричества на несколько дней. В мае в ответ на кибератаку армия Израиля произвела ракетный удар по штабу хакеров группировки ХАМАС. В июне США использовали кибероружие против иранских систем контроля за запуском ракет в ответ на сбитый американский беспилотник.

Инструменты атакующих не установлены, при этом в последнем случае кибератака произошла всего через несколько дней после инцидента с беспилотником. Это подтверждает предположение о том, что критические инфраструктуры многих стран уже скомпрометированы и атакующие просто остаются незамеченными до нужного момента.

Рисунок 4. Целенаправленные атаки на банки



3 НАРУШЕНИЕ СТАБИЛЬНОСТИ ИНТЕРНЕТА НА ГОСУДАРСТВЕННОМ УРОВНЕ

Сегодня максимальный социальный и экономический ущерб может быть нанесен путем отключения людей и бизнеса от связи. При этом страны, выстраивающие централизованный контроль доступа в интернет, более уязвимы и могут стать первой мишенью. За последние годы были опробованы атаки на разные уровни инфраструктуры коммуникаций: на маршрутизацию сети Интернет и BGP hijacking; регистраторов доменных имен; администраторов корневых DNS-серверов, национальных доменов и DNS hijacking; локальные системы фильтрации и блокировки трафика.

4 СКРЫТЫЕ УГРОЗЫ СО СТОРОНЫ ПРОПРАВИТЕЛЬСТВЕННЫХ ГРУППИРОВОК

Хотя за последний период был опубликован ряд исследований о новых пропра-вительственных группировках, эта сфера остается малоизученной. Была замечена активность 38 групп *(7 — новые по сравнению с отчетом 2018 г., их целью является шпионаж)*. Однако это не означает, что другие известные группы прекратили свою деятельность — скорее всего, их кампании просто остались ниже радаров аналитиков.

К примеру, в сфере энергетики известно лишь два фреймворка — Industroyer и Triton *(Trisis)*, и оба были найдены в результате ошибки их операторов. Вероятно, существу-

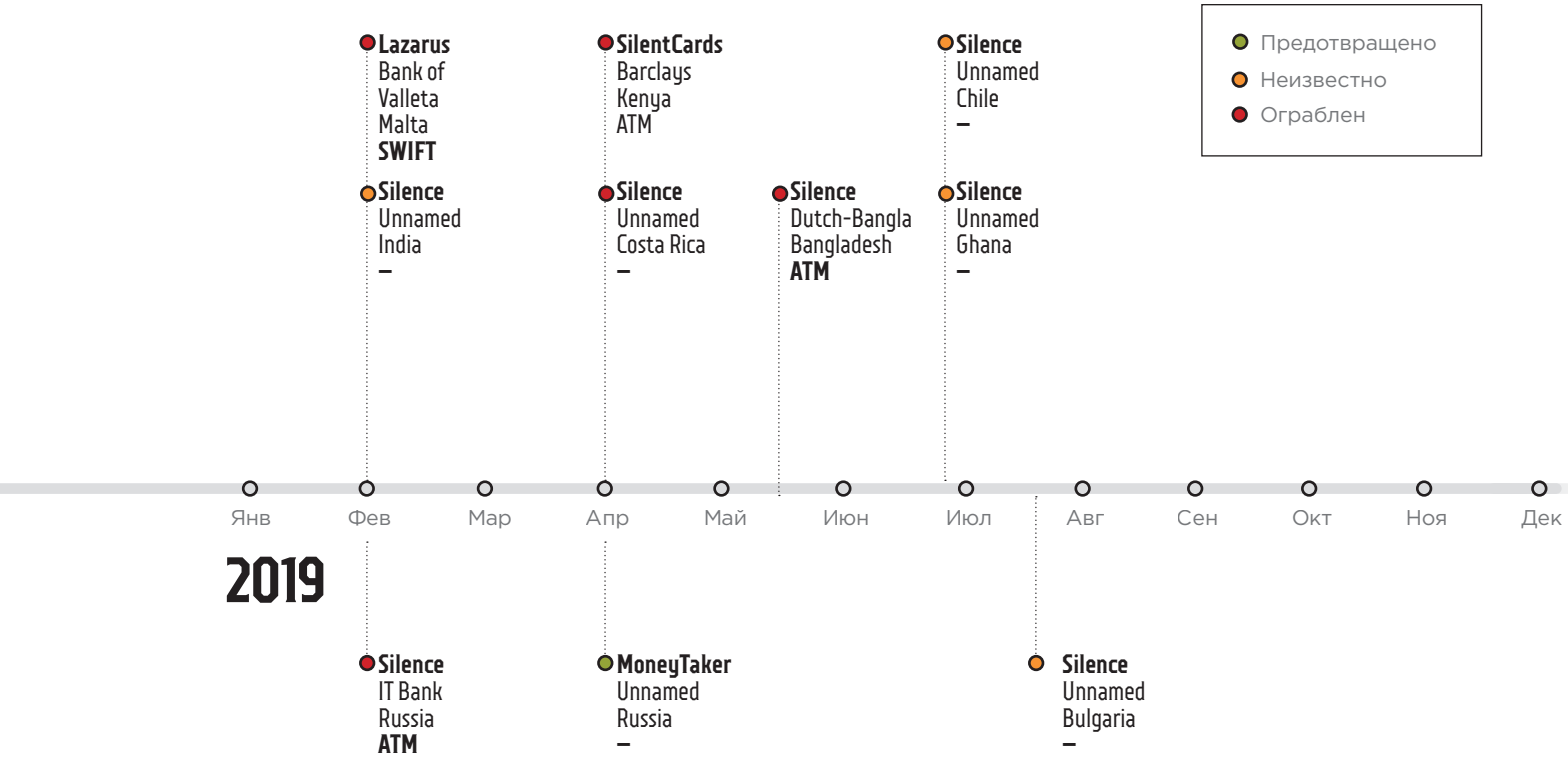
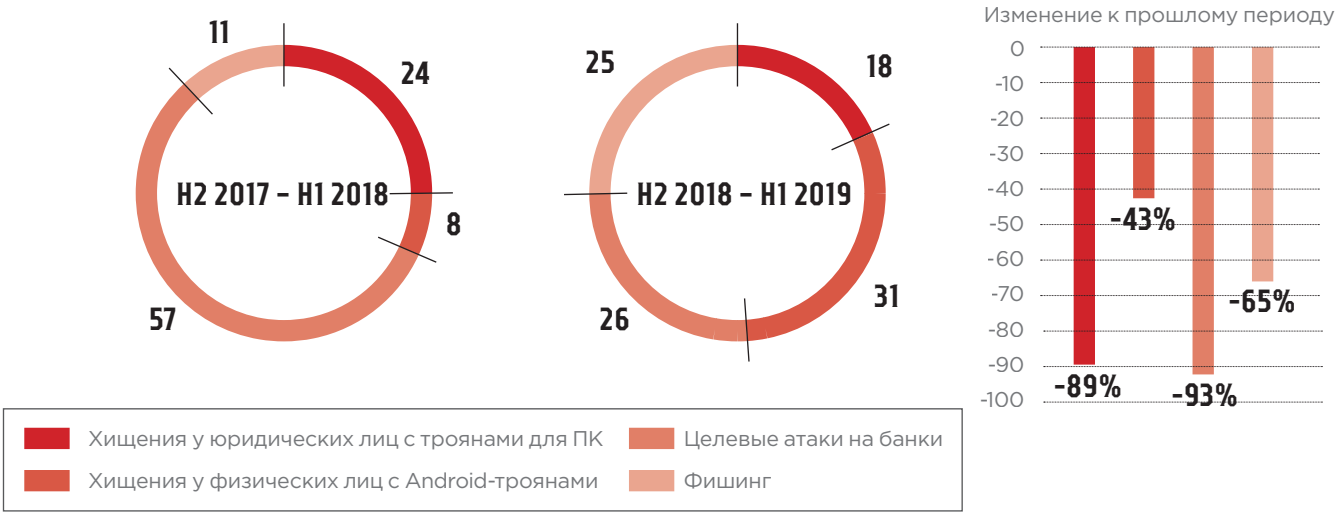


Рисунок 5. **Оценка Group-IB рынка высокотехнологичных преступлений в финансовой отрасли России**

Сегмент рынка в России	Кол-во групп	Общее число успешных атак	Средняя сумма одного хищения (руб.)	Средняя сумма хищения в день (руб.)*	H2 2018 – H1 2019 (руб.)
Хищения у юридических лиц с троянами для ПК	2	0,5	500 000	250 000	62 250 000
Хищения у физических лиц с Android-троянами	5	40	11 000	440 000	109 560 000
Целевые атаки на банки	3	-	31 000 000	-	93 000 000
Фишинг	11	435	800	348 000	86 652 000
Обналичивание похищаемых средств	-	-	-	467 100	158 157 900
Итого				**1 038 000**	**509 619 900 ₽**

* Учтены только рабочие дни.

Рисунок 6. Оценка Group-IB рынка высокотехнологичных преступлений в финансовой отрасли России



ет значительное количество подобных, еще не обнаруженных угроз, и это бомба замедленного действия.

5 ОБРАТНЫЙ ВЗЛОМ: ПРОТИВОСТОЯНИЕ ПРОПРАВИТЕЛЬСТВЕННЫХ ГРУППИРОВОК

В 2019 г. участились случаи появления в открытом доступе информации об инструментах атакующих от имени якобы хактивистов или бывших участников группировки. Чаще всего это примеры обратного взлома, когда злоумышленники сами становятся жертвами. В настоящее время частные компании не имеют права проводить подобные операции, и такие полномочия официально есть только у специальных государственных служб.

6 ЦЕЛЕНАПРАВЛЕННЫЕ АТАКИ НА ИНОСТРАННЫЕ БАНКИ СО СТОРОНЫ РУССКОЯЗЫЧНЫХ ГРУПП

Всего 5 групп сейчас представляют реальную угрозу финансовому сектору: Cobalt, Silence, MoneyTaker *(Россия)*, Lazarus *(Северная Корея)*, SilentCards (новая группа из Кении). В России ущерб от APT-атак на банки со стороны финансово мотивированных группировок за исследуемый период сократился почти в 14 раз. Это связано в том числе с переключением фокуса на иностранные банки.

7 ПОСТЕПЕННОЕ ИСЧЕЗНОВЕНИЕ ТРОЯНОВ ДЛЯ ПК И ANDROID

Тенденция исчезновения троянов для ПК продолжается: в России — на родине этого типа вредоносных программ — их перестали писать. Единственной страной, активно создающей трояны, является Бразилия, но их использование носит локальный характер. Только Trickbot значительно эволюционировал за последний год и теперь может использоваться как для целенаправленных атак на банки, так и для шпионажа, как это было с трояном Zeus.

Трояны для Android исчезают медленнее, чем для ПК, однако количество новых в разы меньше вышедших из употребления. Новые программы эволюционируют от перехвата SMS к автоматическому переводу средств через банковские мобильные приложения — автозаливу. Количество активных троянов продолжит снижаться за счет внедрения средств защиты и резкого сокращения экономической выгоды для атакующих.

8 ЭВОЛЮЦИЯ СПОСОБОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ БЕЗ ИСПОЛЬЗОВАНИЯ ВРЕДОНОСНОГО КОДА

Злоумышленники продолжают использовать поддельные аккаунты в соцсетях, совершают звонки с надежных номеров по хорошо продуманным скриптам, покупают базы паспортных данных и т.д. К относительно новым методам социальной инженерии можно отнести управление телефоном с помощью программ удаленного доступа, которые жертвы устанавливают на свои устройства под руководством мошенников.

9 РОСТ РЫНКА КАРДИНГА ЗА СЧЕТ JS-СНИФФЕРОВ

При падении финансовой отдачи от использования банковских троянов злоумышленники стали применять более эффективный способ заработка — JS-снифферы. Уже сейчас их число превышает количество троянов, а общее количество скомпрометированных с их помощью карт выросло на 38% по сравнению с отчетом 2018 г. JS-снифферы станут наиболее динамично развивающейся угрозой, особенно для стран, где не распространена система 3D Secure.

10 НОВЫЕ АТАКИ НА СТРАХОВЫЕ, КОНСАЛТИНГОВЫЕ И СТРОИТЕЛЬНЫЕ КОМПАНИИ

В 2019 г. мы зафиксировали атаки новой группы, получившей имя RedCurl. Ее основные цели — шпионаж и финансовая выгода. После выгрузки значимой документации злоумышленники устанавливают майнеры в инфраструктуру скомпрометированной компании.

Особенность этой группы — очень высокое качество фишинговых атак. Для каждой компании злоумышленники создают отдельное письмо. RedCurl использует уникальный самописный троян, осуществляющий коммуникацию с управляющим сервером через легитимные сервисы. Это сильно затрудняет обнаружение вредоносной активности в инфраструктуре.

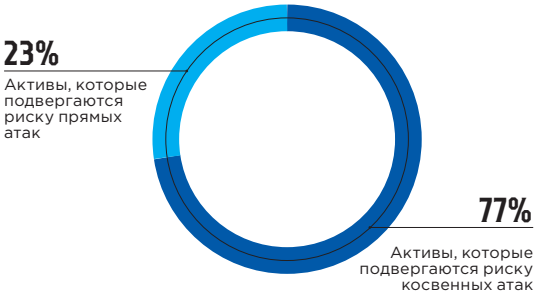
Полный отчет
«Hi-Tech Crime Trends 2019/2020»
доступен по ссылке.

https://www.group-ib.ru/resources/threat-research/2019-report.html

ИСТИННЫЙ МАСШТАБ УЩЕРБА ОТ КИБЕРПРЕСТУПНОСТИ

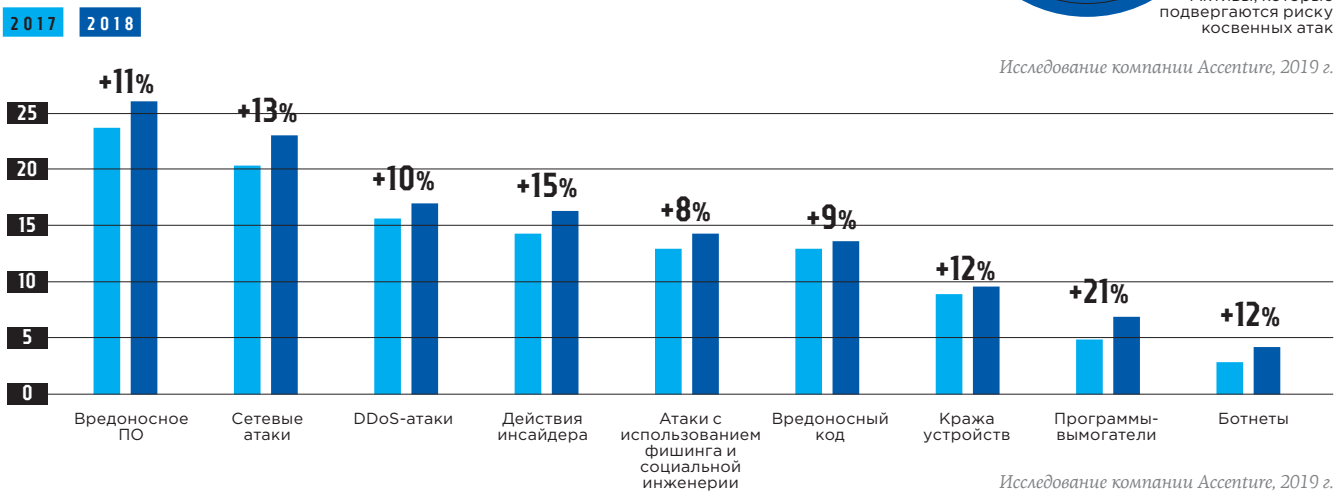
ПОСЛЕДСТВИЯ КИБЕРПРЕСТУПЛЕНИЙ МОГУТ ОТРИЦАТЕЛЬНО СКАЗАТЬСЯ НА РЕПУТАЦИИ КОМПАНИИ, УМЕНЬШИТЬ КЛИЕНТСКУЮ БАЗУ, ПОВЛИЯТЬ НА ВОЗМОЖНОСТИ ФУНКЦИОНИРОВАНИЯ. НО НИЧТО НЕ МОЖЕТ БОЛЕЕ ТОЧНО И ЯСНО ОЦЕНИТЬ УЩЕРБ ОТ ПЛОХОЙ КИБЕРБЕЗОПАСНОСТИ, НЕЖЕЛИ ПОТЕРИ КОМПАНИИ, ВЫРАЖЕННЫЕ В ДЕНЬГАХ.

Общая величина активов, которые подвергаются риску от прямых и косвенных кибератак, кумулятивно за 2019–2023 гг.



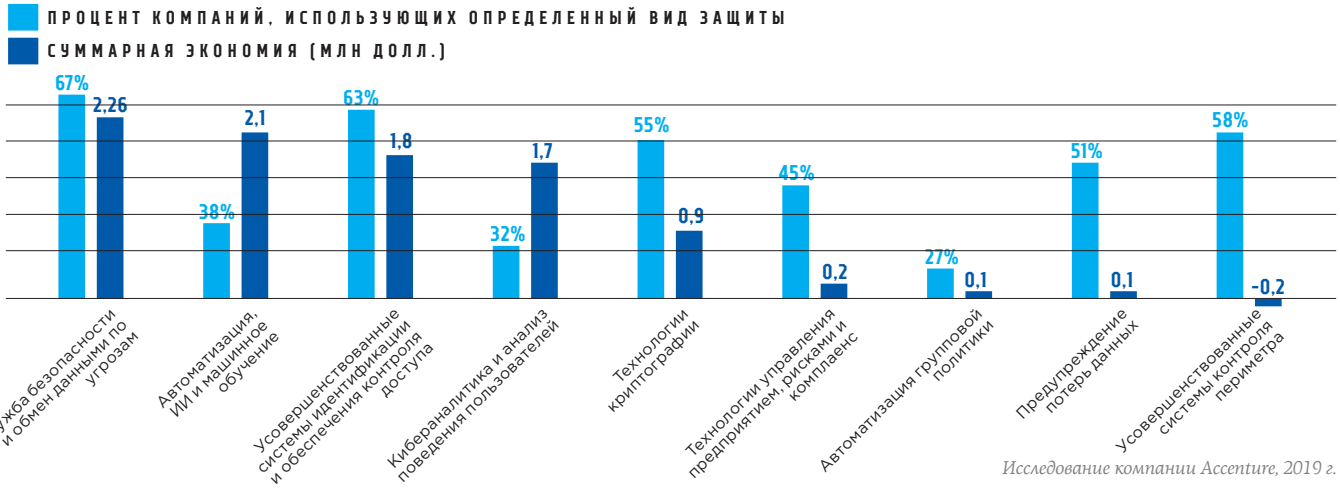
Исследование компании Accenture, 2019 г.

Среднегодовой ущерб от киберпреступности по видам атак (млн долл.)



Исследование компании Accenture, 2019 г.

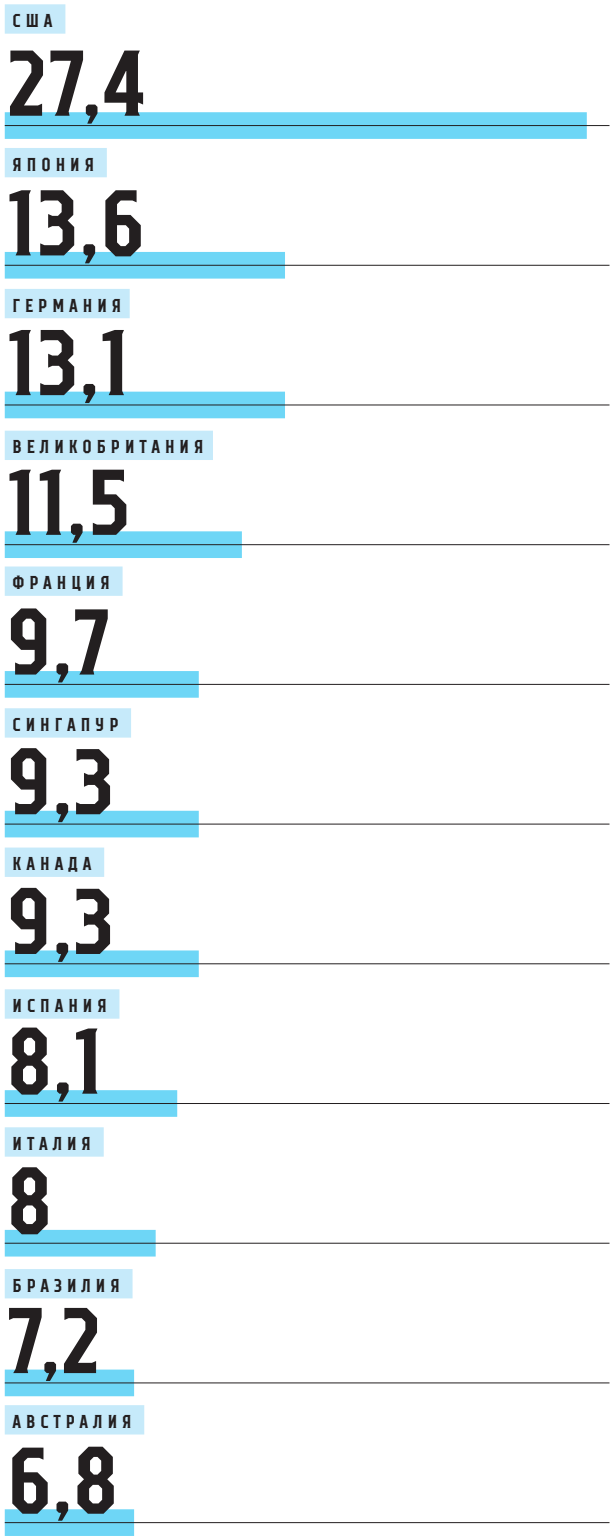
Сколько денег помогут сэкономить компаниям технологии кибербезопасности



Исследование компании Accenture, 2019 г.

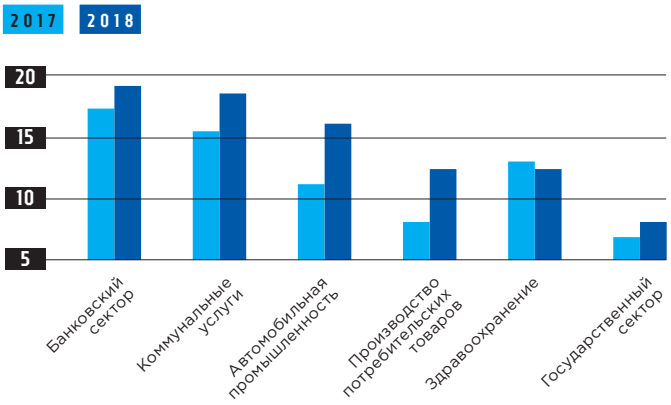
Ущерб от киберпреступлений по всему миру

Среднегодовой ущерб от кибератак *(млн долл.)*



Совместное исследование Института Понемона и компании Accenture, 2019 г.

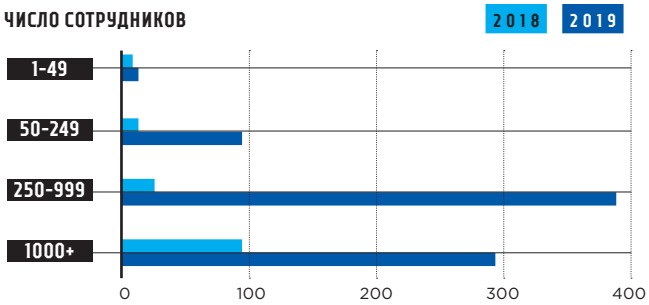
Среднегодовой ущерб от киберпреступности по отраслям (млн долл.)



Исследование компании Accenture, 2019 г.

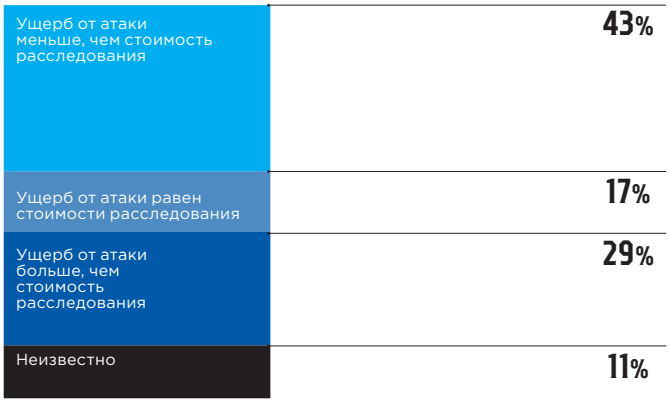
Ущерб от одной крупнейшей кибератаки для европейских и американских компаний (тыс. долл.)

Средний ущерб в зависимости от размера компании



Исследование компании Hiscox, 2019 г.

Время, потраченное на расследование атаки, может стоить больше, чем ущерб от нее



Исследование PwC, 2018 г.

РОССИЙСКИЙ РЫНОК IdM-РЕШЕНИЙ 2014–2018 ГГ.

Исследование компании «Инфосистемы Джет»

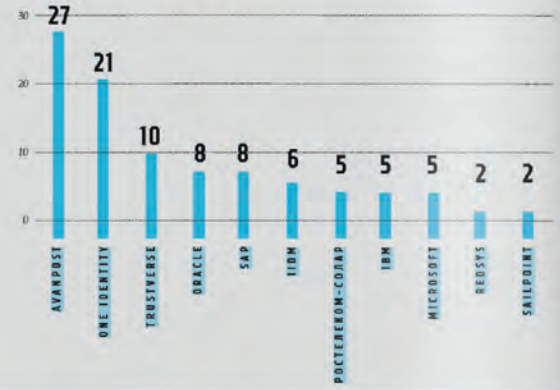
Читайте на стр. 46

СТАТИСТИКА ВНЕДРЕНИЙ

В связи с тем, что проекты по внедрению IdM длительные и масштабные, у нас не было возможности получить данные о качестве реализации и степени завершенности проектов, поэтому при оценке количества внедрений IdM-решений мы учитывали только старт проекта и факт поставки лицензий (см. рис. 1).

Три отечественных вендора (*IIDM, Ростелеком-Солар* и *Redsys*) вышли на рынок IdM в 2015 г. За несколько лет им удалось сравняться с игроками, внедряющими эти решения в России с 2000 гг.

Рисунок 1 Количество внедрений IdM-решений отечественных и зарубежных вендоров в России, 2014–2018 гг.



Н.

Хотелось бы увидеть в исследовании финансовые показатели. Количество проектов, безусловно, главный признак востребованности продукта. Но когда у одной компании 5 проектов по 1 млн руб. каждый, а у другой 1 проект на 20 млн, это также важно для конкурентной оценки. Было бы полезно, если бы отчет включал данные об объеме и потенциале рынка в деньгах.

Наш ответ: «Задачей исследования было расширить спектр критериев выбора IdM-решения и осветить картину российского рынка. Это второе наше исследование, до этого статистика по российскому рынку отсутствовала. При выборе решения заказчики обращаются к отчетам Gartner и Forrester, но известно, что они занимаются аналитикой только зарубежного рынка и не учитывают отечественных вендоров. Мы планируем продолжать выпускать наш отчет, и, возможно, в следующий раз мы попробуем учесть финансовые показатели для более ясной картины».

ОТРАСЛЕВАЯ СЕГМЕНТАЦИЯ

Мы проанализировали изменение востребованности IdM-решений в разных отраслях за несколько периодов (см. рис. 2).

Компании финансового и государственного секторов лидируют по количеству внедрений IdM. Принципиальное различие между ними в том, что пик интереса финансовых компаний к IdM-решениям приходится на период с 2009 по 2013 г., а сейчас наблюдается небольшой спад. В то же время у организаций государственного сектора повышается интерес к IdM-проектам.

Рисунок 2 Отраслевая сегментация рынка IdM, %

Таблица 2. Отраслевая сегментация рынка IdM в разные периоды, в %

Сектор	2004–2008	2009–2013	2014–2018
Финансы	17,65	38,78	30,30
Нефть и газ	29,41	24,49	12,12
Государственный сектор	5,88	16,33	17,17
Другие	47,06	20,41	40,40

ПОБЕДЫ JETINFO НА КОНКУРСАХ КОРПОРАТИВНЫХ МЕДИА

АКМР

x 14

2020

- Клиентские медиа: журнал
- Отраслевые медиа: журнал
- Лучшее медиа в сфере технологий/ телекоммуникаций
- Лучшее корпоративное издание для акционеров и инвесторов
- Лучший дизайн-макет B2B
- Лучшая обложка
- Лучшая фотография
- Лучшая иллюстрация (инфографика)

2019

- Лучшее отраслевое медиа: журнал
- Лучший дизайн-макет
- Лучшая обложка
- Лучшая иллюстрация/ инфографика

2018

- Лучшее корпоративное издание для акционеров и инвесторов
- Лучший дизайн-макет B2B

Серебряные нити

x 6

2019

- Лучший корпоративный журнал
- Лучшая инфографика
- Лучшее интервью

2018

- Лучший корпоративный журнал B2B
- Самая креативная рубрика в корпоративных медиа
- Самое оригинальное решение тематической вкладки

Медиа лидер

x 2

2019

- Лучший дизайн-макет корпоративного СМИ

2018

- Лучший журнал для клиентов

COMNEWS ICT CORPORATE MEDIA AWARDS

x 1

2014

- Лучшее клиентское издание