Исследование

Информационная безопасность в финансовом секторе

QRATOR LABS

валарм

Сентябрь-октябрь, 2017
Москва

Содержание

3 Понимание рисков
7 Угрозы
10 Используемые решения
12 Выводы

Компания Qrator Labs совместно с Валарм на протяжении последних семи лет защищает ведущие российские банки и платежные системы от DDoS-атак и взломов

Мы хорошо знаем, с какими проблемами безопасности сталкиваются наши клиенты, и эффективно решаем их, используя самые передовые технологии, существующие на текущий момент. В то же время мы нередко видим субъективные и объективные факторы, препятствующие внедрению этих технологий. Для нас жизненно важно непрерывно поддерживать диалог со своими клиентами, соответствовать их требованиям и инициативно предлагать методы решения вопросов, которые, мы, как эксперты, считаем наиболее актуальными сегодня, а также в ближайшей и долгосрочной перспективе. Для достижения этих целей мы второй год проводим аналитическое исследование финансовой отрасли (российские банки и платежные системы) по теме проблематики, масштаба и динамики угроз DDoS-атак и взломов. В данном отчете мы также приводим оценку респондентов по уровню защищенности их организаций и эффективности использования тех или иных технологий защиты.

Сравнение оценок респондентов с нашим экспертным мнением, а также с аналогичными результатами прошлого года позволяет сделать выводы о векторе и динамике развития кибербезопасности в банковской сфере, об основных факторах, влияющих на этот процесс, а также о возможных проблемах отрасли, с которыми компании сталкиваются или могут столкнуться в будущем.

Методика исследования

Работы в рамках настоящего исследования проводились в формате полевого опроса.

Респондентам предлагалось ответить на вопросы анкеты. Опрос был организован среди банков и платежных систем, работающих в России. В выборку включены банки из рейтинга ТОП 200 по размеру активов.

Выборка из 200 банков представляет наиболее активную группу заказчиков решений ИБ, располагающих значительными бюджетами (на ИТ в целом и на средства защиты информации в том числе). Данная группа респондентов представляет ТОП 200 российских банков по размеру активов (из 537 кредитных организаций, зарегистрирован-ных Банком России и располагающих действующей лицензией на август-сентябрь 2017 г.) и является репрезентативной для задач настоящего исследования.

В опросе участвовали руководители ИТ-подразделений, их заместители, а также руководители департаментов, отвечающих за вопросы информационной безопасности.

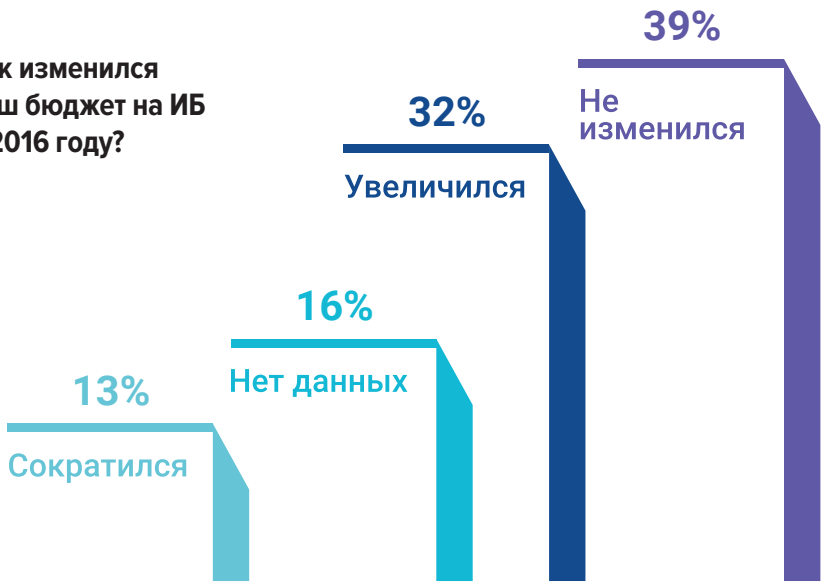
3 Бюджет на ИБ
4 Осознание рисков
5 Замена используемых средств защиты
6 Приобретение решения WAF

Понимание рисков

Бюджет на ИБ

Отрасль информационной безопасности закономерно продолжает расти. По данным проведенного опроса, более трети (32%) респондентов из финансовой отрасли подтвердили увеличение своего ИБ-бюджета в 2016 г., а еще 39% отметили сохранение инвестиций в безопасность в прежнем объёме.

— Как изменился ваш бюджет на ИБ в 2016 году?



Напомним, что по итогам аналогичного опроса 2015 года увеличивали расходы на ИБ около трети респондентов, и еще 44% сохраняли их в прежнем объеме.

Заметно, что рост ИБ-бюджетов становится напрямую связанным с практической составляющей: финансовые организации планируют увеличение расходов на безопасность, оказавшись перед лицом реальной угрозы. Это примечательно по двум причинам: в то время как формальное соответствие требованиям регуляторов перестаёт быть основным драйвером роста, тем не менее, проактивная тактика защиты и планирование ИБ-архитектуры на основе, по крайней мере, тестирования на проникновение (или пентеста) всё ещё таким драйвером не является. 13% респондентов сообщили, что бюджет на ИБ в их организациях в 2016 г. несколько снизился.

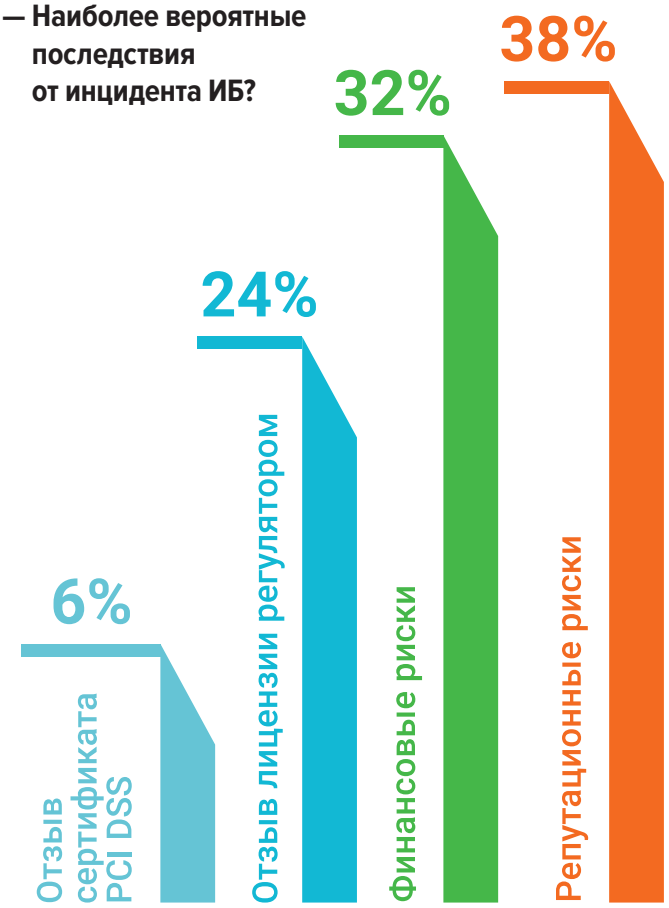
При этом опрошенные в целом отмечают отсутствие связи между снижением бюджета и реальным уровнем угроз – причины снижения ИБ-бюджетов в основном лежат в иной плоскости и не зависят от состояния и вызовов дисциплины ИБ. По сути, перед заметной частью департаментов ИБ в 2016 году была поставлена задача оптимизации расходов при сохранении и даже повышении требуемого уровня защищенности от внешних неблагоприятных условий, хотя в целом по индустрии тенденция к росту бюджетов на данный момент сохраняется.

Осознание рисков

Более половины опрошенных отмечают в числе наиболее существенных последствий от инцидентов ИБ финансовые и репутационные издержки. Повышение риска отзыва лицензии фиксируют около четверти респондентов (годом ранее — более 60%).

Важно, что специалисты по банковской безопасности начинают всё более приоритезировать защиту бизнеса и репутации, а не только соответствие требованиям регулятора. Однако здесь необходимо также учитывать, что, кроме репутационных потерь, дополнительными рисками могут быть слухи о потенциально возможном отзыве лицензии, когда возникшие проблемы

— Наиболее вероятные последствия от инцидента ИБ?



> Индустрия постепенно приходит к пониманию того, что, выполняя «до буквы» требования регуляторов, лицензиаров и сертификационных организаций, пройти большинство проверок можно, а вот построить по-настоящему безопасную систему нельзя. Начинать следует именно с выстраивания эффективных процессов ИБ, а вопросы лицензирования и сертификации должны быть вторичны. Если два года назад многие рассматривали отзыв лицензии как основной риск, то сейчас становится понятно, что он является лишь побочным относительно большинства других проблем.
>
> **— Александр Лямин**
> **Генеральный директор**
> **Qrator Labs**

с информационной безопасностью банка привлекают внимание регулятора. Если слухи одновременно сопрягаются с инцидентами ИБ, то репутационные угрозы растут чрезвычайно интенсивно, начинается отток клиентов, как частных, так и корпоративных и государственных, страдает кредитный рейтинг. Ситуация нарастает, как снежный ком: страдает репутация, ухудшается образ компании в глазах общественности и регулятора, что в свою очередь влияет на доверие и может повлечь за собой отзыв лицензии. Исправить такую ситуацию быстро не получится, так как проблемы ИБ обычно означают отсутствие грамотно выстроенных процессов, а процессы оперативно внедрить практически невозможно. Это объясняет то, почему инциденты ИБ зачастую имеют достаточно длинный шлейф последствий.

Замена используемых средств защиты

Методы защиты, внедряемые ранее, сегодня обеспечивают недостаточный уровень безопасности: выросли угрозы по уже существующим направлениям, появились и новые риски.

В подавляющем большинстве случаев основной стимул для обновления инфраструктуры ИБ — это внешняя активность: инциденты, связанные с демонстрацией недостаточной защиты и проблемами, которые организованы либо «черными шляпами» — взломщиками, либо «белыми» — тестировщиками. Также более четверти респондентов видят для себя необходимость в замене используемых средств защиты при переходе на новые инфраструктурные решения (облака, микросервисы и пр.), где используемые ранее продукты перестают быть эффективными.

— Назовите причины замены используемых средств защиты

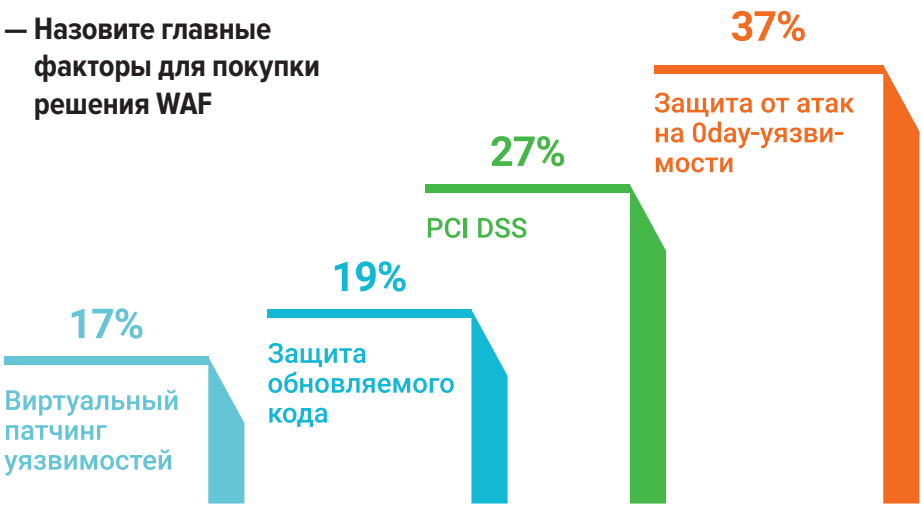
Заметную роль при принятии решения об обновлении используемых средств защиты играет вопрос происхождения закупаемых продуктов: около 13% респондентов ответили, что в первую очередь склонны заменять импортные решения на российские аналоги.

Приобретение решения WAF

В качестве основного фактора для покупки решения WAF респонденты отметили защиту от уязвимостей 0 дня – 37%. Такой возможностью обладают только решения нового поколения, использующие бессигнатурный подход для детектирования атак. По-прежнему значительная часть компаний использует WAF для соответствия стандарту PCI DSS – 27%. По мнению экспертов Валарм, использование коробочного решения без предварительной настройки и обучения персонала не может гарантировать корректную защиту веб-приложений и соответствие стандарту.

36% респондентов используют WAF для обеспечения высокого темпа разработки: 19% – для защиты часто обновляемого кода и 17% – для использования виртуального патчинга уязвимостей. Увеличение числа компаний, применяющих решения по обеспечению безопасности на этапе написания кода, говорит об общем росте осведомленности о стандартных практиках информационной безопасности и формировании качественного подхода к обеспечению комплексной защиты веб-приложений.

— Назовите главные факторы для покупки решения WAF



7 Уровень угроз в 2016
7 DDoS-атаки
8 Инциденты ИБ в 2016 году

Типы угроз

Уровень угроз в 2016 году

По-прежнему DDoS-атаки на организации финансового сектора устраиваются чаще, чем на компании из других отраслей, например, ритейл, СМИ. Однако теперь важно не только то, что злоумышленники обладают всей полнотой знаний, где именно хранятся интересующие их средства, но также они понимают, с помощью каких методов эти деньги можно получить. Запустив DDoS-атаку в качестве отвлекающего фактора, злоумышленники с помощью вредоносных программ могут произвести захват системы управления безналичными платежами и, таким образом, получают возможность переводить деньги между любыми счетами до момента своего обнаружения.

Отсюда следует, что системы защиты, применяемые в финансовых организациях, несовершенны, и подходы к развитию ИТ-инфраструктуры требуют пересмотра и обновления.

55%

Доля отметивших рост уровня угроз DDoS

— Оцените изменение уровня угроз DDoS в финансовом секторе, 2016

DDoS-атаки

Угроза атак на отказ в обслуживании продолжает расти: почти половина опрошенных испытывала по крайней мере одну DDoS-атаку в 2016 году.

Столкнувшись с наличием мер по защите от атак, злоумышленники обычно переключают своё внимание на иные цели. В том числе, вероятно, ввиду этого целый ряд компаний в финансовой сфере столкнулся с DDoS-атаками в 2016 году впервые. При этом, однако, около 20% компаний находятся в фокусе злоумышленников и вынуждены применять продвинутые методы защиты. Среди основных причин, ведущих к попаданию финансовой организации в фокус организаторов DDoS-атак, можно назвать как размеры организации и её популярность на рынке, так и отсутствие внедрённых адекватных контрмер для борьбы с DDoS-атаками, вследствие чего организация может стать лёгкой добычей для кибервымогателей.

Таким образом, по мере широкого внедрения различных решений для борьбы с DDoS-атаками ландшафт рынка может меняться.

В частности, ожидаемое усложнение «пробных» атак продолжит приводить к эволюции средств защиты и к росту угрозы для организаций и предпринимателей, не планирующих адекватные вызовам инвестиции в ИБ.

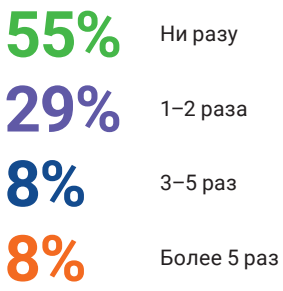
Инциденты ИБ в 2016 году

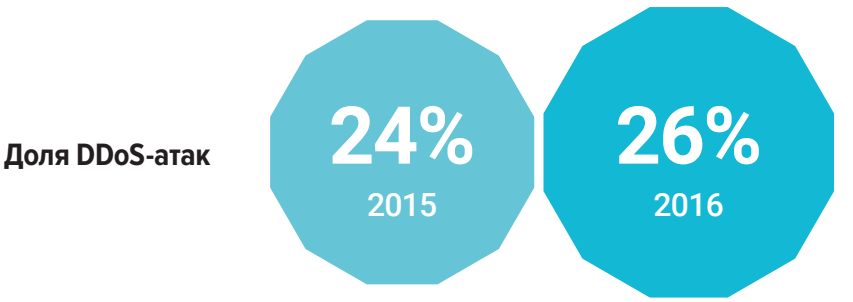
Наиболее часто опрошенные компании из финансового сектора сталкиваются с фишингом (30%) и DDoS-атаками (26%). По сравнению с результатами опроса 2015 года, угроза DDoS-атак осталась примерно такой же (24% в 2015 году). Сохранение числа DDoS-атак и внимания к ним со стороны банковского сектора на достаточно высоком уровне обусловлено волной массированных DDoS-атак на ряд крупных российских банков: в 2016 году были атакованы веб-сайты многих известных финансовых организаций из топ-10.

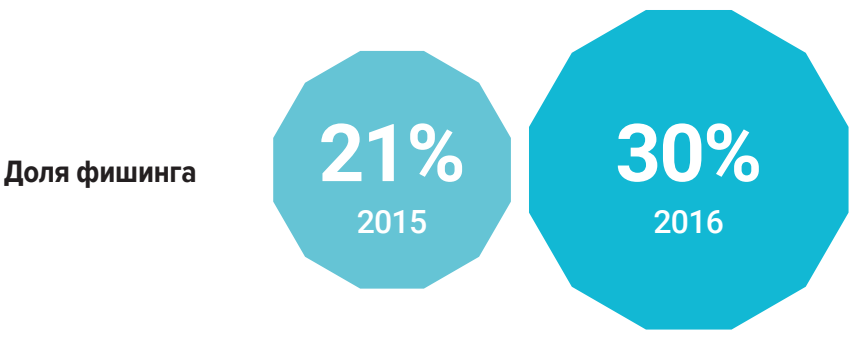
Угроза фишинга существенно выросла (с 21% в 2015 году до 30% в 2016-м) в связи с компаниями, выходящими на ICO. Неутихающий ажиотаж вокруг ICO привел к высокому риску мошенничества, и среднестатистические пользователи не имеют точного представления, как обеспечить собственную защиту и склонны не замечать интернет-мошенничество. В сфере ICO фишинг стал серьезной проблемой, и это позволяет судить о том, что и в смежных отраслях, например, в финансовом секторе, фокус злоумышленников также смещается в сторону такого метода получения доступа к конфиденциальным данным пользователей.

Смещение фокуса в сторону фишинга – одно из следствий развития инструментов, доступных киберпреступникам. В частности, несмотря на то, что число взломов в единицу времени в целом

— Как часто вы сталкивались с DDoS-атаками в 2016 году?







за последние годы сохраняется на одном уровне, на данный момент финансовые организации уже не всегда могут своевременно обнаруживать и точно фиксировать подобные инциденты.

Среднее количество атак на веб-приложения в финансовой сфере, по данным Валарм, составляет 1500 в день. Основная часть из них – это автоматизированные инструменты и сканеры. Такая активность автоматизированных средств создает большой информационный фон и усложняет выявление реальных инцидентов. По статистике Валарм, основные векторы атак на веб-приложения - это внедрение SQLi операторов — 27% и межсайтовая подделка запросов (XSS) — 26%. Повышенный интерес к этим типам атак связан с возможностью получения информации о базах данных клиентов и персональной информации пользователей. Третье и четвертое место занимают выход за пределы значений директории — 25% и удаленное выполнение кода — 19%. При этом основная часть инцидентов — 60% — связана с удалённым выполнением кода.

Атаки на веб- приложения

Типы используемых решений

Большинство респондентов (68%) считают самым эффективным средством противодействия DDoS гибридные решения (на стороне клиента с участием операторского решения, либо распределенной сети). Однако, по мнению экспертов Qrator, у этого метода существует ряд нюансов, которые необходимо учитывать.

> Гибридные решения не компенсируют недостатки друг друга, а комбинируют преимущества и отрицатель-ные свойства в определенных пропорциях, что может негативно сказаться на уровне защиты. В индустрии еще не сложилось четкое понимание подобных рисков: многие до сих пор полагаются на гибридные решения. Однако с ростом угроз можно ожидать, что в дальнейшем рынок отнесется к этой ситуации более серьезно, осознав, что комбинированные системы не могут обеспечить защиту от целых классов атак
>
> **— Александр Лямин**
> **Генеральный директор Qrator Labs**

Наиболее эффективные решения для защиты от DDoS-атак по мнению опрошенных

Показательно также, что никто из опрошенных не считает в настоящий момент эффективными решения CPE. Это означает, что с точки зрения эффективности решения на стороне клиента окончательно устарели, и это признают ведущие компании банковской отрасли.

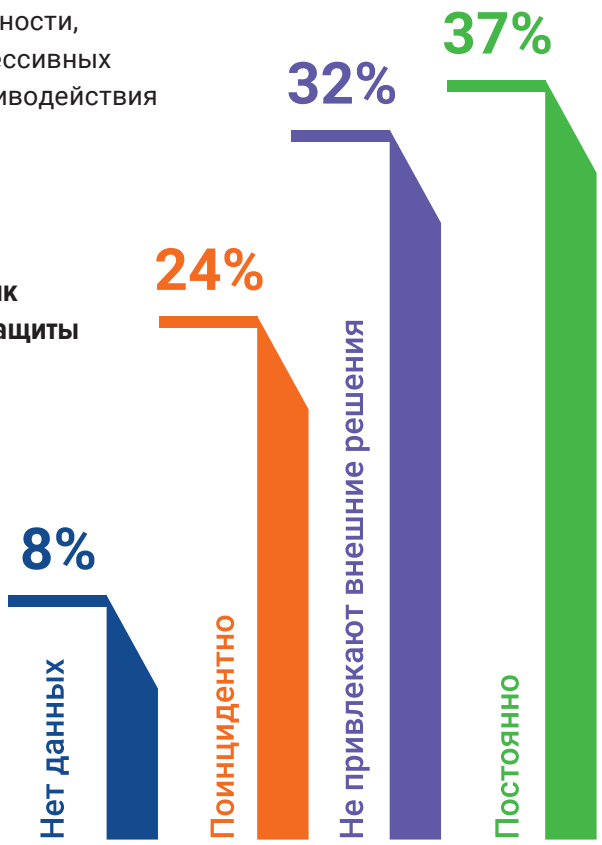
Передача трафика внешнему поставщику услуг

Почти 2/3 опрошенных заявляют, что пропускают трафик через внешнее решение постоянно или поинцидентно. За прошедший год процент банков, использующих сторонние решения для защиты от атак, вырос кардинально — почти в 2 раза.

«В отрасли сформировалось понимание, что с атаками, число которых экспоненциально растет, собственными средствами справиться сложно. Как мы видим, на данный момент доля респондентов, пропускающих трафик через внешнее решение, примерно совпадает с числом тех, кто считает, что уровень угроз за последний год вырос, и с теми, кто реально сталкивался с атаками. Отсюда можно заключить, что не привлекают внешние решения лишь те, кого подобные проблемы пока не коснулись», — комментирует Александр Лямин, генеральный директор Qrator Labs.

Существенную роль в изменении подходов к защите ИТ-инфраструктуры организаций банковской отрасли сыграли рекомендации Центрального банка РФ, который «развернул» банковскую безопасность от формального соответствия требованиям регуляторов в сторону защиты бизнеса и разъяснил необходимость переосмысления политик безопасности, качественной оценки рисков и применения прогрессивных георасспределенных удаленных решений для противодействия DDoS-атакам.

— Как часто вы пропускаете трафик через стороннее решение для защиты от атак?



Выводы

1 Как показало исследование, информационная безопасность остается значимым приоритетом для организаций финансового сектора, и этот приоритет неуклонно растет: отрасль находится в стадии пробуждения. Участники рынка пока неокончательно сфокусировались на угрозах ИБ, но в определенной степени уже можно говорить о достижении российскими финансовыми организациями определенного уровня зрелости в вопросах защиты и управления рисками. Переосмысление политик безопасности в банковской отрасли будет продолжать свое развитие, о чем свидетельствует то, что расходы на ИБ не сокращаются, а, наоборот, в основном растут. В ближайшей перспективе с ростом бюджета мы увидим повышения уровня защищенности компаний.

2 В индустрии хорошо понимают репутационные риски инцидентов ИБ. Во многом это происходит благодаря действиям регуляторов: многие финансовые организации начинают более серьезно относиться к угрозам и принимать меры по противодействию сетевым атакам. Подобная тенденция будет развиваться и далее: сегодня уже заходит речь об обязательной сертификации решений ИБ и проведении регулярных аудитов и страховании рисков.

3 Все больше финансовых организаций осознают, что собственных мощностей их оборудования недостаточно для организации полноценной защиты, и начинают привлекать внешние решения. В зависимости от роста и модификации внешних угроз в будущем индустрия будет двигаться в сторону специализированных сервисов. Сегодня акцент уже сместился от применения CPE-решений в сторону комбинирования решений на стороне клиента с другими — облачными и операторскими. Компании начали заменять используемые ими средства ИБ в случае, если уровень защиты, обеспечиваемый этими решениями, оказывается недостаточным, что подтверждается внешними инцидентами или пентестами. Поскольку внедренная пару лет назад CPE-инфраструктура не отвечает современным требованиям, а построение новой дорого и неэффективно, то при сохранении уровня угроз на достаточно высоком уровне мы будем видеть дальнейшую замену CPE и гибридных решений на внешние средства защиты.

Контакты для прессы

info@onsec.ru
press@qrator.net
qrator.net
wallarm.com