



POSITIVE  
TECHNOLOGIES

# Кибербезопасность 2019—2020:

тенденции и прогнозы



2019





POSITIVE  
TECHNOLOGIES

## Содержание

Введение	3
Состояние и драйверы рынка ИБ	4
Рынок ИБ в России вырос, но этого никто не заметил	4
Смена парадигмы: ability to detect уже здесь	4
Технологии vs. люди	4
Регуляторы драйвят	5
Общие тенденции ИБ	7
APT-группировки vs. защитники: соотношение сил	8
Государство и политика	10
Атаки на пользователей	11
Промышленный сектор под угрозой	13
Небезопасный телеком	14
Безопасность финансового сектора	15
Банкоматы и платежные терминалы	16
Аппаратные уязвимости в фокусе исследований	18
Атаки по побочным каналам	18
Аппаратный реверс-инжиниринг в тренде	18
Смена модели угроз	19
Мобильные угрозы	20
Обход биометрии	20
Отсутствие защиты кода	20
Атаки на пользователей	21
Уязвимости в WhatsApp	21
Безопасность операционных систем	22
Заключение	23





POSITIVE  
TECHNOLOGIES

## Введение

В контексте кибербезопасности 2019 год прошел под знаком АРТ-атак, поиска аппаратных уязвимостей и громких утечек. За то время, пока руководители компаний приходили к осознанию необходимости выстраивать действительно эффективную систему информационной безопасности, преступники прочно обосновались в киберпространстве. Наиболее ярким примером стал рынок в дарквебе, где продается масса запрещенных товаров и услуг, в том числе хакерские утилиты и доступ к уже взломанным инфраструктурам. Кроме того, преступники продолжают использовать неграмотность пользователей в вопросах обеспечения собственной безопасности.

Соотношение сил киберпреступников и защитников оказывается не в пользу последних: АРТ-группировки активно используют новейшие уязвимости, действуют очень быстро, а главное — часто меняют инструментарий и тактики. Непосредственная угроза сложных целенаправленных атак побуждает компании по-новому взглянуть на эффективность систем защиты. Настало время пересмотреть старые подходы и поговорить о новом типе информационной безопасности.

Эксперты Positive Technologies подвели киберитоги последних двенадцати месяцев и рассказали, чего ждать в 2020 году.



## Состояние и драйверы рынка ИБ

### Рынок ИБ в России вырос, но этого никто не заметил

В 2019 году запланированные бюджеты увеличились в среднем на 20%, то есть рынок вырос. Однако это формальный рост: если оценивать его с точки зрения денег, реально потраченных и заработанных участниками рынка, то общая планка практически не превышает показатели прошлого года. Причина неисполнения бюджетов в большинстве случаев состоит в необходимости проходить конкурсные процедуры: компании просто не успевают закупить те средства защиты, которые запланированы или необходимы.



**Борис Симис**

заместитель  
генерального директора  
по развитию бизнеса

### Смена парадигмы: ability to detect уже здесь

В последние пару лет мы отмечали, что парадигма обеспечения информационной безопасности начала меняться и все больше компаний приходят к пониманию, что построение защиты, которую нельзя сломать, — утопично по своей сути. Львиная доля систем либо уже взломана, либо может оказаться взломанной, и главная задача любой системы безопасности — максимально быстро обнаружить атаку и атакующего в системе, сократить окно его возможностей настолько, чтобы он не успел нанести непоправимый вред (то есть сегодня речь идет о так называемой ability to detect). В связи с этим наблюдается рост востребованности высокоинтеллектуальных средств защиты, позволяющих решать задачи по своевременному выявлению атак и инцидентов. В частности, речь идет о системах класса security information and event management (SIEM), network traffic analysis (NTA), комплексных anti-APT решениях. По итогам года мы наблюдаем почти трехкратный рост интереса к технологиям такого типа.

### Технологии vs. люди

Компании, которые ставят перед собой цель реально защитить себя в киберпространстве, сегодня сталкиваются с тотальным дефицитом кадров. Не хватает специалистов, которые имеют достаточный уровень компетенций, чтобы обеспечить высокий уровень ability to detect (то есть глубоко погружены в специфику бизнеса защищаемых компаний, следят за трендами защиты и нападения, разбираются в новейших технологиях и их уязвимостях). Мы видим, что все более востребованы специалисты, обладающие сразу несколькими компетенциями: речь может идти о совмещении знаний в области data science и кибербезопасности, глубокой отраслевой специфики (скажем, АСУ ТП) и информационной безопасности и т. п. Бизнес в итоге осознает, что у него нет необходимого количества специалистов такого уровня, и обычно приходит к аутсорсингу или аутстаффингу, а в редких случаях даже вынужден самостоятельно обучать кадры, которых мало на рынке.



## Регуляторы драйвят

Задачи реальной безопасности все чаще находят отражение в инициативах регуляторов: на практическую безопасность нацелены последние требования, стандарты и нормативы Центробанка, ФСБ, ФСТЭК. В частности, в 2019 году ключевые изменения произошли в законодательстве в области защиты объектов критической информационной инфраструктуры (КИИ), а также в нормативных документах Центробанка и ФСБ. Самое важное в КИИ — новые методические документы, которые определяют порядок взаимодействия субъектов КИИ с НКЦКИ (Национальный координационный центр по компьютерным инцидентам). В них разъясняется, о каких инцидентах сообщать, какую информацию передавать, в какой срок.

Появилось понятие средств ГосСОПКА, сформулированное в приказах ФСБ № 196, 281, 282. В них описаны инструменты, которые должен использовать центр ГосСОПКА. Кроме того, были опубликованы конкретные требования к субъектам ГосСОПКА, и это уже не рекомендации, а обязательные для исполнения документы. Начала складываться практика привлечения к ответственности по ст. 274 Уголовного кодекса («Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»), но пока только по поводу очевидных вещей: наказывают за атаки на субъекты КИИ и за серьезные нарушения должностных инструкций.

В следующем году также ожидается проработка изменений закона № 187-ФЗ, в котором будут скорректированы неоднозначные термины и формулировки. Разрабатываются и методические документы ФСТЭК по анализу угроз в информационных системах: будем надеяться, что в предстоящем году они будут утверждены.

Не менее интересные изменения ожидаются в нормативных документах Центробанка: в следующем году вступят в силу три положения для платежных сервисов. Главный вывод: с 1 января 2020 года финансовые организации должны использовать софт, у которого есть либо сертификат ФСТЭК, либо свидетельство о прохождении анализа уязвимостей. Мы не ожидаем, что разработчики банковского ПО начнут массово проводить сертификацию своих решений, так как из всего объема сертификационных испытаний фактически требуется только проведение анализа уязвимостей и недекларированных возможностей. Это традиционная услуга, востребованная кредитными организациями с высоким уровнем зрелости, но теперь она становится обязательной для всех финансовых организаций. Отдельно стоит отметить, что процедура анализа уязвимостей, на которую ссылаются нормативные документы Центробанка, требует, чтобы разработчики ПО проводили такой анализ самостоятельно, в рамках жизненного цикла разработки своих продуктов.

Уже сегодня это подхлестнуло рынок Application Security. Вендоры банковского ПО начали заказывать услуги анализа защищенности и выстраивать процесс защищенного жизненного цикла. Для самописного ПО банки активно заказывают статический и динамический анализ кода. Если раньше такие услуги интересовали в основном энтузиастов из финтех-компаний, то сейчас они необходимы всем финансовым организациям без исключения.

Анализ защищенности достаточно дорог, исполнителей мало, и за них уже сейчас приходится конкурировать. В последние месяцы спрос вырос так резко, что предложение не успевает. Эксперты крупной компании в сфере ИБ (таких на российском рынке четыре-пять) могут сделать за год 30–50 анализов защищенности, а у каждого банка из первой десятки подобных приложений может быть 15–20. И эти приложения регулярно обновляются, что требует дополнительных проверок на уязвимости. Если у организации много приложений и она часто выпускает обновления, выгоднее будет построить у себя процесс безопасной разработки.

Для производителей финансового ПО прохождение анализа уязвимостей становится конкурентным преимуществом. Уже сейчас многие разработчики банковского ПО говорят о заключении договоров с ведущими компаниями в сфере ИБ на работы по анализу исходного кода. Мы ожидаем, что в течение ближайших двух-трех лет выстраивание доказуемого цикла безопасной разработки станет для вендоров банковского ПО мейнстримом.

Чтобы убрать неопределенность и расплывчатость в требованиях к анализу защищенности, в этом году технический комитет Центробанка (ТК № 122) разработал проект методического документа «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций», где подробно расписывается, как именно нужно проводить анализ уязвимостей приложений. Для России это первый опыт обязательного нормативного документа, подобная конкретизация была только в системе сертификации. Профиль защиты — обязательный документ, он предназначен для открытого рынка, и этому документу придется соответствовать. Не исключено, что примеру Центробанка последуют другие ведомства.

Нельзя не отметить и появление закона о «суверенном интернете»: это первый случай, когда федеральный закон обязывает коммерческие компании (в данном случае — операторов связи) проводить киберучения. Раньше никто не обязывал компании в такой форме оценивать, насколько система способна противодействовать атакующим. Аналогичное требования к владельцам значимых объектов КИИ появилось в нормативных документах ФСБ (владельцы значимых объектов КИИ обязаны составлять планы реагирования на инциденты и отрабатывать их в ходе учений). Если раньше киберучения проводились в организациях с высоким уровнем зрелости, то в ближайшие два-три года они будут проводиться в очень многих компаниях: эти требования касаются всех операторов КИИ.

**Алексей Новиков**

директор экспертного  
центра безопасности

## Общие тенденции ИБ

Крупный бизнес начал осознавать, что АPT-атаки — это по-настоящему значимый риск. Мы провели опрос<sup>1</sup>, и 39% его участников отметили, что защита от АPT-атак — приоритетное направление развития кибербезопасности в их компаниях.

В решение вопросов ИБ вовлекаются топ-менеджеры организаций, и для них остро стоит вопрос эффективности существующей системы ИБ и используемых подходов. Руководство задается вопросом — а действительно ли те системы и меры, которые используются в компании, смогут защитить от реализации самых значимых рисков. Важно, как измерять эффективность ИБ. Новости об успешных целевых атаках АPT-группировок постоянно мелькают в СМИ, и под угрозой не только те компании, которые упоминаются в этих статьях, но и любая другая. Нельзя забывать и о массовых атаках, жертвами которых продолжают становиться крупные компании, выплачивающие выкупы за зашифрованные данные.

Наши проекты по ретроспективному анализу и расследования инцидентов свидетельствуют о том, что многие компании, которые перешли к практике выявления киберинцидентов, обнаруживают следы взломов, произошедшие несколько месяцев, а то и несколько лет назад (в прошлом году была выявлена группировка TaskMasters, которая находилась в инфраструктуре одной из жертв как минимум 8 лет). Это означает, что преступники уже давно контролируют множество организаций, но сами организации не замечают их присутствия, думая, что на самом деле защищены. При этом часто оказывается, что в инфраструктуре таких компаний «живет» даже не одна, а несколько группировок.

Итогом планомерной работы с компаниями стало то, что сегодня они начали действительно интересоваться информационной безопасностью, выявлять киберинциденты в собственной инфраструктуре, анализировать действия хакеров, задаваться вопросом о том, готова ли их инфраструктура к атакам. Это, определенно, положительная тенденция.

Но есть и отрицательная. Преступники все лучше осваиваются в киберпространстве. Мир информационных технологий уже нельзя назвать виртуальным: настолько тесно он связан с реальным. Самый яркий пример — рынок в дарквебе, где продается огромное количество запрещенных товаров и услуг, в том числе и хакерские утилиты. При этом видно, что планомерной государственной программы по повышению осведомленности граждан в вопросах кибербезопасности пока не существует: каждый сам выбирает, как и где ему просвещаться. Поэтому преступники легко могут обманывать доверчивых граждан не только в целях выманивания денег и сведений, но и для пополнения своих рядов малообразованными новичками.

Порог входа в киберпреступность крайне низкий, а обучающие материалы по взлому систем или по различным мошенническим схемам доступны и на интернет-сайтах, и в разных каналах в мессенджерах.

<sup>1</sup> Опрос проводился среди посетителей сайта компании Positive Technologies, аудитории интернет-портала [SecurityLab.ru](https://securitylab.ru) и участников ряда отраслевых сообществ.



Помогает преступникам в их деятельности криптовалюта: на теневых площадках создаются даже собственные биржи для вывода денег с банковских карт в биткойны и обратно. Это облегчает для преступных группировок приток средств, а также позволяет анонимизировать платежи.

## **APT-группировки vs. защитники: соотношение сил**

Расследуя деятельность APT-группировок, в этом году мы выявили рост числа APT-атак на различные отрасли. Если в прошлом году в поле нашего зрения попали 12 APT-группировок, то в этом году предметом исследований стали уже 27 группировок. Эта тенденция коррелирует и с нашими данными о постоянном росте числа уникальных киберинцидентов из квартала в квартал (в третьем квартале 2019 года зафиксировано на 6% больше уникальных киберинцидентов, чем во втором)<sup>2</sup>. Как и ожидалось, целенаправленные атаки в уходящем году существенно преобладали над массовыми. В течение года мы наблюдали рост целенаправленных атак: в третьем квартале их доля составила 65% (против 59% во втором квартале и 47% в первом). Организации год за годом берут на вооружение все более эффективные методы защиты, поэтому массовые атаки попросту перестают работать. Такая тенденция с большой вероятностью сохранится в будущем. Если же говорить о таргетированных атаках, то ситуация иная: средняя скорость реакции компаний сегмента large enterprise на современные угрозы — около трех лет. То есть с момента осознания необходимости покупки решения по выявлению атак и противодействию злоумышленникам до его реального применения в компаниях проходит около трех лет, посвященных бюджетированию, тендерам, пилотным внедрениям, закупке, внедрению, обучению и проч.

При этом злоумышленники активно используют новейшие уязвимости (в 2019 году APT-группировки использовали в своих атаках четыре уязвимости нулевого дня), действуют очень быстро, а главное — часто меняют свой инструментарий и тактики. Например, группировка RTM в течение года использовала три разных способа получения информации о контрольных серверах: через namescoin, через Tor, через bitcoin. Вместе с тем в 2019 году мы видели три разные версии дроппера (установщика основного модуля ВПО), одну версию загрузчика и три различных версий трояна.

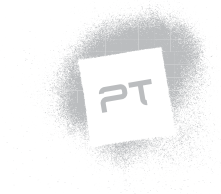
Другая группировка, работающая в финансовом секторе, Cobalt, с осени 2019 года для каждой зараженной машины с контрольного сервера скачивает закодированный CobInt с уникальной хеш-суммой для каждой загрузки: таким образом злоумышленники обходят детектирование их по хеш-суммам финального вредоносного файла.

Одна из группировок, занимающихся кражей данных, в 2019 году использовала семь различных версий ВПО и четыре разные тактики для закрепления и обхода детектирования в инфраструктуре.

---

<sup>2</sup> Эти выводы подтверждаются данными Генеральной прокуратуры: число преступлений в сфере ИТ в уходящем году выросло почти вдвое по сравнению с 2018 годом и к концу года может достичь 270 000 только зарегистрированных случаев, то есть 14% от общего числа всех зарегистрированных преступлений в России.





Таким образом, судя по данным Экспертного центра безопасности Positive Technologies (PT ESC), в 2019 году группировки в среднем использовали по четыре различных варианта ВПО и по пять тактик для закрепления в инфраструктуре. В то же время, 144 месяца — максимальное время, спустя которое стало известно о действиях АРТ-группировки, и 17 месяцев — среднее время, прошедшее с момента атаки до появления о ней публичной информации.

Таким образом, ключевыми критериями, по которым можно оценивать сегодня расстановку сил между злоумышленниками и защитниками, являются:

1. Использование новейших техник атаки против использования новейших средств защиты: здесь в ряде случаев разбег доходит до трех лет не в пользу защиты.
2. Использование новых уязвимостей против среднего времени патч-менеджмента: соотношение практически всегда оказывается в пользу злоумышленников, которые адаптируют новейшие эксплойты для своих атак иногда в течение суток.
3. Стоимость инструментов — стоимость защиты. По нашей оценке, набор инструментов для проведения атаки, направленной на кражу денег из банка, может стоить от 55 тыс. долл. США. Кибершпионская кампания обходится на порядок дороже, ее минимальный бюджет составляет 500 тыс. долл. США. Оценку же полной стоимости защиты, включая стоимость технических средств, затраты на выстраивание процессов и зарплату специалистов, выполнить сложно, так как все зависит от компании и уровня ее зрелости с точки зрения ИБ.

Целями АРТ-группировок по-прежнему являются компании, владеющие важными данными и деньгами. При этом атакуют не только крупные компании, но и предприятия среднего и малого бизнеса, прежде всего для того, чтобы использовать их как плацдарм для нападения на крупный бизнес, а также для маскировки своих действий.

Усиливается тренд атак на провайдеров услуг связи, вендоров и поставщиков услуг. При этом иногда компании даже не подозревают, что от данных организаций может исходить угроза. В качестве примера приведем случай из нашей практики: один из поставщиков вендинговых автоматов просил организовать удаленный канал доступа к автомату через интернет. Автомат был подключен к корпоративной сети и через нее был обеспечен доступ к интернету для работы автомата и его синхронизации с серверами управляющей компании. В результате внутренние ресурсы компании подверглась атаке через этот канал связи.

## Прогнозы

Крупные компании при анализе собственных рисков ИБ продолжают обращать внимание не только на требования регуляторов, но и на необходимость построения практической безопасности, направленной на минимизацию значимых для себя бизнес-рисков. Малый и средний бизнес, не всегда готовый вкладывать достаточные средства в кибербезопасность, будет оставаться под прицелом как массовых киберкампаний, так и целевых атак хакерских группировок. Ввиду повышения защищенности крупных игроков хакерам придется прибегать не только к изощренному фишингу и созданию все более совершенных образцов ВПО, но и к взлому менее защищенных компаний, чтобы проводить через них атаки на целевые организации, в том числе по настроенным между ними доверенным каналам.

Схемы киберуслуг на продажу будут развиваться, набирать обороты и принимать новые формы. В частности, может приобрести большую популярность схема, когда одни злоумышленники взламывают инфраструктуры компаний и проникают во внутреннюю сеть, но не используют такой доступ для своих целей, а продают или сдают его в аренду другим участникам теневого рынка (модель access as a service, «доступ как услуга»). Операторам вредоносного ПО (например, шифровальщиков) не надо будет думать, каким образом заразить системы компании, они просто заплатят некоторую ренту за доступ к уже взломанным сетям. Например, группировка REvil (также известная как Sodinokibi) уже использует такую схему для распространения ВПО. Цены на такой доступ могут варьироваться в зависимости от его уровня. Например, если есть доступ к сотням узлов в сети, он может стоить 3-5 тыс. долл. США, а полный контроль над корпоративными сетями может продаваться за 20 тыс. долл. США и дороже.

Можно прогнозировать рост числа инцидентов в секторе SMB, связанных с ВЕС-мошенничеством (business email compromise) — социальной инженерией с использованием реальных аккаунтов сотрудников компаний, в том числе руководства. Угроза особенно актуальна для компаний, которые регулярно совершают крупные денежные переводы в адрес контрагентов, партнеров, поскольку злоумышленники могут — якобы от имени доверенного лица — просить уполномоченных сотрудников компании-жертвы оплатить счет по подставным реквизитам. Примеры подобных атак уже известны, и, по данным ФБР, за последние три года они уже нанесли ущерб в размере 26 млрд долл. США.

## Государство и политика

За первые три квартала 2019 года мы зафиксировали 167 атак на госучреждения (за такой же период в 2018 году было зафиксировано 133 атаки). Как мы и ожидали, чаще всего атаки проходили с использованием фишинга (49% атак) и ВПО (63% атак), но, кроме этого, не теряют актуальности кибератаки на веб-сайты госкомпаний. В первых трех кварталах 2019 года 18% атак были связаны именно со взломом веб-приложений (в 2018 году этот показатель был почти таким же — 19%).

Сайты атакуют с целью кражи персональных данных пользователей, дефейса, заражения майнерами криптовалют. Фишинг и ВПО используются для доставки в инфраструктуру шифровальщиков и в целевых атаках для шпионажа.

В рамках нашего исследования мы выделили 10 АРТ-группировок, которые на протяжении последних двух лет атаковали государственные компании в России, и отметили, что главным их мотивом был шпионаж. Кроме того, мы провели опрос специалистов в области ИТ и ИБ о готовности их компаний противостоять АРТ-атакам. Каждый второй респондент из госсектора (45%) ответил, что его компания не готова к АРТ, а 68% отметили недостаточную квалификацию своих специалистов по ИБ для противостояния столь сложным угрозам.

## Прогнозы

Крупнейшим политическим событием можно назвать президентские выборы в США в 2020 году. Стоит ожидать резонансных кибератак, которые будут направлены на дефейс сайтов политических партий и кандидатов. Кроме того, можно ожидать попыток повлиять на общественное мнение через социальные сети. Не исключены атаки на электронные системы голосования, уязвимость которых была продемонстрирована в 2019 году.



## Атаки на пользователей

Количество атак на частных лиц продолжает расти. За три квартала 2019 года мы насчитали 231 хакерскую кампанию, направленную на обычных пользователей (за аналогичный период 2018 года — 217 кампаний). Как правило, это массовые атаки, которые затрагивают одновременно множество жертв, и подсчитать точное их число или масштаб ущерба невозможно.

Как и прежде, основными способами добраться до данных пользователей являются социальная инженерия и заражение устройств вредоносным ПО. Преступники продолжают использовать неграмотность людей в вопросах обеспечения собственной информационной безопасности. Еще годом ранее подбор паролей к учетным записям на сайтах и в социальных сетях составлял значимую долю методов атак (12% за три квартала 2018 года), но в 2019 году мы замечаем, что этот тренд сходит на нет: всего в 6% атак использовался такой метод. Мы связываем это с тем, что подавляющее большинство интернет-сервисов сегодня позволяют использовать двухфакторную аутентификацию, что усложняет атаку, — и люди действительно пользуются этой двухфакторной аутентификацией при доступе к своим аккаунтам.

Атаки с целью получения данных составили 64% всех атак на частных лиц в третьем квартале 2019 года. Почти половина этих атак (47%) была нацелена на кражу учетных данных от интернет-сервисов, 23% атак — на кражу данных платежных карт, 12% — на кражу персональных данных, остальные — на доступ к личной переписке.

Злоумышленники активно используют уязвимости веб-сайтов для атак на обычных граждан. По нашей статистике за 2019 год, 92% веб-приложений позволяют проводить атаки на пользователей. При этом 82% уязвимостей, которые мы находили, обусловлены ошибками при разработке кода. Недостатки безопасности в 16% исследованных сайтов позволяли полностью контролировать не только само веб-приложение, но и сервер. Такой контроль дает атакующему возможность проводить серьезные атаки, например распространять вредоносное ПО или внедрять JavaScript-снифферы<sup>3</sup> в код сайта для кражи данных банковских карт. Это тренд прошлого года в сфере электронной коммерции, но глобальная проблема безопасности веб-приложений актуальна и сегодня. Учитывая бурный рост рынка интернет-торговли (двукратный к 2023 году, по данным [Data Insight](#)), можно ожидать усугубления данной проблемы, в том числе из-за атак с помощью снифферов.

Важно отметить участвовавшие случаи публикации в дарквебе баз с пользовательскими данными, которые были украдены у различных организаций в результате атак либо просто не были защищены паролем и хранились в открытом доступе по халатности IT-администраторов. Сложно сказать, насколько этот тренд относится именно к 2019 году, вероятно, что данные раскрывались и ранее, но это не предавалась такой огласке. Сегодня для преступников продажа данных большими объемами или поштучно<sup>4</sup> стала настоящим прибыльным бизнесом.

3 JavaScript-сниффер — небольшой фрагмент JavaScript-кода, который злоумышленники незаметно добавляют к легитимному коду на сайте и крадут вводимую пользователями информацию. Так было в нашумевшей кампании [MageCart](#), о которой известно уже много лет, но по-настоящему громко она заявила о себе во второй половине 2018 года и продолжилась в 2019 году. По данным RiskIQ, 17,3% всех вредоносных объявлений в интернете содержит такие скрипты.

4 Согласно нашему исследованию, стоимость одного набора паспортных данных колеблется около 2 долл. США.

Злоумышленники могут объединять данные утечек, произошедших за последние несколько лет, в одну базу и продавать их оптом. Причем преступникам, распространяющим за деньги такие полные цифровые досье, вовсе не нужно быть хакерами, достаточно просто грамотно переработать информацию об имеющихся в истории той или иной компании утечках. Такие инциденты сказываются прежде всего на репутации компании. Минимизировать риски поможет только комплексный зрелый подход к безопасности — от повышения грамотности сотрудников в вопросах ИБ до жесткого разграничения прав доступа и применения наиболее продвинутых практико-ориентированных средств кибербезопасности.

## Прогнозы

Атаки с использованием уязвимостей сайтов, в том числе с применением JavaScript-снифферов, продолжатся ввиду их высокой эффективности. Обычный пользователь бессилен сделать безопасным интернет-ресурс, где он оплачивает покупку, ответственность за противодействие атакам лежит на владельцах сайтов. Однако пользователям стоит более внимательно относиться к тем ресурсам, где они вводят данные банковских карт: если это недоверенный сайт или малоизвестный, то стоит взвесить все за и против, прежде чем рисковать своими данными. Считается, что более крупные и известные на рынке компании надежнее защищают пользователей от атак, но одной только широкой известности бренда недостаточно, есть примеры атак, когда именно крупные бренды становились жертвами и ставили под угрозу своих пользователей.

Атаки на личные устройства пользователей не потеряют актуальности, поскольку для большинства людей удобство при работе с гаджетом важнее, чем безопасность личных данных. Скорее всего, атакующие будут совмещать атаки на гаджеты с классическими методами социальной инженерии (например, с мошенническими звонками по телефону с целью получить банковские данные). Гаджеты прочно вошли во все сферы нашей жизни, и теперь чтобы выведать какие-то данные или украсть деньги с банковского счета, преступникам необходимо атаковать мобильные устройства.



**Дмитрий Даренский**

руководитель практики  
промышленной  
кибербезопасности

## Промышленный сектор под угрозой

В начале 2019 года было совершено несколько кибератак на крупные промышленные компании. В частности, производитель алюминия Norsk Hydro перевел в ручной режим часть рабочих процессов и приостановил несколько заводов из-за кибератаки, которая привела к шифрованию файлов в инфраструктуре заводов и филиалов компании по всему миру. Ущерб был оценен в 41 млн долл. США. В атаке использовался шифровальщик LockerGoga, который также был выявлен в начале 2019 года в атаках на три химические компании в США. В июне 2019 года атаке уже с использованием другого вымогателя подвергся производитель авиационных деталей ASCO, на время восстановительных работ около 1400 работников компании были отправлены в неплановый отпуск.

Согласно нашим исследованиям, в первых трех кварталах 2019 года в 83% атак на промышленные компании применялся фишинг и в 89% атак использовалось ВПО. Всего за три квартала мы зафиксировали 92 кибератаки, что существенно превышает показатель аналогичного периода 2018 года (25 атак). Массовые атаки в основном связаны с заражениями майнерами криптовалют или шифровальщиками. Основной целью киберпреступников в атаках на промышленные и энергетические компании остается шпионаж: хакеры стремятся на максимально возможное время закрепиться в инфраструктуре компании и получить контроль не только над IT-системами, над ключевыми компьютерами и серверами, но и над технологической сетью с промышленным оборудованием.

### Прогнозы

Атаки с целью шпионажа продолжатся и в 2020 году. При этом можно ожидать, что большинство таких атак станут продолжением успешно проведенных ранее, а компании научатся их выявлять. Внимание к теме кибератак, в особенности целевых АРТ-атак, существенно повысилось, компании осознают необходимость внедрения эффективных систем, которые способны не только противодействовать отдельным угрозам, но и выявлять действия высококвалифицированных хакеров. Это диктуется не только требованиями регуляторов к защите КИИ: руководство промышленных и энергетических компаний в целом осознает необходимость выстраивать действительно эффективные процессы ИБ.

**Павел Новиков**

руководитель группы  
исследований безопасности  
телекоммуникационных  
систем

## Небезопасный телеком

Уязвимости сетей 2G/3G не теряют актуальности и уже используются преступниками для получения доступа к банковским счетам абонентов. Недостатки защиты мобильных сетей позволяют обходить тарификацию, пользоваться услугами связи за счет других абонентов, перехватывать SMS, прослушивать разговоры и вызывать отказ в обслуживании. Немного лучше защищены и сети 4G: они подвержены уязвимостям, которые позволяют злоумышленнику отслеживать местоположение абонентов, обходить ограничения оператора на использование услуг связи, лишать абонентов связи или переводить их в небезопасный режим 3G. Телеком-операторы сталкиваются с атаками злоумышленников ежедневно, но далеко не все понимают, как им противостоять.

Основными потребителями услуг связи постепенно становятся не люди, а вещи. Сейчас в ряде стран уже запущены первые тестовые участки сети 5G, основными потребителями которой станут устройства интернета вещей (IoT). Защищенность умных систем на базе IoT-устройств напрямую зависит от безопасности используемых телекоммуникационных технологий. По нашим данным, в любой сети, будь то 2G, 3G, 4G или даже 5G, злоумышленник может лишить абонентов связи. На сегодняшний день это означает, что в критический момент могут быть недоступны элементы умного дома или промышленные устройства, а с распространением сетей 5G и развитием IoT увеличится и масштаб угроз: жертвами атак могут, к примеру, стать подключенные автомобили или системы жизнеобеспечения города.

## Прогнозы

С внедрением сетей 5G операторы столкнутся с новыми рисками, связанными с широким использованием виртуализации, усложнением задач администрирования, применением хорошо изученных хакерами интернет-протоколов. Кроме того, реальные сети 5G пока опираются на предыдущие поколения: это сети с архитектурой Non-Standalone, то есть построенные на базе опорной сети 4G LTE. На переходном этапе устройства подключаются к частотам 5G для передачи данных, но для голосовых вызовов и SMS все еще используются сети 4G и 2G/3G. Соответственно, все недостатки защиты этих сетей еще долгое время будут актуальны и для абонентов 5G.

Нельзя надеяться на то, что проблемы 2G/3G в ближайшее время утратят свою актуальность. По прогнозам GSMA<sup>5</sup>, число пользователей сетей 4G/5G только начинает приближаться к таковому для сетей 2G/3G. Существенного уменьшения числа абонентов в сетях 3G не предвидится как минимум до 2025 года, и даже тогда доля пользователей сетей 2G/3G будет, предположительно, составлять четверть от общего числа (без учета устройств IoT). Процент пользователей сетей 4G будет только увеличиваться по крайней мере до 2024 года, а сети 5G пока строятся на базе инфраструктуры 4G.

<sup>5</sup> Ассоциация GSM — торговая организация, представляющая интересы операторов мобильной связи по всему миру.





### Ярослав Бабин

руководитель группы  
исследований безопасности  
банковских систем

## Безопасность финансового сектора

За первые три квартала 2019 года мы зафиксировали 61 атаку на финансовые компании (за аналогичный период 2018 года их было 69, а за весь 2018 год — 92). Причем в 74% атак использовался фишинг и в 80% атак вредоносное ПО. Это основные методы проникновения из интернета в локальную сеть финансовых организаций.

Предполагаем, что незначительный спад числа кибератак на финансовые организации связан с несколькими факторами. Во-первых, мы заметили существенное снижение доли массовых атак на такие учреждения — например, в третьем квартале 2019 года всего 4% зафиксированных атак носили массовый характер, а в аналогичный период годом ранее этот показатель был на уровне 32%. Можем объяснить это тем, что большинство банков, особенно крупных, сегодня готовы эффективно отразить массовую атаку (например рассылку шифровальщика), и хакеры сконцентрировали свое внимание на других, менее защищенных отраслях.

Во-вторых, число целенаправленных атак на финансовые организации не снижается, группировки не только обновляют арсенал используемого ВПО и свою инфраструктуру, но и обращают внимание на новые регионы, выбирают жертв, менее готовых к таким атакам.

Согласно нашему исследованию, как минимум пять APT-группировок за последние два года угрожали финансовым компаниям в России. Другие пять группировок не были замечены в атаках на Россию, но поскольку в списке их жертв значатся иностранные финансовые компании, мы полагаем, что они представляют потенциальную угрозу для финансовых организаций на территории Российской Федерации, а также для их дочерних компаний, находящихся за рубежом. Для проникновения все эти группировки используют комбинацию методов фишинга и заражения вредоносным ПО. Три из 10 группировок доставляют ВПО в инфраструктуру банков через легитимные сайты в интернете (методом watering hole<sup>6</sup>). Также 3 из 10 группировок для проникновения взламывают сначала инфраструктуру менее защищенных компаний-партнеров или филиалов, из которой есть легитимные каналы доступа в целевую финансовую организацию.

В первом и во втором кварталах мы выделяли атаки APT-группировок Cobalt и Silence, а также еще одной группы, которая использовала сетевую инфраструктуру, схожую с инфраструктурой группы FinTeam. В третьем квартале мы фиксировали активность группы Cobalt в России, Казахстане и странах Европы, а также фишинговые рассылки группы TA505 в адрес европейских и африканских банков и группы RTM в адрес банков России и Белоруссии.

Искусственный интеллект все чаще применяется в финансовых организациях. Исследования банковского рынка в России и за рубежом свидетельствуют о расширении сферы применения этой технологии, прежде всего машинного обучения. Машинное обучение не только обеспечивает удобство конечного потребителя при использовании банковских сервисов, но и успешно применяется для противодействия мошенничеству в банковской сфере.

6 Атака watering hole — это распространение вредоносного ПО через профильный веб-ресурс, который посещают сотрудники атакуемой компании.

## Банкоматы и платежные терминалы

По данным некоммерческой организации [European Association for Secure Transactions](#) (EAST), в первом полугодии 2019 года основной ущерб от кибератак на системы самообслуживания европейских банков пришелся на атаки в отношении платежных терминалов (124 млн евро) — притом что в результате атак на банкоматы с использованием ВПО и техники black box<sup>7</sup> был зафиксирован лишь незначительный финансовый ущерб, не превышающий 1000 евро.

Растет число мошеннических операций с бесконтактной оплатой; в основном это связано с операциями ниже лимитов CVM (Cardholder Verification Method), при которых пользователю для подтверждения транзакций не нужно вводить PIN.

Если лет 15 назад число поставщиков финансовых услуг ограничивалось банком — эмитентом карты, компанией, предоставляющей услуги эквайринга, и платежной системой (Visa, MasterCard), то сейчас гораздо больше лиц имеют доступ к картам и к информации, с ними связанной: Apple Pay и Samsung Pay, производители mPOS-терминалов, операторы мобильных сетей, производители смартфонов и т. п. Количество «свидетелей платежа» увеличивается, все они опосредованно имеют доступ к банковскому счету и информации держателя карты, а следовательно — повышается риск утечек и мошеннических операций. Аналогичная ситуация сложилась и с онлайн-банкингом.

В странах Евросоюза в этом году приступили к внедрению новой [директивы платежных транзакций PSD2](#), которая призвана создать условия для инноваций в финансовом секторе и предоставить дополнительную защиту клиентам. Директива подразумевает:

- предоставление банками открытого API всем сторонним поставщикам финансовых услуг (Open Banking);
- требование по усилению аутентификации плательщика (Strong Customer Authentication). Данное требование говорит об обязательной двухфакторной аутентификации, например о необходимости проверять наличие двух из трех элементов периодически (PIN, отпечаток пальца, лицо и т. п.). В соответствии с этим требованием, например, после каждой пяти бесконтактных транзакций плательщик будет обязан вставлять карту в считыватель чипа, а мобильное приложение будет периодически запрашивать PIN, даже если введена функция авторизации по отпечатку пальца.

Комплексное внедрение таких мер позволит повысить безопасность банковских систем, особенно в такой чувствительной части, как бесконтактная оплата и карточные платежи.

Это, несомненно, большой шаг к безопасности финансового сектора, причем на государственном уровне, и можно только приветствовать появление аналогичных стандартов в области проведения платежей по всему миру, в том числе и в нашей стране.

---

<sup>7</sup> Атака на банкомат путем подключения стороннего устройства к устройству выдачи купюр (диспенсеру).



## Прогнозы

Преступники будут продолжать использовать фишинг и ВПО для проникновения в сети банков, так как эти техники не теряют эффективности. Изменяться будут инструменты злоумышленников: чтобы обходить средства защиты, им необходимо менять и запутывать код ВПО. Также хакеры будут продолжать использовать вновь опубликованные эксплойты для атак в течение нескольких часов после публикации, это существенно повышает шансы на атаку. Учитывая, что эксплойты для уязвимостей нулевого дня на теневом рынке дороги, хакеры не будут их активно использовать, чтобы атаки окупались. К тому же, уже известные уязвимости, для которых вендоры уже выпустили обновления безопасности (например, CVE-2017-11882 в MS Office), все еще успешно эксплуатируются злоумышленниками из-за несвоевременного обновления систем в банках, и необходимости тратить на дорогостоящие эксплойты у злоумышленников нет.

Ввиду того, что для конечных пользователей все более доступной становится услуга мобильного банкинга, злоумышленники с большой долей вероятности будут переходить на атаки мобильных банковских приложений. Скорее всего, преступников будут интересовать уязвимости, связанные с раскрытием информации о пользователях. В связи с этим в будущем году можно ожидать новостей об утечках персональных данных, в том числе данных банковских карт. Мы также предполагаем рост атак на пользователей с применением простейших способов социальной инженерии (например, фейковых SMS-сообщений и звонков из банка): к сожалению, они наиболее эффективны, поскольку знания о безопасности у массового потребителя все еще практически отсутствуют.

Внедрение искусственного интеллекта в финансовом секторе продолжится, в том числе в целях повышения кибербезопасности и развития технологий антифрода. Это дает нам основание полагать, что злоумышленники будут изобретать новые способы мошенничества в системах онлайн-банкинга или переходить к атакам на более простые сервисы, такие как интернет-магазины, онлайн-сервисы по продаже билетов и др.

**Дмитрий Складов**

руководитель отдела  
анализа приложений

**Марк Ермоллов**

ведущий специалист  
отдела исследований  
безопасности ОС  
и аппаратных решений

## Аппаратные уязвимости в фокусе исследований

Аппаратные уязвимости можно в прямом смысле назвать приветом из прошлого. Это касается, прежде всего, нашумевших процессорных уязвимостей Spectre и Meltdown, проблем в Intel ME, Intel VISA, а также касается и многих других уязвимостей, доклады о которых все чаще стали мелькать на конференциях по информационной безопасности.

Целый ряд аппаратных уязвимостей, о которых пишут и говорят сегодня исследователи всего мира, являются, по сути, следствием достаточно спорных решений, вызванных желанием повысить скорость работы или облегчить разработку ПО.

### Атаки по побочным каналам

Архитектура процессоров x86, основы которой закладывались в 80-е годы, и используемая ею система разграничения доступа к ресурсам процессора позволяют реализовать уязвимости, связанные со спекулятивным выполнением, в обход существующих механизмов защиты.

Эти уязвимости в механизмах спекулятивного выполнения, такие как Spectre и Meltdown, при использовании кэша данных процессора в качестве побочного канала с помощью специальных методик (таких как FLUSH+RELOAD) позволяют извлекать критически важные данные системы, доступ к которым должен быть ограничен для непривилегированного кода. Уязвимость Spectre была впервые обнаружена исследователем из Google (проект Zero), а Meltdown — группой специалистов из Грацкого технического университета (Австрия) в 2017 году.

Уязвимости Spectre и Meltdown представляют опасность для большинства современных процессоров Intel и AMD, а также для некоторых процессоров архитектуры ARM.

Атаки, основанные на подобных уязвимостях, позволяют обходить аппаратные средства защиты и, например в облачных конфигурациях, получать доступ к информации всех прочих пользователей, задачи которых исполняются на удаленном сервере.

Никто, конечно, не закладывал возможность доступа к конфиденциальной информации в архитектуру умышленно, но комбинация ошибок и спорных решений, накопленных за время разработки и усовершенствования микропроцессоров, такую возможность дает.

### Аппаратный реверс-инжиниринг в тренде

Два последних года показали нам только верхушку айсберга аппаратных уязвимостей, их поиск стал настоящим трендом среди исследователей, которые в поиске «дыр в железе» переходят на все более низкий уровень, ищут (и находят!) уязвимости на уровне печатной платы, элементов аппаратной логики.

Специалисты активно переходят к аппаратному реверс-инжинирингу, на различных площадках публикуют фото ядер чипов, сделанных при помощи электронных микроскопов. Если раньше исследования процессоров велись в основном энтузиастами и были интересны очень узкому кругу специалистов, то сейчас, учитывая такие масштабы изысканий, вовлеченность широкого круга исследователей и интерес прессы к проблеме, аппаратные уязвимости представляются настоящей угрозой.

## Смена модели угроз

Понятно, что угроза такой атаки для конечного пользователя исчезающе мала, она пока скорее потенциальная. Пользователь, конечно, тоже свое получит, но пока такие атаки слишком сложны и дороги.

Но бизнес уже вынужден рассматривать такие угрозы, понимать риски, готовиться к отражению атак. Пока еще говорить об ущербе нельзя, но говорить о наличии проблемы надо, и крупные компании это хорошо понимают, закладывая в свою модель угроз такие уязвимости: выделяют бюджеты на защиту от таких угроз, инвестируют в разработку защитного оборудования и обучение персонала. Это серьезные средства, и они тратятся на затыкание тех самых «дыр из прошлого», с которых мы начали рассказ. Ведь уязвимы не только компьютеры в офисе, уязвимости находят в роутерах и маршрутизаторах, серверах, принтерах, мобильных устройствах.

Утечка конфиденциальной информации, болезненная даже для обычного пользователя, способна фактически парализовать работу крупных коммерческих и государственных организаций, нарушить бесперебойную работу предприятий инфраструктуры и здравоохранения.

Исправление ошибок, сделавших возможными такие уязвимости, ведется разработчиками процессоров совместно с исследовательскими центрами и крупнейшими разработчиками ПО, но масштаб проблемы не позволяет надеяться на скорое ее решение. Бизнес и инфраструктурные объекты по-прежнему находятся в зоне повышенного риска. При этом производители признают наличие уязвимостей, исправляя их в процессорах нового поколения.



**Николай Анисеня**

руководитель группы  
исследований безопасности  
мобильных приложений

## Мобильные угрозы

Сегодня более половины населения нашей планеты являются владельцами смартфонов. Активное проникновение умных мобильных устройств заставляет киберпреступников искать и новые сценарии атак. Актуальные векторы угроз, на наш взгляд, связаны с новыми способами получения root и jailbreak (checkm8 и др.), техниками обхода биометрии, пиннингом<sup>8</sup>, отсутствием защиты кода и атаками на пользователей.

### Обход биометрии

Исследователи из X-Lab за 20 минут разблокировали смартфон с помощью отпечатка пальца его хозяина, взятого со стакана. Воссоздать отпечаток пальца позволило приложение Tencent Security, способное реконструировать отпечаток даже по его фрагментам, снятым с нескольких предметов, а также гравировальный аппарат стоимостью 140 долл. США.

Подавляющее большинство мобильных банковских приложений позволяет использовать биометрию (отпечаток пальца, лицо) для входа. Нужно помнить, что это упрощенная аутентификация — упрощенная и для легального пользователя, и для злоумышленника. Приложение в этом случае вынуждено хранить аутентификационные данные на устройстве. И хотя у пользователя довольно часто есть возможность использовать вход по логину и паролю, соблазн простой аутентификации по PIN-коду или с использованием биометрии часто перевешивает безопасность. Наша практика показывает, что 25% приложений позволяют локально подбирать PIN-код — и 5 из 8 приложений проверяют PIN-код локально.

Пример атаки может выглядеть следующим образом. Получив на какое-то время незаблокированное устройство, злоумышленник сможет попытаться подобрать PIN банковского приложения, если защита от подбора PIN-кода не реализована или реализована некорректно. В большинстве случаев атакующему понадобится не более 10 000 попыток для успешного входа и доступа к банковским данным. Простым перебором вручную PIN-код можно подобрать в течение нескольких часов. Получить незаблокированный телефон можно просто выхватив его из рук жертвы в момент использования.

### Отсутствие защиты кода

Получение прав root и jailbreak на мобильном устройстве существенно снижает его безопасность. При этом разработчики по-прежнему уделяют мало внимания защите мобильных приложений от атак с использованием root или jailbreak. Две трети проверенных нами в 2019 году приложений не блокировали свою работу при наличии прав root или jailbreak либо не предупреждали пользователя об опасности работы в таких конфигурациях. И ни одно из проверенных за прошедший год приложений не содержало признаков запутывания кода основной логики, достаточного для противодействия анализу кода. Это на руку злоумышленникам, ведь вредоносные приложения охотно пользуются повышенными привилегиями.

<sup>8</sup> Технология Certificate Pinning заключается в зашивании сертификата для установления защищенного соединения в код приложения. Это позволяет защититься от атак подмены сертификатов на защищенное соединение даже если пользователь установил на устройство сертификат злоумышленника как доверенный. В случае такой атаки соединение не будет установлено и никакие данные передаваться не будут, тем самым пользователь будет защищен.

## Атаки на пользователей

В атаках на пользователей лидируют по-прежнему вредоносные приложения, которые пользователь устанавливает сам. Они запрашивают специальные разрешения, в том числе связанные с администрированием устройства, наложением поверх других окон, accessibility services (службами для лиц с ограниченными возможностями), screen share. Однако в некоторых случаях никаких специальных разрешений не требуется. Примером может служить обнаруженная нашим экспертом уязвимость в Android WebView.

## Уязвимости в WhatsApp

Громкие уязвимости в популярном мессенджере WhatsApp показывают, что даже проверенные миллион раз приложения могут содержать серьезные уязвимости, которые к тому же могут быть реализованы удаленно. Также среди исследователей наметился небольшой тренд на атаки через медиафайлы — через видео и изображения.

Как и ожидалось в прошлом году, развитие функциональных возможностей телефонов не осталось незамеченным для киберпреступников: атаки с использованием приложений удаленного доступа на смартфонах все чаще упоминаются в СМИ. Взломщики могут использовать возможности удаленного доступа, чтобы подсмотреть пароль в мобильном банке или выполнить от лица жертвы какие-то действия.

Компания Google в 2019 году сделала большой шаг в сторону обеспечения безопасности популярных мобильных приложений в Google Play. Теперь по программе Google Play Security Rewards Program исследователи могут получить выплаты за уязвимости любого Android-приложения с числом установок от 100 миллионов. Такая мера ожидаемо приведет к улучшению защищенности популярных Android-приложений.

**Александр Попов**

ведущий специалист отдела исследований безопасности ОС и аппаратных решений

## Безопасность операционных систем

В области безопасности операционных систем в последние годы происходят заметные изменения. Все началось с того, что в сообществах разработчиков и в компаниях, создающих операционные системы, постепенно укрепилось осознание невозможности исправить все до одной ошибки в программном коде.

Несмотря на все усилия, в код операционных систем, который становится все сложнее, новые ошибки добавляются быстрее, чем исправляются старые. Часть из этих ошибок приводит к уязвимостям информационной безопасности, что является серьезной проблемой. Чтобы ее решить, в отрасли появилось два взаимодополняющих подхода, которые начали улучшать ситуацию с безопасностью операционных систем.

Первый подход: ядро операционной системы должно обладать средствами самозащиты. Иными словами, в случае ошибки или атаки система должна безопасно обработать эту ситуацию. Существует популярная аналогия, где разработка операционных систем наших дней сравнивается с автомобильной индустрией 60-х годов XX века: тогда из-за огромного травматизма в ДТП автопроизводители начали разрабатывать средства безопасности для пассажиров, чтобы автомобиль был не только надежен в обычной ситуации, но и безопасен в случае аварии. Аналогичные технологии разрабатываются в наши дни для операционных систем. В частности, в этом году специалисты Microsoft Security Response Center представили детальный обзор типов уязвимостей и способов борьбы с ними в ядре Windows. Есть также разработанная мной карта средств защиты ядра Linux, которая отражает взаимосвязи между типами уязвимостей, методами их эксплуатации и имеющимися механизмами защиты.

Однако на практике внедрение средств самозащиты ядра операционной системы не бывает бесплатным. За повышение безопасности обычно приходится платить падением производительности и дополнительными сложностями для разработчиков системы. Наглядным примером этого служат попытки устранения аппаратных уязвимостей Spectre, Meltdown, MDS на уровне операционных систем.

Второй подход к решению проблемы ошибок в операционных системах — это непрерывное использование автоматических средств динамического и статического анализа. Наши операционные системы написаны на низкоуровневых языках программирования по целому ряду причин. Такие языки дают разработчику большую мощь и при этом требуют от него большой внимательности и профессионализма. А людям свойственно ошибаться, поэтому на помощь приходят автоматизированные средства проверки. Это и разнообразные методы статического анализа, включая поиск ошибок по паттернам, и технологии динамического анализа, одной из самых популярных среди которых стал фаззинг (методика тестирования ПО случайными данными). Примером проекта, вносящего значительный вклад в безопасность многих операционных систем, является фаззер syzkaller.

При этом у развития автоматизированных средств поиска уязвимостей есть важный побочный эффект: они доступны не только защитникам, но и атакующим.



## Заключение

Накопление проблем ИБ в различных сферах достигает предельной отметки. Аппаратные уязвимости пока не нанесли ущерба, однако дальновидные компании стали включать в свою модель угроз такие проблемы уже сейчас, понимая, что когда преступники научатся эксплуатировать подобные уязвимости, защищаться будет уже поздно.

А вот АРТ-атаки, напротив, «отработали» по полной, угрожая не только бизнесу, но и государственным учреждениям и объектам инфраструктуры.

Новости об утечках данных в этом году стали особенно громкими, в том числе и потому, что злоумышленники предположительно объединили утечки прошлых лет в единый массив для торговли на теневом рынке более полными цифровыми досье пользователей.

Многие технологии имеют свою темную сторону, которая может выйти из-под контроля и стать угрозой для всех. С грядущим распространением сетей 5G эксперты связывают возникновение новых рисков для телеком-операторов. Развитие искусственного интеллекта и технологий машинного обучения не только делает жизнь удобнее, но и дает мощный толчок для совершенствования инструментов взлома, а также для новых методов социальной инженерии.

Всеобъемлющая интеграция технологий порождает множество векторов атак. Противостояние угрозам в постоянно меняющемся мире современных технологий, адаптация к новым потребностям корпоративного и частного пользователя — первоочередные задачи специалистов ИБ, решение которых может потребовать принципиально новых подходов к обеспечению кибербезопасности.

---

### О компании

ptsecurity.com  
pt@ptsecurity.com  
facebook.com/PositiveTechnologies  
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.