

Интернет изнутри



ЗЛОВРЕДЫ В ИНТЕРНЕТЕ

**Тятя, тятя,
наши сети притащили ВПО**

История борьбы снаряда и брони:
путь от экспериментальных
вирусов до многофункционального
ВПО, созданного искусственным
интеллектом

с. 6

**Защита периметра цифровой
безопасности в эпоху массового
сканирования Сети**

Без повышения компьютерной и
сетевой культуры пользователей
никакая защита не сможет
справиться с кибератаками

с. 18

**Межоператорский бизнес
в России в период массовых
DDoS-атак**

Выживает не самый большой, а
самый гибкий и подготовленный

с. 46

**Евгений Панков: «Опасности и
киберугрозы будут меняться
вместе с технологиями»**

Эксперт рассказывает о том, как
сегодня защищена российская
доменная инфраструктура

с. 52

**Интернет-управление на
практике: невидимые
механизмы, которые держат Сеть**

За громкими дискуссиями
о свободе слова, цифровом
суверенитете и глобальной
политике нередко забывают
о технической составляющей
Интернета - а в этой области
сегодня называют важные
перемены

с. 74

**Знаки уходящего
телекома на чугуне**

Двухвековая история телекома -
у нас под ногами

с. 82

Содержание:

Интернет в цифрах	с. 2	Инфографика
Технология в деталях	с. 6	Тятя, тятя, наши сети притащили ВПО
	с. 18	Защита периметра цифровой безопасности в эпоху массового сканирования Сети
	с. 22	Эволюция фишинга: от примитивных писем к deerfake и целевым атакам
	с. 26	Самораспространение вредоносного программного обеспечения в локальной сети
	с. 32	Как искусственный интеллект влияет на ландшафт киберугроз и эволюцию инструментов для защиты от атак
	с. 36	Методы машинного обучения в обнаружении вредоносного ПО на разных типах платформ: защита ПК, мобильных устройств, устройств Интернета вещей и облачных сред
Инфраструктура	с. 46	Межоператорский бизнес в России в период массовых DDoS-атак
	с. 52	«Опасности и киберугрозы будут меняться вместе с технологиями». Интервью с Евгением Панковым
Образование и наука	с. 57	Анализ информации TLS-сертификатов оконечных узлов и меток времени (SCT) для российских логов Certificate Transparency
	с. 62	Специализированное in-методу хранилище информации о TLS-сертификатах и TLS-узлах с быстрым поиском
Технология и право	с. 68	Управление Интернетом — конец мультистейкхолдеризма?
	с. 74	Интернет-управление на практике: невидимые механизмы, которые держат Сеть
Вокруг технологии	с. 82	Знаки уходящего телекома на чугуне
Новости	с. 90	Новости науки и техники
	с. 92	Новости доменной индустрии

Сетевое издание
Журнал «Интернет изнутри»
info@internetinside.ru

Выпуск №23,
дата выхода:
Ноябрь 2025 г.

Свидетельство о регистрации
СМИ в Федеральной службе
по надзору в сфере
связи, информационных
технологий и массовых
коммуникаций.
Регистрационный номер:
ЭЛ № ФС 77 — 85232 от
25.04.2023 ISSN: 2949-1967

Все статьи размещаются
и индексируются
в НЭБ «e-Library»

Издатель: **Фонд развития
сетевых технологий
«ИнДата»**

Главный редактор:
Алексей Платонов

Выпускающий редактор:
Ирина Пыжова

Редакционная коллегия:
**Елена Воронина
Марат Биктимиров
Алексей Платонов**

Продакшн:
Алексей Гончаров

Дизайн и вёрстка:
Антон Иванов

Корректор:
Наталья Рябова

Обложка разработана
с использованием ресурсов
сайта Freepik.com

Зловреды в Интернете

Дорогой читатель,

Не секрет, что сложность решения многих проблем в Интернете, особенно связанных с безопасностью, связана с тем, что замечательные качества Сети — как, например, открытость и глобальная связность, — ценны как для полезной, так и для вредоносной деятельности. Открытая архитектура обеспечила впечатляющий рост Интернета и его приложений, а глобальная связность означает, что любой ресурс, подключённый к Сети, мгновенно становится её частью и может быть доступен всем пользователям. Но в то же время открытость позволяет вредоносам более свободно распространяться по Сети, а её глобальный охват означает, что жертвами зловредов могут стать кто угодно и где угодно.

Первая вредоносная программа появилась ещё до того, как термин «Интернет» вошёл в обиход. В 1971 году была разработана экспериментальная самовоспроизводящаяся программа Среерг, которая перемещалась между компьютерами в сети ARPANET, предшественнице современного Интернета. Хотя Среерг не была вредоносной в полном смысле этого слова, а была создана в исследовательских целях, её можно считать прототипом настоящих вредоносов, или вредоносного программного обеспечения (ВПО), которыми наводнена Сеть сегодня. Кстати, для поиска и удаления Среерг была создана программа Реарг, которая, по существу, стала первым антивирусным программным обеспечением.

В этом выпуске журнала мы поместили статьи, подробно рассматривающие составляющие этой экосистемы, механизмы работы и взаимодействия, а также тенденции её развития.

Сегодняшнее ВПО отличается большим разнообразием, способностью к адаптации и использованием новейших технологий, включая искусственный интеллект. За ВПО стоит многомиллиардный бизнес, правда, и борьба с ним является не менее внушительным бизнесом. Можно сказать, что с самых истоков Интернета ВПО и «анти-ВПО» развиваются рука об руку.

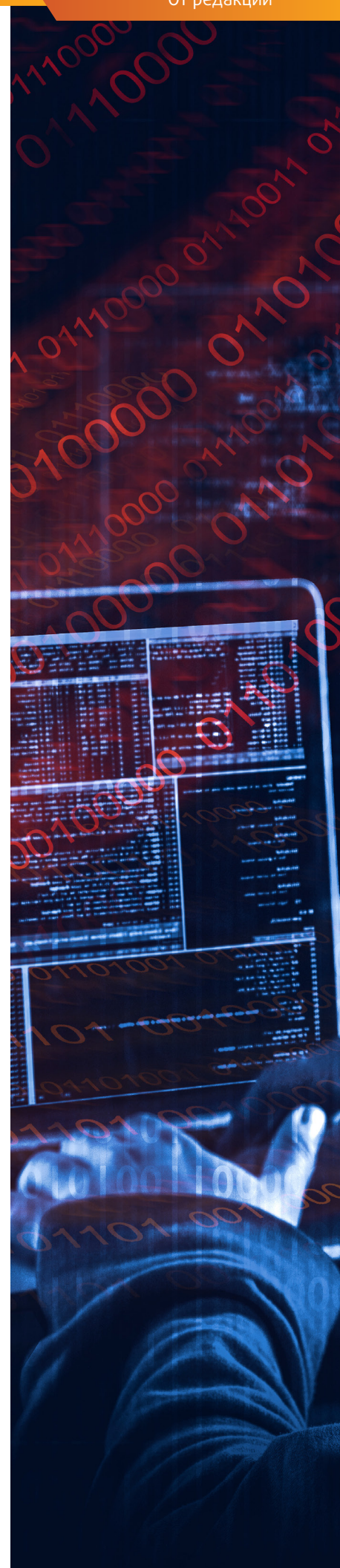
Открывает журнал статья Михаила Кадера и Алексея Сивенкова, в которой он обсуждает современное состояние этой «борьбы снаряда и брони» и тенденции развития как ВПО, так и средств защиты от него. За ней следует ряд интересных статей, рассматривающих различные аспекты ВПО и методы борьбы с ним.

Необычный взгляд на историю телекоммуникаций предлагает Алексей Кипчатов в статье «Знаки уходящего телекома на чугуне». За чугунами люками — артефактами этой почти двухвековой истории — спрятались интересные факты о развитии бизнеса и технологий связи в XIX-XX веках.

Конечно, мы продолжаем поддерживать наши стандартные разделы. В разделе «Образование и наука» вы найдёте специализированные исследования, связанные с сертификатами TLS. В разделе «Технология и право» вернёмся к теме управления в Интернете. А в «Новостях» мы познакомим вас с самыми значимыми событиями последних месяцев в мире Интернета и доменной индустрии.

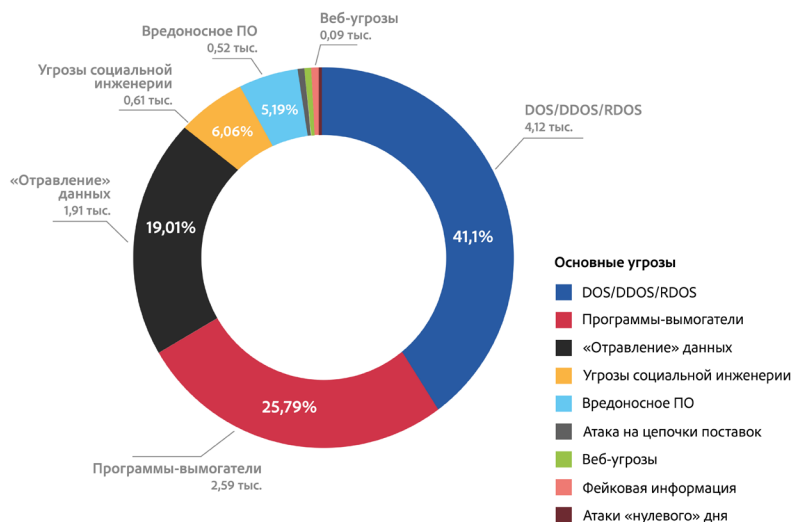
Как всегда, нам очень интересно и важно знать ваше мнение. Что понравилось и что можно улучшить? Какие темы вы хотели бы увидеть в следующих выпусках? Пишите нам по адресу info@internetinside.ru.

Редакция журнала ■



Распределение инцидентов по типам угроз (с июля 2023 по июнь 2024)

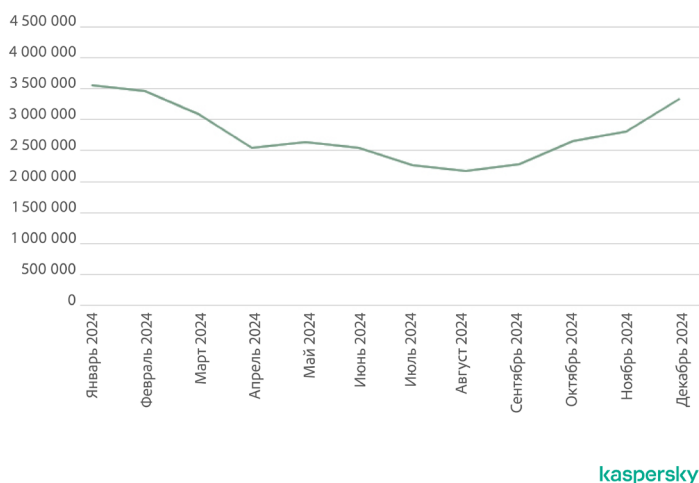
Согласно отчёту ENISA Threat Landscape за период 2023-2024 гг. программы-вымогатели и DDoS-атаки оказались наиболее часто регистрируемыми типами атак и суммарно составили более половины зафиксированных инцидентов. За ними по частоте выявления последовали угрозы, связанные с данными. В некоторых случаях инциденты были связаны с более чем одной категорией угроз и, таким образом, учитывались во всех проанализированных категориях. Принимая во внимание, что результаты исследования основывались на общедоступной информации, которая не всегда точно отражает полную картину, в некоторых случаях выявленные инциденты оказалось невозможным отнести к какой-либо конкретной категории угроз.



Источник: ENISA THREAT LANDSCAPE 2024, https://securitydelta.nl/media/corn_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf

Количество атак на пользователей мобильных решений «Лаборатории Касперского» в 2024 году

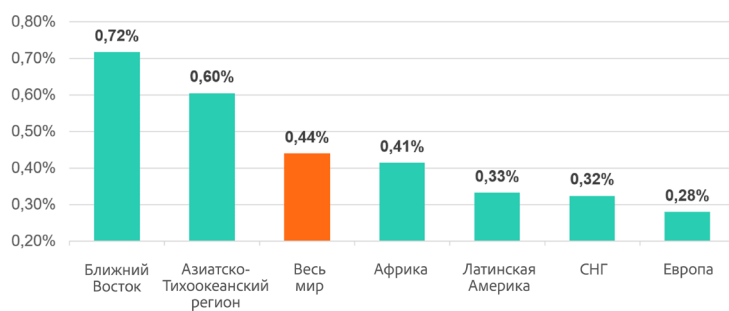
В 2024 году в среднем в месяц злоумышленники совершали около 2,8 миллиона атак на мобильные устройства с использованием вредоносного, рекламного или нежелательного ПО. Всего продукты «Лаборатории Касперского» предотвратили 33 265 112 атак за год. Самой распространённой угрозой для мобильных устройств стало рекламное ПО — 35% от всех выявленных угроз. Было обнаружено 1,1 миллиона вредоносных и потенциально нежелательных установочных пакетов, из которых почти 69 тысяч относились к мобильным банковским троянцам.



Источник: SECURELIST by Kaspersky. Мобильная вирусология 2024
<https://securelist.ru/mobile-threat-report-2024/111730/>

Доля пользователей, подвергшихся атакам программ-вымогателей (по регионам)

По данным Kaspersky Security Network, регионы Ближнего Востока, Азиатско-Тихоокеанского региона и Африки лидируют по доле пользователей, атакованных программами-вымогателями, за ними следуют Латинская Америка, СНГ (Содружество Независимых Государств) и Европа. В период с 2023 по 2024 год доля пользователей, пострадавших от атак программ-вымогателей, в среднем во всём мире увеличилась до 0,44%. Этот кажущийся небольшим процент типичен для программ-вымогателей и объясняется тем, что злоумышленники редко используют этот тип вредоносного ПО в массовом порядке, а в основном отдают предпочтение атакам на конкретные наиболее важные цели, что и сказывается на размере его доли относительно общего количества атак на пользователей.

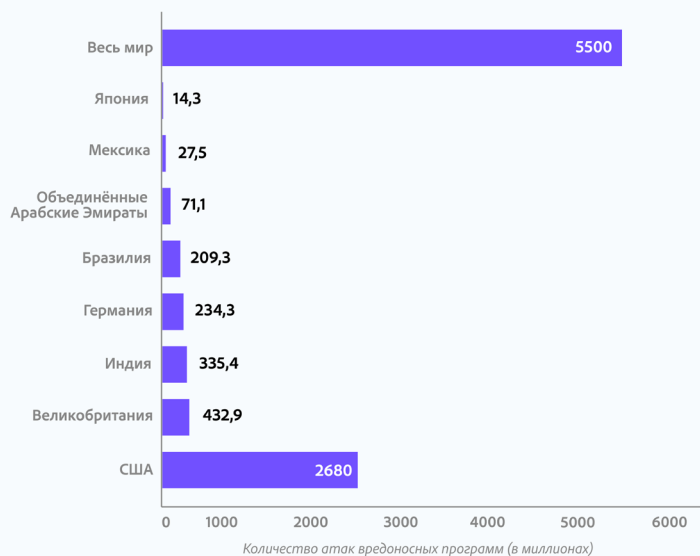


Data from Kaspersky Security Network

Источник: Kaspersky State of Ransomware Report-2025: Global and Regional Insights for International Anti-Ransomware Day, <https://www.kaspersky.com/about/press-releases/kaspersky-state-of-ransomware-report-2025-global-and-regional-insights-for-international-anti-ransomware-day>

Объём вредоносных атак в разбивке по странам

США являются страной, наиболее часто подвергающейся атакам вредоносных программ. В 2022 году на США было совершено около 2,7 миллиарда атак вредоносных программ из примерно 5,5 миллиардов атак по всему миру. Северная Америка остаётся регионом, наиболее часто подвергающимся атакам вредоносных программ. Однако в 2022 году количество атак снизилось на 10% в годовом исчислении – до 2,75 миллиарда, что является самым низким показателем в регионе с 2017 года. В 2022 году в Европе, Латинской Америке и Азии было зафиксировано двузначное увеличение количества атак вредоносных программ – на 10%, 17% и 38% соответственно.



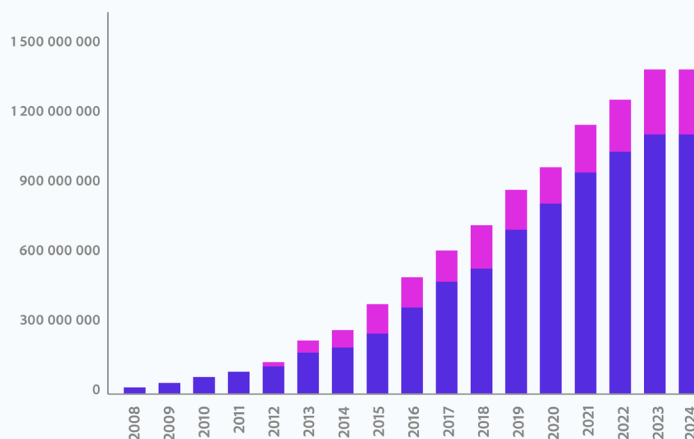
Количество атак вредоносных программ (в миллионах)

Источник: Malware Statistics for 2025, <https://www.stationx.net/malware-statistics/>

Общее количество вредоносных программ и потенциально нежелательных приложений (по годам)

В настоящее время существует около 1,2 миллиарда вредоносных программ и потенциально нежелательных приложений (PUA). С помощью AV-тестирования было выявлено более 100 миллионов разновидностей вредоносных программ и PUA-вирусов. Самым активным годом для появления новых разновидностей вредоносных программ был 2021 год, когда было выявлено около 150 миллионов новых программ. В прошлом году злоумышленники развёртывали в среднем 200 454 уникальных вредоносных скриптов в день, или примерно 1,5 новых образца в минуту.

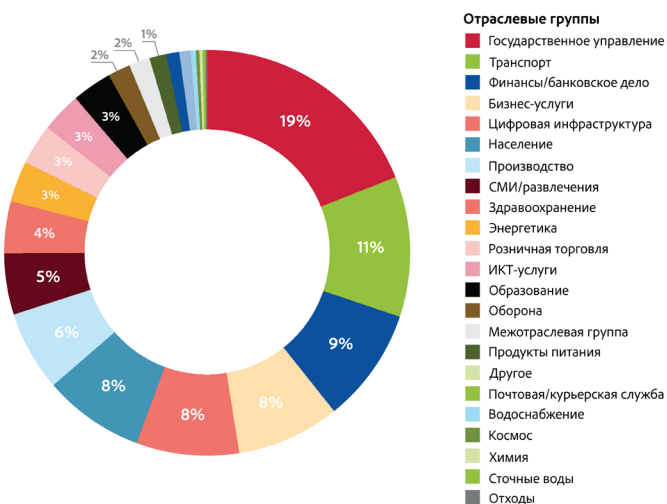
■ Вредоносная программа
■ Потенциально нежелательные приложения (PUA)



Источник: Malware Statistics for 2025, <https://www.stationx.net/malware-statistics/>

Распределение инцидентов по секторам экономики (июль 2023 – июнь 2024)

Киберугрозы носят всеобъемлющий характер, затрагивая широкий спектр отраслей и секторов экономики. Это является прямым следствием высокой степени цифровой взаимосвязанности в современном мире. Представленная диаграмма показывает, что злоумышленники атакуют практически все отрасли, что подчёркивает универсальность существующих киберрисков. На глобальном уровне зафиксировано значительное количество инцидентов, нацеленных на организации государственного управления, транспортного сектора и финансовой сферы. Существенную долю инцидентов составили атаки на цифровую инфраструктуру и на предприятия, относящиеся к сектору бизнес-услуг. Также отмечено значительное количество атак, направленных на население и не относящихся к какому-либо конкретному сектору экономики. К ним в том числе относятся инциденты, связанные с социальной инженерией.



Источник: ENISA THREAT LANDSCAPE 2024, https://securitydelta.nl/media/com_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf

СТАНЬТЕ ЧАСТЬЮ КРУПНЕЙШЕГО В РОССИИ СООБЩЕСТВА INTERNET EXCHANGE



Прямой доступ к интернет-аудитории,
контенту и сервисам Рунета



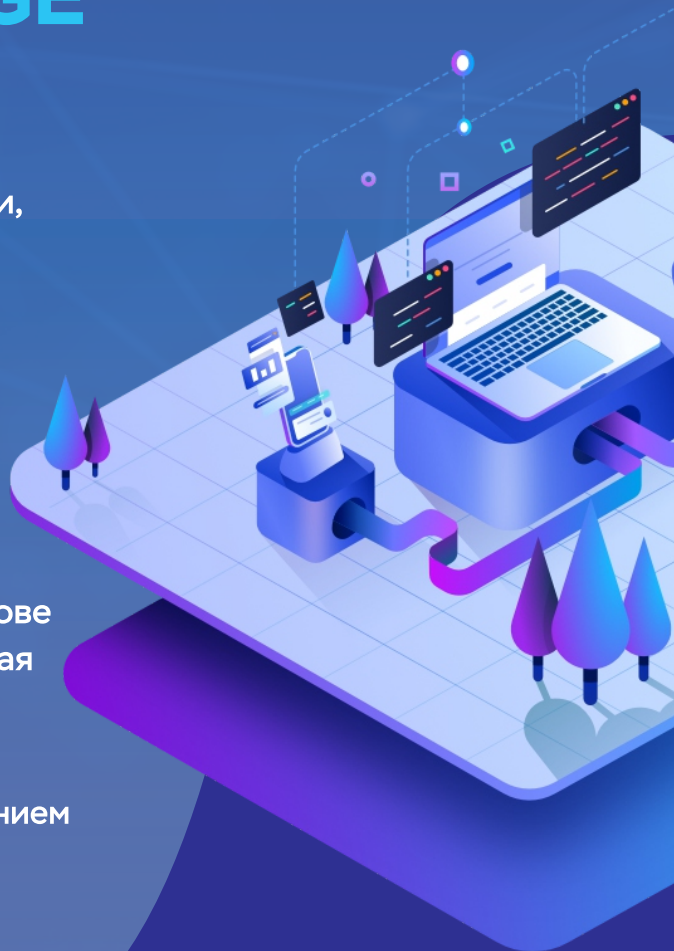
Прямое подключение в 10 городах
России или в любом городе через
партнеров



Многоуровневая архитектура на основе
дублированных ядер, обеспечивающая
полноценное резервирование



Синхронизация времени с использованием
NTP-сервера MSK-IX (Stratum I)



+7 495 737-92-95
msk-ix.ru



Тятя, тятя, наши сети притащили ВПО

Михаил Кадер
Алексей Сивенков



Аннотация

Вредоносное программное обеспечение (ВПО) и способы противодействия ему имеют давнюю историю. С момента появления первых вирусов и до сегодняшних дней ВПО постоянно совершенствовалось — от незатейливых червей и вирусов до сложных, многокомпонентных и масштабных систем, создаваемых при помощи искусственного интеллекта. Параллельно развивались и средства защиты от ВПО, пройдя путь от простых антивирусов с сигнатурным анализом до сложных, многофункциональных систем защиты от продвинутых кибератак. Постоянная борьба снаряда и брони никогда не закончится, так давайте же посмотрим на современное состояние ВПО, средств защиты от ВПО и тенденций развития — как ВПО, так и средств защиты от него.

Ключевые слова:

Malware, ВПО, искусственный интеллект, botnet, антивирус, sandbox, EDR.

Malware или ВПО — вредоносное программное обеспечение.

ИИ — искусственный интеллект.

Botnet — управляемая злоумышленником сеть заражённых машин.

Обфускация (запутывание) кода — процесс намеренного изменения программного кода для запутывания

исследователей программного обеспечения с целью сокрытия истинных целей работы программы с сохранением функционала работы программы.

Антивирус — программное обеспечение, предназначенное для обнаружения, предотвращения вредоносного действия и удаления вредоносного программного обеспечения.

Sandbox или песочница — устройство контролируемого запуска и анализа программного обеспечения.

EDR (Endpoint Detection and Response) — средство обнаружения и реагирования на целевые, сложные и длительные кибератаки на конечных точках (рабочих станциях, серверах, мобильных устройствах).

Введение

Хотелось бы начать эту статью с истории. На заре этого века группа экспертов сидела в офисе АДЭ (Ассоциации документальной электросвязи) и работала над документом, который потом стал называться «Базовый уровень информационной безопасности операторов связи». Кстати, интересно то, что этот документ в 2007 году был одобрен на уровне МСЭ-Т (Международного союза электросвязи), также известном как ITU-T, в рамках работы ИК-17. И вот в процессе работы этой группы возник вопрос, а как называть это самое пресловутое «вредоносное программное обеспечение». Представитель одной уважаемой организации предложил всё ВПО называть просто словом «вирус», но часть остальных экспертов почувствовала подвох. Ведь если всё назвать «вирусом», то люди будут наивно думать, что «антивирус» — это средство от всех болезней. Так что предложение не прошло, и термин ВПО вошёл и в этот документ. И одной из причин несогласия с коллегой было именно то, что уже тогда термин ВПО охватывал множество разных вариантов вредоносных. Подробнее об их классификации и отличительных признаках мы поговорим чуть позже. А сейчас можем вернуться к базовым определениям.

Давайте быстро пробежимся по основам и вспомним, что классическое определение обеспечения информационной безопасности говорит о триумвирате «конфиденциальность», «целостность», «доступность». Нарушить его могут, по сути дела, два широких класса угроз — атаки типа «отказ в обслуживании», направленные против «доступности», и атаки типа НСД (несанкционированный доступ к данным), направленные против «конфиденциальности» и «целостности».

При этом современный мир гораздо разнообразнее наших классических определений. Давайте рассмотрим два практических момента. Первый из них напоминает детскую считалочку для запоминания цветов радуги: «Каждый Охотник Желает Знать, Где Сидит Фазан». И вот сейчас таким фазаном является любое устройство, любым образом подключённое в сеть. Неважно, компьютер это или смартфон, умный телевизор, колонка или датчик системы управления умным домом. И охотниками тоже являются все, начиная от браузеров и заканчивая агентами ИИ. Конечно же, все эти охотники преследуют разные цели. Поэтому, если мы говорим о сборе данных, таких как «где находится», «что хочет купить», «что искал в сети» и тому подобном, это является нарушением конфиденциальности, но не обязательно говорит о вредоносности использования. А вот когда охотники хотят узнать данные банковских карт, пароли, паспортные данные, получить доступ к содержимому нашей электронной почты, то в этом случае нарушение конфиденциальности представляет собой реальную угрозу. Точно так же, как нарушение целостности информации, например, уничтожение данных на рабочих местах и их резервных копий, шифрование информации с целью получения выкупа, манипуляция записями в базе данных — тоже примеры однозначно вредоносного воздействия. Второй обещанный практический момент — это то, что успешная атака типа «отказ в обслуживании» делает информационные системы или ряд связанных с ними активов просто недоступными для использования. Например, перестают работать определённые ресурсы в Интернете, мобиль-

ные приложения банков и тому подобное. В этом случае уже не так важно, что сами данные не пострадали, так как проку от них в этом моменте времени просто ноль.

Почему же мы написали, что современная жизнь многообразнее? Чтобы лучше ответить на этот вопрос, давайте попробуем дать ответ на другой вопрос — как проще всего нанести ущерб? Очевидно, что нужно оказаться в том месте, где расположена интересующая злоумышленника информация, или откуда к ней может быть доступ. То есть задача номер один — это осуществить взлом ряда систем для проникновения в них. После этого можно делать с данными всё что угодно. Теперь давайте очень быстро посмотрим на структуру современного ВПО. Многочисленные исследования подтверждают, что рынок ВПО, включая его разработку, продажу и сопровождение, огромен! Некоторые сравнивают его по размеру с общим рынком разработки легитимного ПО. При этом он эволюционирует гораздо стремительнее, по той причине, что защитники тоже не дремлют и постоянно разрабатывают новые средства для идентификации и противодействия атакам с использованием ВПО.

Но вернёмся назад к структуре. Современное ВПО является модульным и централизованно управляемым. В качестве его основных компонентов можно выделить модуль проникновения на устройство, например, рабочее место пользователя или умный домашний телевизор. В том случае, если это просто устройство, проникновение обычно происходит через уязвимости, присутствующие в системном или прикладном ПО. Если же это устройство, за которым сидит человек, то задача упрощается — в дополнение к различным уязвимостям начинают работать и «человеческие факторы», такие как доверчивость, безалаберность, любопытство и прочие. Ими как раз и пользуются злоумышленники для распространения ВПО, например, через фишинг в электронной почте, социальные сети, мессенджеры и прочее. Потом это ВПО пытается закрепиться на устройстве — подменяет файлы, пишет себя в реестр и т.п.



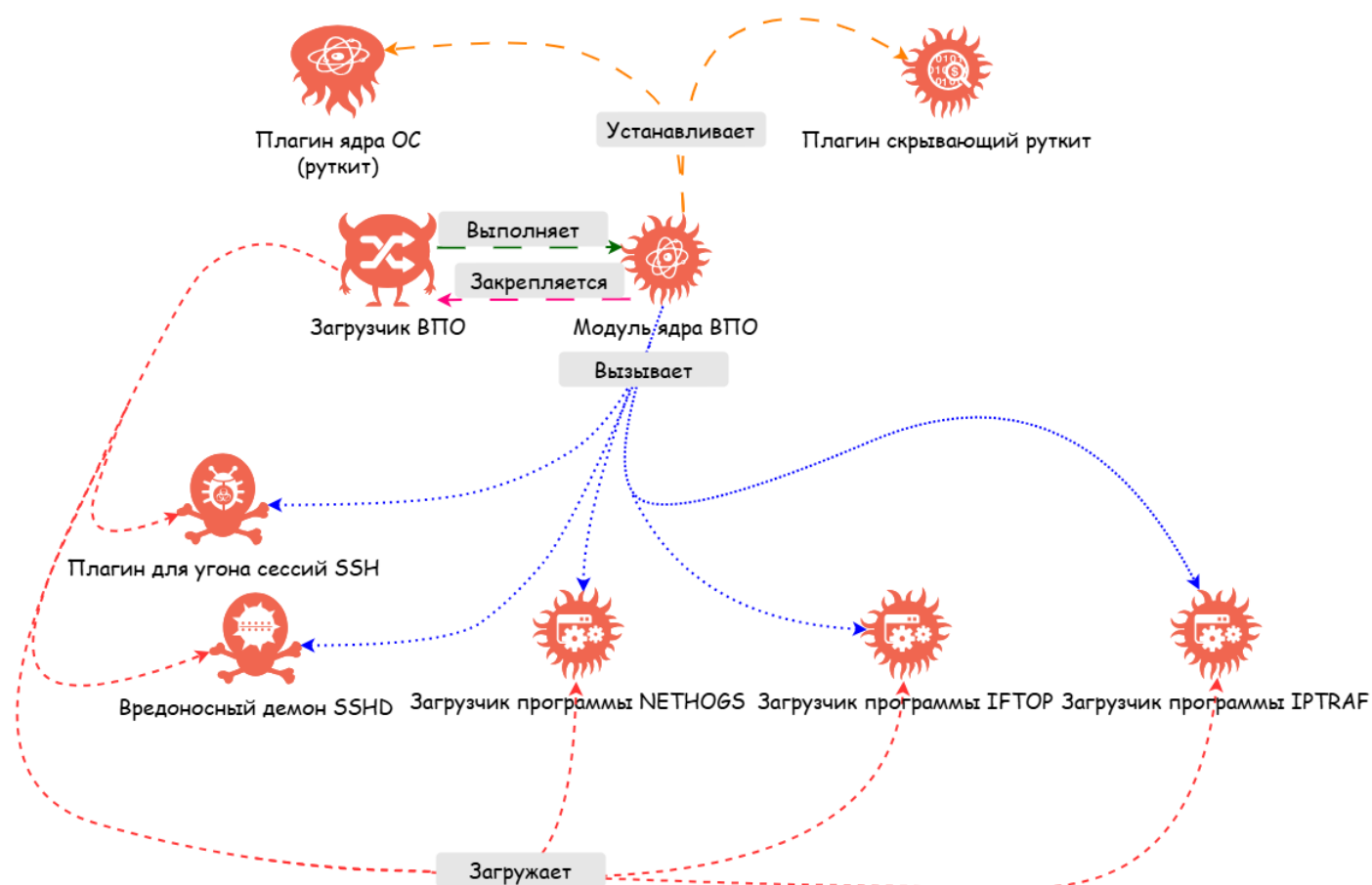


Рис. 1. Модульная архитектура ВПО.

Следующая стадия — установление связи с центром управления, а то и с распределённой сетью управления. Причём и тут ВПО непрерывно эволюционирует. От собственных центров управления и использования простых протоколов злоумышленники перешли к использованию службы имён DNS, зашифрованным каналам, размещению центров управления у глобальных облачных операторов и многому другому. А дальше в дело вступает процесс получения модуля нанесения ущерба от этого самого центра управления, а потом и модуль дальнейшего распространения по другим узлам. Модуль нанесения ущерба может быть разным и поставляется на устройство в зависимости от задачи. Например, в данный момент злоумышленник хочет собрать максимум информации, включая файлы, пароли, записи экрана и тому подобное. Потом он, например, планирует зашифровать данные и запросить выкуп, после чего решает уничтожить всё, максимально скрыв свои следы. И на самом деле, возможны любые комбинации вредоносного воздействия. Обратите внимание, что мы много раз упоминаем слово «модуль» — именно потому, что современное ВПО имеет модульную структуру и позволяет легко сочетать и комбинировать все свои компоненты. Это и делает его настолько эффективным, регулярно обходящим самые современные механизмы защиты, и человек ему в этом в помощь.

Всё, что вы знали или не знали о различных видах malware (классификация и отличительные признаки различного ВПО)

Давайте посмотрим на модули ВПО, те самые атомарные единицы, из которых может состоять ВПО.

Компьютерный вирус

Древнейшим представителем ВПО является известный практически всем компьютерный вирус. Компьютерный вирус — это самореплицирующаяся программа, которая прикрепляет саму себя к другим исполняемым файлам или программам для своего размножения. Компьютерному вирусу требуется участие пользователя для активации, так как он не умеет самостоятельно реплицировать сам себя или самостоятельно действовать, в отличие от других классов ВПО. Но после активации (заражения) компьютерный вирус способен внедрять свой код в другие программы, создавая в них свои копии для дальнейшего распространения. Компьютерный вирус обычно имеет небольшой размер, так как чаще всего содержит лишь код, который был разработан для нанесения вреда, ради которого он и был создан. Немаловажной особенностью компьютерного вируса является то, что ему нужен объект для заражения и, как уже было сказано выше, это исполняемый файл или программа, или документ.

Для затруднения своей нейтрализации компьютерные вирусы используют различные техники и методы сокрытия, которые затрудняют их обнаружение антивирусным программным обеспечением. Эти техники и методы сокрытия включают в себя:

- изменение своего кода при каждом инфицировании, чтобы избежать обнаружения при помощи сигнатурного анализа антивирусным ПО;
- шифрование собственного кода для затруднения анализа такого кода и выявления шаблонов обнаружения;
- маскировку себя под легитимный процесс или файл в операционной системе, что может позволить компьютерному вирусу избежать обнаружения при помощи поведенческого анализа;
- обфускацию кода для усложнения его чтения и анализа как человеком, так и антивирусным ПО.

Необходимость активации компьютерного вируса человеком и зависимость его от объекта заражения — файла — диктуют основные способы распространения компьютерных вирусов:

- при помощи загрузки и запуска компьютерного вируса из сети, чаще всего сети Интернет;
- при помощи открытия заражённого вложения в сообщении электронной почты или сообщении мессенджера;
- при помощи запуска компьютерного вируса с внешнего носителя данных, такого как USB-флешка.

Как и его биологический аналог, вирус, компьютерный вирус может причинить разнообразный вред отдельной машине и в компьютерной сети. В частности, он может:

- удалить или повредить данные;
- сделать работу машины нестабильной;
- вызвать деградацию производительности машины или компьютерной сети, в которой находится заражённая машина;
- украсть персональные или конфиденциальные данные;
- вызвать повреждение аппаратного обеспечения машины.

Компьютерный червь

Следующим, не менее древним представителем ВПО является компьютерный червь. Основное отличие компьютерного червя от вируса — возможность самостоятельного размножения в компьютерных сетях без какого-либо участия человека или программы, установленной на физической или виртуальной машине. Компьютерные черви используют уязвимости в программном обеспечении операционной системы и её приложений для своего распространения и инфицирования ещё не заражённых машин. Компьютерные черви могут стремительно распространяться по сети и быстро инфицировать незаражённые машины. Возможности самостоятельного и быстрого распространения делают компьютерного червя хорошим кандидатом на распространение и доставку на заражённые машины другого ВПО. И позволяют быстро интегрировать заражённые компьютерным червём машины в управляемую злоумышленником сеть — ботнет.

Первоначальные каналы заражения компьютерным червём совпадают с вышеперечисленными способами для активации компьютерного вируса.

Для затруднения своего обнаружения и последующей нейтрализации компьютерные черви могут изменять свой код и поведение, чтобы избежать сигнатурного или поведенческого анализа, и могут использовать шифрование и обфускацию кода для затруднения обнаружения и анализа как человеком, так и средствами антивирусной защиты.

Быстрое заражение множества машин в сети компании компьютерным червём может привести к:

- значительному потреблению ресурсов заражённых машин и сети компании;
- краже персональной и корпоративной информации, чувствительных данных;
- повреждению и/или удалению файлов и данных;
- созданию зазоров в безопасности компании при помощи создания чёрных ходов;
- вовлечению множества машин компании в ботнет, который будет использоваться для злонамеренных целей;
- установке другого ВПО на машины компании.

«Троянский конь»

Ещё одним представителем ВПО является «троянский конь», который ведёт себя, как и его исторический прототип, благодаря которому грекам удалось взять неприступную Трою. Скрывая свою истинную сущность, троянский конь маскируется под легитимное программное обеспечение или безвредный файл и использует свои возможности мимикрии для обмана пользователей, чтобы побудить их установить троянского коня на свою машину. В отличие от компьютерных вирусов и червей, троянский конь самостоятельно не реплицируется, вместо этого для своего распространения он использует взаимодействие с пользователем, в том числе и при помощи методов социальной инженерии, побуждая пользователя установить троянского коня на свою машину. В процессе установки троянец активирует свои вредоносные функции без взаимодействия с пользователем.

Для защиты от обнаружения средствами антивирусной защиты троянский конь может:

- использовать техники перехвата и изменения функций операционной системы для эффективного сокрытия инфицированного файла или программы от пользователя и/или антивирусного ПО;
- изменять свой код при каждом новом инфицировании, чтобы затруднить обнаружение при помощи сигнатурного анализа;
- шифровать или обфусцировать свой код для затруднения обнаружения или анализа человеком или антивирусным ПО;
- встраивать себя в существующие процессы операционной системы, чтобы спрятать себя, слившись с обычной активностью ОС.

А основными способами распространения троянского коня являются:

- передача во вложениях электронной почты и мессенджеров;
- загрузка с фишинговых ресурсов и других ресурсов в Интернете;
- запуск с переносных носителей данных.

И — как и его исторический прототип — компьютерный троянский конь может привести к:

- краже данных;
- повреждению файлов;
- получению контроля над заражённой машиной;
- созданию чёрного хода для обхода систем информационной безопасности компании;
- установке другого ВПО на заражённую машину.

Шифровальщик

Широко распространённый в последние годы тип ВПО. Чаще всего используется для предотвращения доступа пользователей к их данным или машинам при помощи шифрования данных и/или операционных систем целиком, часто с последующим запросом на перевод значительных денежных средств злоумышленнику за расшифровку зашифрованных данных. Пострадавшим пользователям обычно предоставляются инструкции по оплате за расшифровку, часто — для сокрытия следов — в криптовалюте, в обмен на ключ для расшифровки данных. Выплата денег за получение ключа для расшифровки данных очень часто не даёт никакой гарантии на то, что зашифрованные данные будут корректно восстановлены. Скорость и сложность современных методов шифрования затрудняет обнаружение шифровальщиков в течение основной, самой критичной фазы атаки — самого шифрования данных.

Для защиты от обнаружения средствами антивирусной защиты шифровальщик может использовать следующие методы:

- обфускация и переупаковка кода, добавление бессмысленного кода, шифрование собственного кода, чтобы сделать свой код нечитаемым и непонятным для вирусных аналитиков и антивирусного программного обеспечения;
- шифрование данных небольшими частями в течение длительного времени для затруднения обнаружения;
- использование техник внедрения в ядро операционной системы для сокрытия своего наличия в системе путём сокрытия процессов шифрования из списка процессов ОС или же с помощью маскировки процессов шифрования под легитимный, доверенный процесс;
- отключение антивирусной защиты до момента обнаружения шифровальщика.

Чаще всего шифровальщик распространяется при помощи скачивания его с фишинговых или скомпрометированных сайтов в Интернете или через вложения, в том числе и в виде ссылок в сообщениях электронной почты или мессенджеров.

Шпионское ПО

Шпионское программное обеспечение, проникающее на машину для тайного сбора чувствительных данных, таких как учётные записи и пароли, персональных и конфиденциальных данных, для отслеживания пользовательской активности при использовании браузера, создания скриншотов и записи экрана компьютера, записи нажатия клавиш клавиатуры (такой тип ВПО часто выносится в отдельный класс ВПО — клавиатурный шпион), а также для установки другого ВПО.

Для распространения шпионское программное обеспечение часто упаковывается вместе с инсталлятором легитимного ПО, появляясь при установке как дополнительный компонент программы, безопасное вложение или инсталлятор другой программы для установки и часто устанавливаясь без участия пользователя. Также другими каналами распространения шпионского ПО могут являться:

- фишинговые или злонамеренно созданные сайты со ссылками на скачивание легитимного программного обеспечения;
- вложения или ссылки в сообщениях электронной почты или мессенджерах.

А для защиты от обнаружения шпионское ПО может использовать следующие методы:

- скрытое выполнение своих операций: шпионское ПО часто работает в фоне, избегая любых видимых признаков своего присутствия в системе;
- сокрытие в легитимных приложениях, которые скачиваются с неофициальных ресурсов распространения программного обеспечения;
- маскировка под легитимное ПО;
- использование техник внедрения в ядро операционной системы для сокрытия своего присутствия в ОС;
- отключение средств защиты информации, чтобы гарантировать непрерывность своей работы и предотвратить своё обнаружение.

Мошенническое ПО

Мошенническое программное обеспечение маскируется под легитимные приложения, часто под программы — средства защиты информации, чтобы обманом заставить пользователей платить за несуществующие услуги или за угрозу раскрытия персональной информации. Мошенническое ПО часто выдаёт себя за антивирус или системную утилиту, пугает пользователя «обнаруженными угрозами» и требует оплаты за «лечение».

Помимо этого, мошенническое программное обеспечение может привести к:

- краже чувствительной и конфиденциальной информации, персональных данных;
- деградации производительности системы;
- установке другого ВПО.

Для защиты от обнаружения мошенническое ПО может использовать:

- обфускацию, переупаковку и шифрование собственного кода для затруднения обнаружения и анализа вирусными аналитиками и антивирусным ПО;
- изменение конфигурации системы для предотвращения удаления или отключения мошеннического ПО;
- использование техник сокрытия своего процесса в списке процессов операционной системы.

Rootkit

Руткит — один из самых опасных видов ВПО, который предназначен для предоставления атакующему удалённого управления атакованной системой или устройством путём предоставления ему привилегированного доступа и сокрытия его активности в системе. Руткит достигает этих целей путём модификации компонентов ядра операционной системы, делая невероятно трудным своё обнаружение и удаление.

Руткиты часто устанавливаются как часть другого, легитимного программного обеспечения, используя уязвимости в ПО, а также техники фишинга и социальной инженерии, которые принуждают пользователя к установке ПО в режиме использования повышенных привилегий пользователя (административный или root-доступ).

После установки в операционной системе руткит может использоваться для:

- обеспечения атакующему скрытого удалённого доступа к атакованной системе;
- установки и сокрытия другого ВПО;
- вовлечения машины в управляемую сеть зараженных машин — ботнет;
- кражи чувствительных, персональных, финансовых, конфиденциальных данных;
- отключения или обхода средств защиты информации в атакованной системе.

Руткит является одним из наиболее трудно определяемых и одним из наиболее опасных типов ВПО, т.к. он работает на уровне ядра операционной системы и может вмешиваться и изменять работу не только прикладного программного обеспечения, но и самой ОС и установленных в ней средств защиты информации при помощи перехвата и модификации вызовов Application Programming Interface (API), инструкции которых используются для взаимодействия прикладного ПО с операционной системой. А также при помощи прямой манипуляции объектами ядра, изменяя внутренние структуры ядра, что позволяет обойти списки контроля доступа и предоставить неавторизованный доступ к ресурсам.

Backdoor

«Чёрный ход», или backdoor — это вид ВПО, который создаёт скрытую точку доступа к машине, программному обеспечению или сети, обходя обычную аутентификацию и меры

защиты, разрешая пользователю неавторизованный доступ с повышенными привилегиями или даже с правами администратора или root-правами (т.н. суперпользователь). Backdoor может быть намеренно оставлен разработчиками программного приложения, случайно создан из-за наличия уязвимости, но чаще всего он устанавливается атакующими после компрометации системы для неавторизованного доступа и закрепления в системе.

При помощи backdoor атакующий может осуществить:

- кражу чувствительных данных, таких как учётные записи и пароли;
- кражу конфиденциальной и персональной информации;
- установку другого ВПО;
- дальнейшую компрометацию системы при помощи манипуляции настройками системы, отключением и удалением компонентов и файлов системы.

Для защиты от обнаружения backdoor может использовать:

- установку другого ВПО, такого как rootkit, для сокрытия своего присутствия в операционной системе;
- обфускацию и шифрование кода, а также маскировку под легитимные системные файлы или процессы;
- зашифрованные каналы передачи данных между атакующим и скомпрометированной системой для слияния с обычными сетевыми соединениями;
- соединение с легитимными платформами в сети Интернет для отправки команд и инструкций, пряча свои действия среди обычной пользовательской активности;
- удаление логов и изменение конфигурации системы для сокрытия своей активности и затруднения обнаружения компрометации системы;
- внедрение в цепочку поставок на уровне производства аппаратного или программного обеспечения, чтобы стать частью доверенных компонентов и сделать свое обнаружение максимально сложным.

Dropper

Ещё один тип ВПО — dropper («разносчик»), который используется для доставки ВПО на устройство-жертву. За счёт использования различных способов доставки, таких как вложение в сообщении электронной почты или мессенджера, скачивание с скомпрометированных сайтов или поставки в составе доверенного ПО, dropper, будучи установленным в систему без всякого взаимодействия с пользователем, начинает загружать на устройство-жертву различное ВПО по сценарию атакующего. Использование dropper для доставки ВПО на устройство-жертву затрудняет обнаружение ВПО на скомпрометированной машине, т.к. сам dropper обычно не вредоносен и чаще всего используется только для доставки ВПО, а не для выполнения какого-то деструктивного воздействия, что затрудняет его обнаружение. Для закрепления в атакованной системе dropper использует создание ключей реестра и/или задач в планировщике задач для своей повторной установки после перезагрузки системы. После установки dropper загружает основной вредоносный модуль, а затем часто самоуничтожается.

Для затруднения обнаружения dropper использует:

- шифрование или обфускацию своего кода;
- выполнение своего кода в памяти вместо своего сохранения на диске;
- запуск и выполнение при старте операционной системы до запуска средств защиты информации.

Bootkit

Bootkit — это тип ВПО, который инфицирует загрузчик или

Как мы можем видеть, различные типы ВПО используют похожие техники сокрытия своего присутствия в скомпрометированной системе. Часто один тип ВПО используется для доставки другого или для взаимодействия с ним с целью расширения возможностей атакующего — как на уровне скомпрометированной системы, так и на уровне распространения своего влияния на другие системы, с целью их захвата и объединения в сеть управляемых злоумышленником ресурсов — botnet.

В живой природе нам могут встретиться перечисленные виды ВПО — как в чистом виде, так и в виде симбиоза различных



другие предзагрузочные компоненты, такие как главная загрузочная запись (Master Boot Record) или Unified Extensible Firmware Interface, выполняющиеся до загрузки операционной системы. Это делается для обхода средств защиты информации уровня ОС и/или уровня приложений. Даёт атакующему постоянный контроль над атакованной системой и позволяет ему оставаться незамеченным.

Чаще всего bootkit устанавливается в систему с использованием внешнего носителя.

При помощи bootkit атакующий может:

- загружать на скомпрометированную систему другое ВПО;
- отключать или модифицировать средства защиты информации;
- красть конфиденциальную и персональную информацию.

Но основной функцией bootkit является обеспечение скрытого постоянного доступа к скомпрометированной системе, который продолжит функционировать даже после замены дисков или переустановки операционной системы, делая своё обнаружение и удаление достаточно трудным. Его главное преимущество — устойчивость: он выживает даже после переустановки ОС или замены диска.

видов ВПО, собранного в виде набора либо вредоносных фреймворков с различным функционалом, либо атомарных микрофункций вредоносного инструментария атакующего, что и в том, и в другом случае предоставляет атакующему различные техники и тактики атак.

Давайте попробуем взглянуть на некоторые образцы ВПО, которые могут нам встретиться в «дикой природе».

Ах, какой «красавец», какой образец!
(некоторые примеры часто встречающегося в настоящее время ВПО в живой природе)

Ранее мы разобрали основные типы ВПО. Но какие шансы встретить определённый тип ВПО в реальной жизни? Какие типы ВПО чаще всего встречались пользователям ранее? А какие чаще встречаются сейчас?

С одной стороны, технологии создания ВПО, как и технологии создания другого программного обеспечения, развиваются стремительно. Можно смело говорить, что искусственный интеллект уже не просто делает первые шаги, а используется

как один из инструментов для достижения целей атакующего, расширяя и автоматизируя кибератаки, делая их более сложными, персонифицированными и более трудными для обнаружения. Искусственный интеллект сегодня применяется для создания более убедительных персональных голосовых и видеодипфейков для использования в сценариях социальной инженерии, генерации фишинговых страниц и писем, более таргетированных и реальных, заточенных под определённого пользователя или организацию, что повышает их шансы пройти антифишинговую защиту и убедить пользователя выполнить действия, необходимые злоумышленнику. В то же время ИИ

пользуют одни и те же семейства и типы ВПО. Мы можем зайти на страницу компании ANY.RUN со статистикой наиболее часто используемых образцов ВПО [1] и увидим, что в числе 15 наиболее используемых семейств ВПО за прошедшие 365 дней будут следующие:

- Тусоон 2FA (набор для фишинга);
- Lumma (ВПО для кражи информации);
- EvilProxy (набор для фишинга);
- XWorm (троян);
- Mamba 2FA (набор для фишинга);



помогает создавать ВПО, которое динамически адаптируется к мерам безопасности, делая обнаружение более сложным. ИИ помогает анализировать огромные объёмы данных, находя в них интересующие атакующего зависимости и уязвимости по отношению к исследуемым им сетям и/или системам. Благодаря ИИ мошенникам удаётся лучше взаимодействовать с потенциальными жертвами, собирая у них в режиме реального времени персональную и конфиденциальную информацию, чтобы обеспечивать и поддерживать более точные и стратегически масштабные атаки. ИИ помогает ещё существеннее снизить порог входа и увеличить скорость выхода на «рынок» киберкриминала различных типов ВПО, создавая новые образцы ВПО. Естественно, злоумышленники используют не общедоступные модели искусственного интеллекта, а специальные модели со снятыми ограничениями по безопасности, которые позволяют генерировать фишинговые материалы, инструкции к эксплуатации уязвимостей и само ВПО. Доступ к таким моделям предоставляется по сервисной модели на теневых форумах и каналах. Такие модели ИИ используются не только для создания ВПО, но и для сокрытия кода уже существующего ВПО, генерируя множество новых образцов ВПО и участвуя в целевых атаках как неотъемлемый элемент самого сценария атаки, с возможностью генерации кода ВПО или выполняемого им действия в реальном масштабе времени.

С другой стороны, если мы посмотрим на статистику трендов использования ВПО за текущий или более ранние годы, то мы увидим, что в большинстве случаев киберпреступники ис-

- AsyncRAT (троян с функцией удаленного доступа);
- Remcos (троян);
- Agent Tesla (троян);
- Amadey (ВПО для кражи информации);
- Stealc (ВПО для кражи информации);
- RedLine (ВПО для кражи информации);
- WannaCry (шифровальщик);
- Sneaky zFA (набор для фишинга);
- DCRat (троян с функцией удаленного доступа);
- Quasar RAT (троян с функцией удаленного доступа);
- Emotet (троян).

А вот список из наиболее используемого ВПО с того же ресурса за 2021 год:

- **Emotet;**
- Trickbot;
- Formbook;
- LokiBot;
- Qbot;
- NanoCore RAT;
- **RedLine;**
- **Agent Tesla;**
- **Quasar RAT;**
- **RemCosRAT;**
- **AsyncRAT;**
- STRRAT.

Повторяющиеся названия мы выделили цветом, и можно констатировать, что очень многие семейства ВПО присутствуют как в статистике за 2024-2025 год, так и в статистике за 2021 год.

Аналогичную картину дают и другие исследования. Например, в статистике по трендам ВПО от 21 августа 2025 года от компании Positive Technologies [2] приводятся следующие данные по наиболее часто встречающимся в России семействам ВПО:

- **Agent Tesla;**
- SnakeKeylogger;
- **FormBook;**
- SteganoLoader;
- **Emotet;**
- Remcon;
- Evilnum;
- LokiBot;
- Carbon;
- Prometei.

И в этой же статье мы можем видеть, что аналогичные семейства ВПО наблюдались и за 2023-2024 год. А основными способами заражения ВПО были электронная почта, компрометация рабочей станции и загрузка ВПО из Интернета.

Из этого можно сделать вывод, что несмотря на совершенствование технологий в создании ВПО, старые проверенные образцы ВПО не потеряли своей актуальности у злоумышленников и разработчиков ВПО, а использование различных методов сокрытия и модификации кода у уже много лет известных образцов ВПО, о которых мы говорили выше, позволяет малыми усилиями создавать большой объём новых экземпляров ВПО для обхода средств защиты информации, в особенности тех, что основаны на сигнатурном анализе образцов программного обеспечения.

До чего дошёл прогресс, вкалывают роботы, а рад ли человек? (ботнеты и их роль в распространении ВПО)

Ботнет — это сеть из подключённых к сети Интернет устройств, компьютеров, ноутбуков, планшетов, телефонов и устройств Интернета вещей (Internet of Things, IoT), инфицированных ВПО и удалённо управляемых злоумышленниками. Устройства, подключённые к ботнету, используются в скоординированных атаках на другие системы и сети, позволяя организовывать распределённые атаки отказа в обслуживании (Distributed Denial of Service, DDoS), рассылать фишинговые и спам-письма, красть чувствительную и конфиденциальную информацию с заражённых устройств, участвовать в распространении ВПО, использоваться в распределённых атаках по подбору учётных данных доступа к другим ресурсам в Интернете и использоваться в другой злонамеренной активности.

Классический ботнет состоит из командного центра, часто включающего в себя несколько устройств и управляемого злоумышленниками. Этот центр, в свою очередь, управляет сетью заражённых устройств. Такие ботнеты считаются построенными по централизованной модели. Но всё чаще применяются P2P-сети, где нет единой точки отказа — это делает ботнеты устойчивыми к блокировке. А захват правоохранителями инфраструктуры такого ботнета не даёт гарантии, что ботнет и его командный центр уничтожены, и позволяет ботнетам возрождаться вновь через некоторое время, почти как Фениксу из пепла.

Ботнеты используются злоумышленниками для автоматического распространения и установки ВПО, что может быть достигнуто при помощи автоматического поиска неисправленных уязвимостей на других системах. Это позволяет автоматизировать эксплуатацию найденных уязвимостей для получения доступа к новым устройствам-жертвам и автоматического распространения на них ВПО, необходимого злоумышленнику.

Автоматизация атак, широкий охват по количеству заражённых устройств и их территориальному распределению делают ботнет очень удобным инструментом для злоумышленников, позволяя быстро и эффективно заразить большое количество устройств без трудоёмкой ручной деятельности, что повышает эффективность атак и затрудняет обнаружение и нейтрализацию сетей атак и распространения ВПО, которыми и являются ботнеты.

Следует отметить, что для создания ботнета злоумышленнику уже давно не нужно подготавливать свой собственный инструментарий, так как готовый ботнет можно купить на тёмном рынке (dark web), и цены на данный товар не очень высоки, от нескольких сотен до нескольких тысяч в долларовом эквиваленте, а экономическая выгода от его использования может покрыть злоумышленнику эти расходы менее чем за месяц использования ботнета. Часто владельцы ботнетов используют механизмы сервисных продаж, предоставляя доступ к управлению ботнетом на некоторый период времени за умеренную плату, что ещё больше снижает порог входа и затраты для атакующих. Часто злоумышленнику вообще не нужно покупать или получать доступ к ботнету, ему достаточно арендовать его использование для распространения своего ВПО и/или организации атаки на какое-то время, и это тоже уменьшает издержки злоумышленников и повышает доходность от атак.

«Тенденция, однако» (ботнеты и ВПО, взгляд в будущее)

Кратко рассмотрев основные виды ВПО и его взаимодействие с ботнетами для осуществления злонамеренной деятельности, можно сделать некоторый прогноз на ближайшее будущее.

В ближайшем будущем ожидается рост атак, управляемых и создаваемых при помощи искусственного интеллекта. Уве-

личится количество и качество создаваемых цифровых двойников (дипфейков) — как в отношении отдельных лиц, так и в отношении группы лиц. Будут всё шире использоваться различные каналы обмана пользователей, применяться социальная инженерия и фишинг. Также вырастет доля фейковых сообщений как текстового, так и аудиовизуального характера, созданных с привлечением ИИ, что ещё больше осложнит дифференциацию и корректное обнаружение фейковой и корректной коммуникации между пользователями. Основной (и наиболее опасной) угрозой из мира ВПО останется шифровальщик, предоставляемый злоумышленникам по сервисно-подписочной модели, распространяющийся через ботнеты или при помощи прямой продажи, или созданный по запросу на теневом рынке для обеспечения всё более сложных типов атак, подобных атакам на цепочку поставок с использованием ещё не известных уязвимостей в стороннем ПО или инфраструктуре. Трояны удалённого доступа также останутся на вершине предложений ВПО, предоставляя возможности по удалённому доступу и распространению другого ВПО на целевые машины и сети организаций. Трояны могут даже вытеснить долю типового ВПО для кражи данных из общего объёма ВПО. Представленное на теневом рынке и в «дикой природе» ВПО будет пересобрано разработчиками ВПО для поддержки современных технологий программирования, получивших развитие в последние годы, а также для обхода современных средств защиты, включая, в основном, средства защиты от известного на данный момент ВПО — такого, как традиционные антивирусные средства и средства защиты, полагающиеся, в основном, на статические средства анализа ВПО.

Ботнеты, как и ранее, будут увеличивать охват заражённых устройств и, соответственно, мощности производимых ими атак. Значительно вырастет доля ботнетов, созданных с применением ИИ. Это позволит ботнетам становиться более интеллектуальными и автономными и адаптироваться под возможности современных средств защиты информации для обеспечения более сложных и комплексных атак. Также ботнеты будут активно использовать резидентные IP-адреса и прокси-сервисы, состоящие из IP-адресов домашних пользователей и домашних сетей, для затруднения обнаружения и обхода механизмов защиты, основанных на списках IP-адресов, в том числе и геораспределённых.

«И вновь продолжается бой...» (методы и способы борьбы с ботнетами и ВПО)

Кажется, в этом недружелюбном и опасном мире, с засилием ВПО и ботнетов, сложно защитить себя, организацию, в которой работаем, от проникающего вредоносного воздействия ботнетов и ВПО. Однако не стоит посыпать голову пеплом и прятать, как страус, голову в песок. На любую меру воздействия всегда есть адекватный ответ. Давайте посмотрим, что нам поможет защититься от ВПО в наших сетях и на наших компьютерах.

Традиционным и известным практически всем в мире IT средством защиты от ВПО являлся антивирус. Который хорошо находил известные ему угрозы, используя:

- сигнатурный метод, основанный на отпечатках известных вредоносных, например, по хешам файлов ВПО, полным или частичным, или повторяющимся шаблонам кода ВПО;
- эвристический метод, основанный на поисках характеристик и поведения, свойственного и общего для многих типов ВПО, позволяющий находить потенциально вредоносный код, даже если его сигнатура отсутствует в базе;
- поведенческий анализ, который используется для анализа текущей активности программ и файлов, находя неизвестное ВПО по его поведению, например, по попыткам изменения критических системных файлов, репликации самого себя или выполнения других действий, характерных для ВПО.

Однако для борьбы с современным ВПО одних только антивирусных средств в настоящее время уже недостаточно. Современное вредоносное программное обеспечение разрабатывается с учётом механизмов его обнаружения и противодействия. На теневых ресурсах разработчики ВПО могут проверить работу своих образцов ВПО на возможность их обнаружения средствами защиты информации и предпринять меры по нейтрализации обнаружения, скрывая свой код при помощи шифрования, запутывания, добавления мусорного кода, внесения механизмов обнаружения и нейтрализации средств защиты информации, такой как антивирусы, и вовлечения в атаку самого слабого звена информационной безопасности — человека, оператора того самого устройства-жертвы, на которую в данный момент и нацелено ВПО злоумышленника. Антивирусные средства защиты хорошо работают с известными им угрозами и хорошо дополняют другие средства защиты информации, такие как песочницы (Sandbox) — устройства контролируемого запуска и анализа программного обеспечения — и средства обнаружения и реагирования на конечных точках (Endpoint Detect and Response, EDR). Эти средства применяются в части нейтрализации ВПО и используются как защитные средства на основных каналах распространения ВПО: электронной почте, мессенджерах и конечных устройствах (рабочих станциях, серверах, ноутбуках, мобильных устройствах и т.п.). Но антивирусные средства часто пасуют перед неизвестными им образцами ВПО или перед неадекватными угрозами, но понятными по сценарию атаки действиями пользователей, а также при использовании атакующим инструментария операционной системы и/или прикладного ПО, подписанного и, следовательно, легитимного с точки зрения антивирусного средства программного обеспечения, которое уже захвачено атакующим (либо подпись легитимного ПО используется мимикрирующим под него инструментарием атакующего).

Мы упомянули такие решения, как песочницы и EDR. Остановимся на них поподробнее.

Что из себя представляет песочница (Sandbox)? Это изолированное, управляемое виртуальное окружение, которое используется для тестирования и анализа потенциального ВПО без воздействия на операционную систему и приложения, а также сетевое окружение той машины, где запускается данное виртуальное окружение. Песочница позволяет запустить внутри виртуальной машины подозрительный файл, который передаётся ей другими средствами сетевой защиты, например, межсетевым экраном, расположенным на периметре организации, или внешним

почтовым сервером, расположенным в демилитаризованной зоне, или при помощи агента EDR с машины в локальной сети организации или расположенной удалённо от неё. После запуска переданного песочнице удалённого файла песочница отслеживает его поведение, идентифицирует наличие или отсутствие вредоносной активности после его запуска, эмулирует действие пользователя при помощи порождения событий от клавиатуры и мыши для активации возможного вредоносного воздействия исследуемого образца, эмулирует быстрое течение времени при анализе образца, позволяя активировать ВПО, срабатывающее с задержкой по времени, а также создаёт приманки, которые могут спровоцировать образец на выполнение вредоносной деятельности. После всестороннего анализа исследуемого образца песочница выдаёт вердикт о его вредоносности или безопасности и передаёт безопасные образцы конечным пользователям, которые их ожидают, а в случае ВПО позволяет забрать его на исследование вирусным аналитикам.

Средства обнаружения и реагирования на конечных точках (EDR) позволяют осуществлять постоянный мониторинг конечной точки (под конечной точкой подразумеваются физические или виртуальные устройства, подключённые к сети, такие как ноутбуки и рабочие станции, серверы, смартфоны, планшеты и т.п.), собирать с неё и анализировать постоянно и в реальном времени необходимые данные для идентификации ВПО и реагирования на его деструктивные действия, не позволяя заразить конечную точку неизвестным и известным ВПО или дать ВПО возможность распространения по инфраструктуре. При помощи использования поведенческого анализа, машинного обучения и ИИ EDR обнаруживает сложные атаки, которые может пропустить антивирус, позволяя увидеть ВПО на конечной точке, предотвратить его деструктивную деятельность и восстановить работу конечной точки, приведя её к состоянию, предшествующему заражению ВПО. Причём данная защита работает вне зависимости от того, находится ли конечная точка внутри периметра организации или вне его, удалённо. Во всех случаях EDR защитит конечную точку от деструктивного воздействия ВПО.

Следует отметить, что все три рассмотренных выше средства защиты информации: антивирус, песочница и EDR, — очень хорошо работают вместе, позволяя закрыть все основные, рассмотренные ранее каналы проникновения ВПО на конечные точки и в организации, дополняя друг друга своими возможностями по защите от ВПО и обогащая найденной информацией об угрозах со стороны ВПО, что позволяет выстроить крепкую и эшелонированную защиту.

Последним и самым важным элементом любой системы безопасности является человек, так как именно его действия или бездействие могут привести к негативным последствиям, связанным с заражением и проникновением ВПО на устройства пользователя и в организацию. Поэтому одними лишь техническими средствами защиты информации обеспечить защиту от ВПО невозможно.

Нетехнические средства защиты от ВПО фокусируются на пользовательском поведении и постоянном обучении

пользователей по предотвращению заражений, что включает в себя:

- скептическое отношение к письмам, даже от «знакомых» отправителей;
- отказ от скачивания файлов с сомнительных сайтов;
- проверку URL перед вводом паролей;
- использование сложных паролей и менеджеров паролей;
- регулярное обновление ПО и ОС;
- осторожность в публичных Wi-Fi.

Всё это позволяет повысить защищённость отдельного пользователя, а значит, и всей организации, в которой он работает.

Заключение

Теперь, возвращаясь к началу статьи, становится понятно, что классический антивирус — это точно не средство защиты от современного ВПО. Какие же ещё подходы можно обсудить для реальной защиты от него, кроме тех, что обсуждались выше? Первый, широко используемый в настоящее время и показывающий хорошие результаты, — резервное копирование данных и систем. При этом его надо выполнять регулярно, возможно, в несколько хранилищ, соблюдая версию и обеспечивая защиту копий, а то ВПО «любит» найти эти самые копии — и зашифровать их или уничтожить. И обязательно надо проводить «боевое» тестирование восстановления. А то окажется, как часто бывало и ещё не раз будет: «Чисто писано в бумаге, да забыли про овраги» (с) Лев Николаевич Толстой. Если же всё работает, то основная задача обеспечения защиты информации выполнена. Как минимум, с точки зрения её целостности и гарантированного времени восстановления доступности.

Второй важный момент — активное использование аналитики угроз. Обмен информацией об угрозах (TI — Threat Intelligence), включая IOC (индикаторы компрометации), это та область, где взаимодействуют практически все компании, реально занимающиеся защитой от угроз. Даже если они конкурируют в продуктах и технологиях. Поэтому после обнаружения нового ВПО информация о нём достаточно быстро становится известной. Эта информация может включать и соответствующие хеши, и информацию о центрах управления, и признаки его присутствия, и даже информацию о группировках, его использующих. Таким образом, если применяемые средства защиты информации активно используют TI, то это существенно повышает их эффективность при защите от ВПО. При этом в корпоративной среде можно и нужно активно пользоваться разрешающими списками. А именно — внедрение подхода «всё, что не разрешено, то запрещено»; это может касаться и файлов на рабочих местах пользователей, и процессов на серверах, и доступа к внешним ресурсам Интернета. То есть такой TI — не про плохое, а про хорошее. Мы уже обсуждали с вами выше, что ВПО крайне многообразно и стремительно эволюционирует. В отличие от используемых нами служебных ресурсов, систем и прочего программного обеспечения. И одним из сценариев защиты является именно разрешение использования известного хорошего, отслеживание возникающих блокировок, их анализ на предмет того, была ли это попытка легитимного действия, и, если необходимо, адаптация разрешающих списков.

И, как уже обсуждали выше, третий, один из важнейших элементов борьбы с ВПО — это защита слабейшего элемента, а именно человека. Пока мы готовили эту статью, одному из авторов в Telegram, в чат, который посвящён уже прошедшему выезду детей в летний лагерь в 2022 году, пришёл файл с именем «Фотографии.арк». Что-то удержало его от попытки открыть этот файл и заставило позвонить человеку, от чьего имени он был размещён. Причём позвонить не через Telegram, а по обычному телефону. Можно посчитать это профессиональной паранойей, но лучше потратить пару минут на проверку, чем потом разбираться с тем, что твой телефон контролируют другие люди. Причём злоумышленники хорошо синхронизируют свои действия с ожидаемыми событиями. Когда наступает дата выставления налогов, люди начинают получать на почту «налоговые уведомления», когда планируется повышение пенсий, люди получают на почту письма от «Пенсионного фонда», и тому подобное. Именно поэтому важно обеспечивать не только реактивное уведомление людей, а и проактивное. Тут как раз нам и поможет ранее обсуждавшаяся аналитика угроз. И она должна использоваться не только для повышения эффективности работы средств защиты информации, но и для своевременного уведомления людей.

А закончить эту статью хотелось бы тем, что, видимо, мы никогда не сможем избавиться от ВПО. Скорее, мы будем говорить о том, что оно будет эволюционировать ещё стремительнее, будучи первым в адаптации под свои задачи самых современных технологий, например, искусственного интеллекта. Что может быть прекраснее, чем сразу заложить «точку входа» в генерируемый код? При этом мы надеемся, что качественная реализация подходов, описанных выше, в том числе подразумевающая совместную работу индустрий, позволяет нам сформировать другой ИИ, а именно Искусственный Иммуниет для эффективного противостояния угрозам, реализуемым с использованием разнообразного ВПО. ■

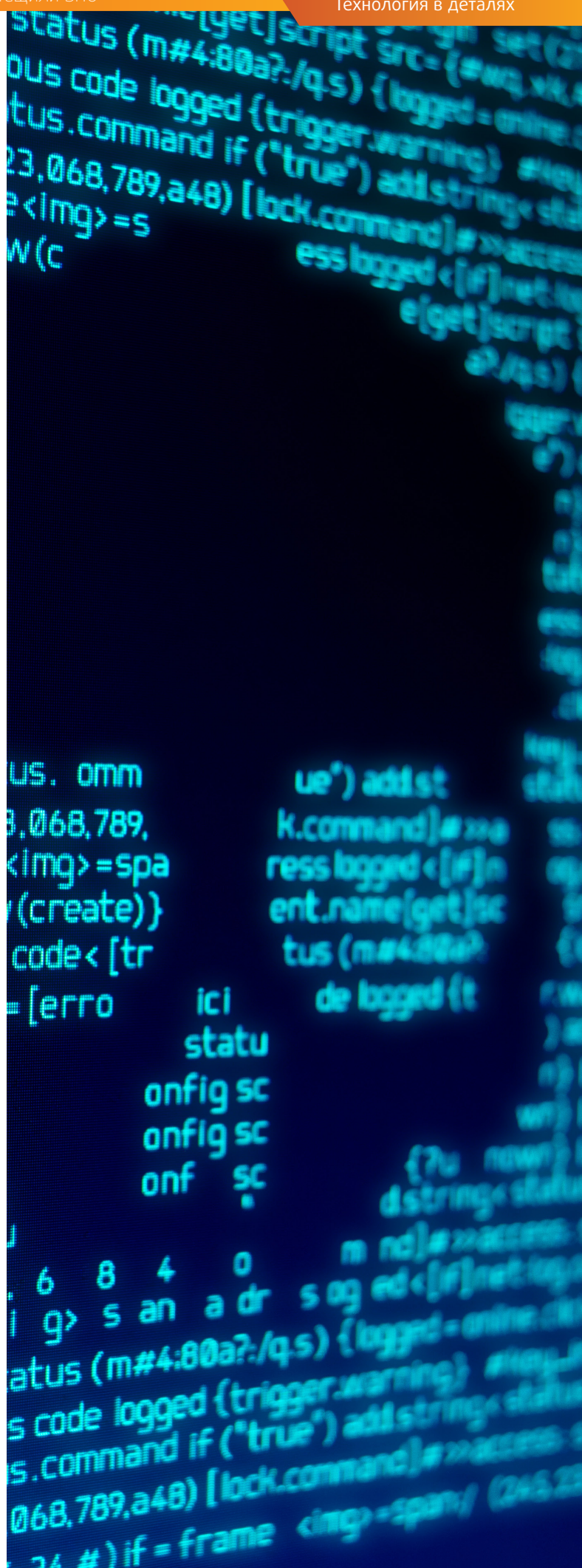
Список литературы:

- [1] <https://any.run/malware-trends/> дата просмотра — 01.10.2025 г.
- [2] <https://ptsecurity.com/ru-ru/research/analytics/trendy-v-razvitii-vredonosnogo-po-i-ego-rol-v-kiberatakah/#id1>
дата просмотра — 02.10.2025 г.

Об авторах

Кагер Михаил Юрьевич — ООО «Юзергейт», Москва

Сивенков Алексей Владимирович — ООО «Юзергейт», Москва



Защита периметра цифровой безопасности в эпоху массового сканирования Сети

Арсений Великород



Аннотация

В статье систематизированы векторы атак для большинства категорий интернет-хостов, приведены типичные примеры (RDP Blue-Keer, уязвимости WinBox, CUPS и др.), обсуждены роль открытого ПО и массовых сканеров, а также практики защиты: грамотная организация удалённого доступа, осторожность с внешними носителями, своевременные обновления и повышение компьютерной и сетевой культуры.

Ключевые слова:

сетевая безопасность, вредоносы, сканирование Интернета, уязвимость.

Сегодня, несмотря на окончание ресурса свободной IPv4-адресации и весьма слабое развитие IPv6, число устройств, имеющих доступ в глобальную Сеть, не перестаёт расти. Кроме того, сама жизнь всё больше интегрируется с сервисами, доступными через Интернет. Вместе с этим, конечно, растёт и поле возможных злонамеренных действий — взломов, несанкционированного доступа к информации и управлению. В отличие от эпохи начала 90-х, когда вирусы были немногочисленны, сегодня в арсенале злоумышленников находится широкая гамма инструментов, которые имеют не только техническую природу, но в том числе и социальную (т.н. человеческий фактор). В этой статье, не претендуя на исчерпание проблематики, автор попытался, как минимум, систематизировать возможные векторы действия «зловердов» в сети Интернет и напомнить ставшие классикой некоторые правила работы в Сети, которые, увы, сегодня не все и не всегда помнят.

Прежде всего приведём основные актуальные на сегодня категории объектов атак в Интернете (т.е. хостов). Это видится необходимым ввиду того, что реализуемость атак подчас зависит именно от программного «форм-фактора» устройства-хоста. Предлагается следующее деление на категории:

- полноценные операционные системы (серверы и рабочие станции);
- сетевое оборудование;
- IoT (в том числе камеры, «умный дом», встроенные системы и т.п.).

В разрезе этих категорий далее и будет выстраиваться анализ. Следует сказать, что для всех трёх категорий существует один общий и во многом решающий фактор, который делает возможными или невозможными атаки и проникновение зловердов в ПО устройств (т.е. превращение устройств в злонамеренных агентов — части возможных «ботнетов»), — это качество кода в смысле следования в нём общим прин-

ципам безопасного программирования. И здесь имеются в виду основные правила, которые известны каждому, кто когда-либо занимался созданием софта: контроль длины записи в буфер и вообще контроль входящих от пользователя данных, использование механизмов, которые позволяют предотвратить атаки, основанные на состоянии блокировки в протоколах [1], а также возможность самому пользователю создавать ситуации, способствующие лёгкому несанкционированному доступу к его устройству (слабые или типовые пароли, оставление фабричного пароля и т.п.).

Сделаем короткий обзор основных моментов, которые делают возможными атаки на хосты в каждой из категорий.

Для ОС семейства Windows на сегодня известно множество векторов атак, основанных на уязвимостях внешних протоколов коммуникации как средства проникновения и захвата привилегированного доступа к системе с правами администратора в результате внутренних уязвимостей в реализации системных служб. Чаще всего последние вызваны возможностью записи за пределами буфера, а также относительно лёгким доступом к записи произвольных данных в память процесса.

В этом плане WinAPI делает «подарок» для злоумышленников, вводя с версии Windows XP функцию WriteProcessMemory [2]. При наличии привилегированного доступа к системе она открывает широкие возможности для запуска произвольного кода изнутри легального исполняемого кода. Такой подход можно встретить в нескольких фреймворках spyware, разработанных в АНБ и ЦРУ и обнародованных WikiLeaks.

Стоит отметить, что в последние годы проблемы с безопас-

ностью исполняемого кода от самой Microsoft становились причиной массовых сбоев в работе их ПО по всему миру, нередко связанных с инфицированием вирусами и сетевыми червями, которые используют обнаруженные уязвимости в коде. Здесь стоит вспомнить уязвимость в протоколе RDP BlueKeep [3], обнаруженную в 2019 году, которая сделала возможным инфицирование множеств систем Windows в т.ч. серверных. Последствия этих атак были во многом катастрофическими т.к. в основном заражение производилось вирусами-шифровальщиками, что приводило к потере данных, с которыми работал бизнес.

Переходим к обзору **для ОС Linux**. Здесь основным носителем уязвимостей является стороннее ПО. И если говорить о самом распространённом способе внедрения, то им остаётся небезопасный код веб-фреймворков, таких как Drupal, WordPress и т.п. Через небезопасные места в коде этих фреймворков злоумышленники подчас не только превращают серверы в части своих ботнетов, но и полностью берут доступ к ним под свой контроль. Конечно, после такого вторжения у владельцев серверов остаётся единственный путь — переустановка ОС.

В стороне, но совсем не забытыми остаются и программные продукты-«старожилы» экосистемы Linux. Так, например, в прошлом 2024 году обнаружился ряд критических уязвимостей в ПО сервера печати CUPS [4]. Уже в этом году стало известно об уязвимостях в некоторых дистрибутивах, которые позволяют несанкционированно получить привилегии root [5].

В целом в последнее время в мире Linux сложилась тенденция, характерная для популярного и динамично развивающегося ПО — развивается как сама операционная система, так и продукты под неё, ведётся как разработка новых продуктов, так и исследование кода существующего ПО. Поэтому, в отличие от эпохи начала взлёта Linux, где система и ПО оставались нишевыми, сегодня, с появлением зрелых коммерческих дистрибутивов и программного обеспечения под них, ситуация с безопасностью кода начнет меняться по образу того пути, который прошли компоненты Windows и ПО для неё.

Однако, не только полноценные серверы и рабочие станции сегодня подвержены атакам со стороны зловредов в Сети. Если не на равном, то хотя бы на сопоставимом уровне в зоне риска находится сегодня и **сетевое оборудование**.

Более всего уязвимы домашние роутеры. Довольно часто их пользователи-владельцы непреднамеренно подвергают опасности свои роутеры и устройства домашней сети, открывая бесконтрольный доступ к службам и интерфейсам устройств, которые совершенно для того не предназначены (отсутствие аутентификации, стойкой к взлому, или небрежно написанный код приводят иногда даже к взлому самого роутера). В этом плане особую роль играет человеческий фактор, хотя известны не единичные случаи нахождения уязвимостей в веб-интерфейсах управления роутерами, а также в некоторых других протоколах управления ими.

Особенно показательным случаем является обнаружение в 2018 году уязвимости в проприетарном протоколе комму-

никации между утилитой WinBox и роутерами Mikrotik [6], которые всё чаще сегодня используются как домашние. В результате этой уязвимости, при определенных условиях, стало возможно получить доступ целиком к управлению роутера и произвольно менять его настройки. Позже, в 2023 году, была выявлена другая [7] уязвимость.

В целом, даже не стоит уточнять, насколько опасным является факт неограниченного доступа к веб-интерфейсу любого домашнего маршрутизатора. Возможность взлома устройств при этом возрастает в разы, прежде всего, из-за неприспособленности таких интерфейсов к нахождению в открытом неконтролируемом доступе в Интернете.

Надо сказать, что в этом плане оказываются беззащитны и вполне серьёзные продукты, предназначенные для операторов связи. Так, в 2023 году была обнаружена уязвимость [8] маршрутизаторов под управлением IOS XE, которая предоставляла возможность «без прохождения аутентификации получить полный доступ к системе с максимальным уровнем привилегий, при наличии доступа к сетевому порту, через который функционирует веб-интерфейс». Ранее обнаруживались также и уязвимости в реализации протоколов SNMP [9] и CMP [10].

В этом смысле в ещё более сложной ситуации находится вопрос безопасности для **устройств Интернета вещей**. Ведь чаще всего их аппаратная часть обладает ещё более скромными характеристиками по сравнению с оборудованием связи, что, собственно, налагает вполне очевидные ограничения на их программные возможности (любые программные возможности требуют дополнительного исходного кода, а значит, и пространства на ПЗУ для хранения бинарного исполняемого файла). Чаще всего код программного обеспечения «интернет-вещей» заточен под их вычислительные характеристики в ущерб безопасности. Взлом камер, регистраторов, контроллеров умных домов, встроенных систем и даже IPMI серверов — это не редкость.

Всё это показывает, что любое устройство, доступное из Интернета и имеющее хоть какую-то значимую по сложности интеракцию с неограниченным числом пользователей, не может быть гарантированно защищено от несанкционированного доступа и взлома через уязвимости с помощью «простых защит» вроде более сложного пароля. Сегодня, когда сложность как программного обеспечения, так и взаимодействия его компонентов между собой растёт, перед разработчиками и тестировщиками встают задачи по тестированию их продуктов, по сложности эквивалентные сложности самого кода.

В этой ситуации изначальным моментом любой защиты от «зловредов», взлома и несанкционированного доступа должна стать компьютерная и сетевая грамотность — минимальные практические представления о том, как функционирует Интернет и какие угрозы сегодня существуют в нём для любого хоста. Сегодня практически каждый хост-мастер (специалист, который обслуживает и производит настройку веб-серверов) знает, что как только веб-сервер становится доступным в Сети, уже буквально через сутки он обнаруживается множеством сетевых сканеров, которые, как в целях вполне безобидных (PaloAlto, например, регулярно сканиру-

ет Интернет — скорее всего, для обновления каких-то своих баз безопасности), так и вполне злонамеренных — с целью обнаружения старых уязвимых версий веб-фреймворков, небезопасных словарных паролей, неаккуратно оставленных файлов с дефолтными настройками — сканируют круглосуточно всё адресное пространство Интернета.

Поэтому нужно осознавать, что сама по себе информация о новых версиях и поправленных в них «багах» и уязвимостях прошлых версий (файлы RELEASE и BUGS, поставляемые в комплекте с установочными файлами) — это информация сразу для двух сторон: для тех, кто пользуется программным обеспечением, и для тех, кто ищет уязвимости в нём для злонамеренных действий на чужой инфраструктуре. В эпоху ПО с открытым исходным кодом (если взять несколько шире — в эпоху легкодоступных открытых данных) все эти данные более не являются тайной. Следует вполне серьёзно брать в расчёт возможность того, что эти данные могут быть и будут использованы в целях не вполне благонамеренных — для поиска тех, кто ещё использует WordPress старой версии с уязвимостью, или тех, кто оставил файл с паролем пользователя admin в веб-директории с возможностью его чтения всеми пользователями.

Какие основные моменты обеспечения безопасности можно упомянуть в рамках статьи? В отношении организации удалённого доступа к ресурсам домашней или корпоративной сети следует сказать, что вопрос всегда состоит в разумном компромиссе между техническими возможностями сетевой инфраструктуры, удобством доступа и управления им. Причём этот выбор всегда зависит в равной степени как от возможностей сетевого оборудования (маршрутизатора или файервола), так и от характеристик ресурса внутренней сети и протоколов доступа к нему.

И выбор здесь действительно широк. В плане технологии доступа обычно возможны: прямой доступ через веб, ограничение списками доступа (ACL), проброс портов, ssh-туннель, разнообразные типы VPN и т.п. С точки зрения самого ресурса, также возможны разные варианты доступа, причём порой одновременно несколько. И, в конечном итоге, разумное решение этого действительно комплексного вопроса во многом зависит от осведомлённости хозяев инфраструктуры о том, какие сетевые ресурсы возможно выставлять «голым» интерфейсом в Интернет, а какие нет; какие риски, неудобства и преимущества несёт то или иное решение по доступу к ним.

Надо сказать, что оценка пригодности интерфейсов для нахождения в среде открытого публичного доступа в Интернете является самостоятельной задачей. Как понять, что можно оставлять без условного ACL, а к чему возможен доступ только через VPN с IPSEC? Конечно, в первую очередь, примитивные соображения об уровне доступа, который может получить потенциальный взломщик в случае взлома. Но, как было сказано ранее, есть и менее очевидные моменты. В какой степени реализация того же веб-интерфейса является безопасной? Ответ на этот вопрос далеко не тривиален. Ведь есть ситуации, когда возможность SQL-инъекций или внедрения шелл-кодов совершенно не очевидна обычному пользователю. Чтобы узнать это, часто необходим анализ кода приложения на уровне опытного программиста. И эта

задача становится действительно ещё сложнее, если приложение запускается в embedded-окружении. В рамках этой статьи совершенно не представляется возможным подробно рассмотреть этот вопрос. Однако следует подчеркнуть его значимость для обеспечения устойчивого периметра безопасности.

Переходя к более простым вещам, не обойдём вниманием и безопасность паролей. К сожалению, этот вопрос и в наши дни далёк от решения. Автору статьи не раз приходилось видеть несерьёзное отношение к сложности пароля или к вопросу его сохранения в тайне. А ведь пароль тем и ценен, что в идеале он известен только одному человеку. Ещё хуже сегодня ситуация с применением тактики периодической смены паролей. Сегодня уже понятно, что эта тактика требует определённой переоценки, т.к. иногда или нереализуема вообще, или вырождается в побочные проблемы безопасности. Современные возможности перебора паролей дают широкие возможности для того, чтобы совершить подбор в умеренные сроки, особенно если мы говорим о персистирующих сетевых червях и ботнетах. Поэтому, чем дальше используемый пароль от «словарных наборов», тем сложнее произвести его подбор. Увы, возможности злоумышленников в современных реалиях осознаются далеко не всеми. И несмотря на масштабное развитие методов «социальной инженерии» (фишинг и ему подобное), словарный подбор продолжает занимать совсем не последнее место в обиходе доступных методов несанкционированного доступа к системам и данным.

Последними в очереди, но первыми по значимости идут старые как мир предостережения об осторожности при использовании чужих флешек. Ведь именно они довольно часто являются носителями вредоносных программ. Также стоит избегать неконтролируемого доступа третьих лиц к персональным компьютерам и информации, хранящейся на них. Желательно, чтобы чувствительная информация не хранилась в незашифрованном виде. Это позволяет, при определённых условиях, сделать её резервные копии и держать на внешнем хранилище (иногда даже облачном).

Завершая статью, следует сказать, что своевременное обновление программного обеспечения и компонентов операционных систем является также одним из моментов безопасности. Конечно, и здесь не стоит проявлять маниакального рвения накатить каждое обновление. Всё же, чаще всего сегодня возможно чётко определить критичность обновления, и ограничиться только самыми необходимыми.

Несомненно, столь обширный вопрос, как сетевая безопасность в эпоху всеобщей интернетизации и открытого доступа, невозможно охватить одной или даже несколькими статьями. А если учитывать всё многообразие ситуаций, то, наверное, можно написать целый учебник на эту тему. Однако взломы, заражения сетевыми червями, шпионскими вредоносами, а также утечки информации происходят в последнее время всё чаще. Поэтому необходимо подчеркнуть, что эпоха относительной безопасности Интернета в смысле пассивности угроз в нём закончилась. Сегодня как от профессионалов, так и от обычных пользователей требуется всё больше и больше знаний, чтобы сохранять свои данные в безопасности, а частную жизнь и корпоративные данные

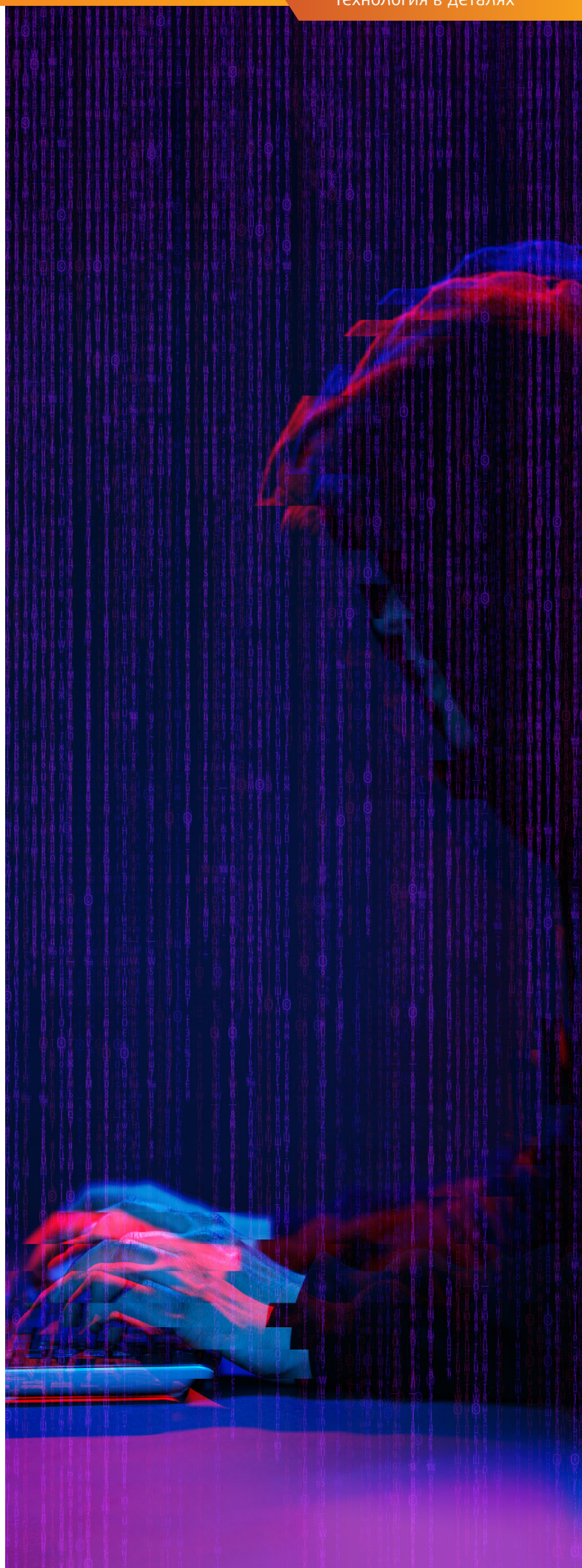
неприкосновенными. И в этом обзоре автор постарался подсветить технологический охват и сложность проблемы сетевой безопасности в современных реалиях. ■

Список литературы:

- [1] Пример пентеста, основанного на проверке возможности такой атаки: <https://github.com/pentestfunctions/CVE-2024-6387/blob/production/7etsuo-regreSSHion.c>
- [2] <https://learn.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi-writeprocessmemory>
- [3] <https://www.securitylab.ru/blog/company/PandaSecurityRus/346879.php>
- [4] https://habr.com/ru/companies/spring_aio/articles/846498/
- [5] <https://www.securitylab.ru/news/563447.php> <https://cloudsecurityalliance.org/blog/2023/10/17/new-container-exploit-rooting-non-root-containers-with-cve-2023-2640-and-cve-2023-32629-aka-gameover-lay#>
- [6] <https://habr.com/ru/articles/416067/> , <https://habr.com/ru/articles/359038/>
- [7] <https://habr.com/ru/news/750608/>
- [8] <https://www.opennet.ru/opennews/art.shtml?num=59948>
- [9] <https://www.opennet.ru/opennews/art.shtml?num=46868>
- [10] <https://www.opennet.ru/opennews/art.shtml?num=46522>

Об авторе

Великород Арсений Валентинович,
старший сетевой инженер CDN-Video,
ORCID: <https://orcid.org/0009-0003-6549-8292>





Эволюция фишинга: от примитивных писем к deepfake и целевым атакам

Николай
Гавриченко



Аннотация

В статье прослеживается эволюция фишинговых атак от их зарождения до современности. Предлагается классификация развития фишинга по четырём ключевым этапам, согласно методам и временным периодам. Особое внимание уделяется переходу от массовых атак к целевым, основанным на социальной инженерии, и новейшим опасным трендам, таким как генерация убедительных текстов с помощью AI и подмена голоса и лица в реальном времени с помощью deepfake.

Ключевые слова:

фишинг, кибербезопасность, целевой фишинг, искусственный интеллект (AI), социальная инженерия, информационная безопасность, кибермошенничество.

Введение

Фишинг представляет собой одну из самых распространенных интернет-угроз, целью которой является получение личных данных пользователя, например, учётных данных, номера карты, кода из SMS и т.д. Методы фишинга развиваются в соответствии с техническим прогрессом.

Раньше достаточно было обращать внимание на адрес отправителя, корректность ссылок и просто орфографические ошибки. Сегодня атаки стали технологичнее, точнее и менее очевидными. Данная статья о том, как киберпреступники идут в ногу со временем, используя актуальные инструменты в связке с уязвимостями человеческой психологии.

Результаты

Эволюцию фишинга можно классифицировать по временным периодам и уровню сложности, выделив четыре основных этапа, которые отличаются методами и целями атак.

1. Примитивный массовый фишинг

На ранних этапах фишинг характеризовался массовостью и минимальной избирательностью. Злоумышленники использовали рассылки на миллионы случайных электронных почтовых адресов.

Техническая реализация была примитивной: письма часто отправлялись с бесплатных почтовых сервисов, содержали огромное количество грамматических и орфографических ошибок, а их дизайн лишь отдалённо напоминал бренды, под которые они маскировались.

Провокационные заголовки, а также явная подделка известных URL позволяли легко определять нежелательную рассылку. Согласно статистике, эффективность таких атак составляла менее процента, но с учётом количества писем фишинг приносил значительный доход.

Реальный случай: «Нигерийские письма» или «письма счастья». Пользователь мог получить письмо с заголовком «Срочно! Помогите получить наследство!» В тексте некая «Мария Джонсон» из Лондона рассказывала трогательную историю о миллионах долларов, замороженных на счёте её покойного мужа, и просила помочь с переводом денег в обмен на 10% от суммы. Для получения средств требовалось «всего лишь» предоставить данные банковского счёта и оплатить небольшие «законные издержки». Другой распространённый пример — письма от имени «службы безопасности» eBay или PayPal с грубыми ошибками в логотипе и тексте, требующие «проверить учётную запись» по ссылке, ведущей на сайт paypal-security.com.

2. Технологический фишинг

С повышением общей осведомлённости пользователей, а также развитием спам-фильтров и антивирусного программного обеспечения киберпреступники стали адаптироваться и применять более серьёзные инструменты [1].

Значительно выросло качество исполнения. Злоумышленники создавали полноценные сайты, копирующие дизайн и логику (например, авторизацию) оригинального ресурса.

Электронные письма подкреплялись вложениями с вредоносными программами, имели качественную HTML-вёрстку, а также часто содержали ссылки, которые сокращались через специальные сервисы и перенаправляли на вредоносные ресурсы. Эффективность на данном этапе выросла до 10%, так как обнаружить подделку стало проблематичнее.

Реальный случай: В 2010-х годах прокатилась массовая волна фишинговых писем от имени популярных сервисов, например, DHL. Письмо с темой «Ваша посылка ожидает получения» выглядело идеально: фирменные шрифты, логотипы, корректная вёрстка. В письме сообщалось, что для получения заказа не-

обходимо скачать и распечатать «накладную» во вложении. Этим вложением был файл TTH_Nº12345.exe, который на самом деле являлся трояном-кейлоггером. Также имел место всплеск фишинговых писем от имени Netflix с угрозой блокировки аккаунта и ссылкой на идеально скопированную страницу входа, которая похищала учётные данные.

3. Целевой фишинг

К этому этапу атаки стали носить точечный характер. Жертва заранее изучается через открытые источники, например, соцсети, а также используя слитые данные, утечки или купленную информацию. Целью является собрать все возможные личные данные — имя, место работы, контакты, даже круг общения [2].

Таким образом, электронное письмо или сообщение в мессенджер формируется для конкретного адресата, используя информацию о нём.

Речь в данном случае идёт о похищении значительных сумм или интеллектуальной собственности. Успешность достигает 35%.

Целевой фишинг имеет несколько специализированных разновидностей.

Spear Phishing (копьевого фишинг) — стандартный и широко используемый метод целевого фишинга. Атака нацелена на конкретного сотрудника внутри организации. Примером является сообщение бухгалтеру от «руководителя компании» с указанием срочно перевести деньги на мошеннический счёт.

Реальный случай: Бухгалтер компании получает письмо от имени финансового директора. Текст звучит правдоподобно: «Здравствуйте, [Имя бухгалтера]. Я на совещании, срочно нужно провести платёж по договору №45/ИП от сегодняшнего числа. Все детали во вложении. Связь плохая, пишите только на почту». Во вложении — инфицированный документ или ссылка на фальшивую страницу корпоративного портала.

Whaling (фишинг на топ-менеджмент) — по сути является копьевым фишингом, отличие в том, что целью являются чиновники высшего звена, директорат и другие высокопоставленные лица. Изучение жертвы проходит более тщательно, легенда формируется точнее и имитирует, например, судебные разбирательства или предложения от партнёров по бизнесу.

Реальный случай: В 2016 году киберпреступники, выдав себя за руководителя дочерней компании, с помощью серии фишинговых писем убедили CEO австрийского производителя авиационных компонентов FACC перечислить 50 миллионов евро на мошеннический счёт.

Smishing (SMS-фишинг) — данный метод может быть как обособленным, так и являться частью мошеннической схемы. Каналом связи в данном случае выступает служба коротких сообщений, текст которых содержит уведомление о выигрыше, курьерской доставке, блокировке карты и, конечно же, подозрительную ссылку.

Реальный случай: Сообщение: «Банк «XXX». По подозрению в мошенничестве ваша карта заблокирована. Для разбло-

кировки перейдите по ссылке: bank-xxx.ru/confirm». Ссылка вела на фишинговый сайт, запрашивающий все данные карты, включая CVV и одноразовые коды.

Vishing (голосовой фишинг) — атака, осуществляемая по телефону либо в мессенджерах. Мошенник, используя собранные о жертве данные, звонит ей под видом сотрудника IT-отдела, службы безопасности банка или техподдержки сервиса. Социальная инженерия и психологическое давление помогают выманить конфиденциальные данные, пароли или разрешить удалённый доступ к компьютеру.

Реальный случай: Звонок на номер сотрудника: «Здравствуйте, это техподдержка Microsoft. На вашем компьютере зафиксирована критическая уязвимость. Для её устранения нам потребуется удалённый доступ. Откройте программу AnyDesk и сообщите нам код». Далее под предлогом «защиты» мошенники похищали конфиденциальные данные или устанавливали шпионское ПО.

4. Высокотехнологичный фишинг

Современный фишинг использует передовые IT-технологии, такие как машинное обучение и генеративные AI. К сожалению, это значительно повышает его успешность. Автоматизация сбора и сортировки информации делает целевой фишинг массовым, что влияет на частоту атак.

Ключевые технологии и их применение

Тексты. Нейросети (например, ChatGPT, Gemini) применяются для создания орфографически и стилистически корректных сообщений на любом языке. Отсутствие явных ошибок позволяет обходить спам-фильтры и усложняет обнаружение пользователями. ИИ может написать текст на любую тематику, от официального до дружеского обращения.

Реальный случай: Мошенники используют ИИ для генерации персональных писем жертвам, найденным на LinkedIn, «Хабре» и других ресурсах. Вместо шаблонного «Уважаемый пользователь», письмо начинается так: «Здравствуйте, [Имя]. Прочитал вашу статью о кибербезопасности на Хабре — очень впечатляюще. У меня есть деловое предложение, ознакомиться можно здесь: [фишинговая ссылка, маскирующаяся под DocSend]». Отсутствие ошибок и персонализация обходят фильтры и вызывают доверие.

Deepfake (глубокие фейки) — самый опасный инструмент высокотехнологичного фишинга.

Используя технологии синтеза голоса по образцу голоса (например, на основе короткого аудиофрагмента публичного выступления или видео в социальной сети), хакеры создают поддельные голосовые сообщения или совершают телефонные звонки голосом, неотличимым от голоса настоящего человека.

Технология deepfake позволяет в режиме реального времени подменять лицо и голос человека на видео. Мошенник может организовать видеоконференцию, где на экране будет цифровой двойник генерального директора, отдающего приказ финансовому директору. Такие атаки обладают максимальной разрушительной силой, поскольку преодолевают последний барьер недоверия — визуальную верификацию.

Реальный случай (голосовой глубокий фейк): В 2019 году CEO британской энергетической компании получил телефонный звонок от своего «босса» — главы немецкой материнской компании. Голос с характерным немецким акцентом приказал срочно перевести 220 тысяч евро на счёт венгерского поставщика. Перевод был совершён немедленно, так как голос был абсолютно идентичен настоящему.

Реальный случай (видео глубокий фейк): В 2021 году мошенники использовали видео с глубокой подделкой лица и голоса директора инвестиционной компании, чтобы организовать фиктивную видеоконференцию с сотрудниками и юристами и санкционировать незаконную финансовую операцию.

Обсуждение

Представленная классификация демонстрирует, что эволюция фишинга происходит в тесном контакте технологий и человеческой психологии. Это определяет смену вектора противодействия угрозам с программно-аппаратных методов на комплексные подходы, ориентированные на человека.

На заре фишинга противодействие было в первую очередь техническим и фильтрующим. Почтовые фильтры отсеивали массовый спам по формальным признакам. Однако по мере того, как фишинг становился более целевым и изощрённым, одних лишь технических барьеров стало недостаточно. Мошенники начали использовать социальную инженерию, обходя стандартные защиты за счёт доверия к личности отправителя или релевантности содержимого. Это привело к смещению фокуса на человеческий фактор: повсеместному внедрению тренингов по киберграмотности, моделированию фишинговых атак для обучения сотрудников и разработке строгих организационных процедур (например, обязательной устной проверки для финансовых транзакций).

В настоящее время, с наступлением эры высокотехнологичного фишинга с использованием искусственного интеллекта и глубоких фейков, мы наблюдаем синтез этих двух подходов. Технологии снова выходят на первый план, но уже на качественно новом уровне. Для противодействия ИИ-генерации контента и голосовых подделок требуются столь же продвинутые средства защиты. Ожидается, что это повлечёт за собой повсеместное внедрение криптографических методов аутентификации, основанных на принципах «нулевого доверия», и усиление роли биометрических верификационных протоколов, которые сложнее скомпрометировать дистанционно [3]. Таким образом, будущее противодействия фишингу лежит в области гибридных моделей, где передовые технологии защиты усиливают бдительность человека, а осведомлённый пользователь становится последним и самым важным рубежом обороны.

Таблица 1.
Классификация эволюции фишинговых атак

	Ключевые характеристики	Примеры	Методы противодействия
1. Примитивный массовый фишинг (1990-е – ~2005)	Широкие нецелевые рассылки, низкое качество, лёгкое обнаружение	Письма от «банка» с просьбой подтвердить данные	Базовые фильтры спама, обучение пользователей распознаванию очевидных признаков (орфографические ошибки, подозрительные адреса отправителей), проверка URL перед кликом
2. Технологический фишинг (~2005 – ~2015)	Использование уязвимостей, трояны, улучшенный дизайн	Внедрение кейлоггеров, фишинговые сайты-клоны	Антивирусное ПО, фаерволы, регулярное обновление ПО для закрытия уязвимостей, двухфакторная аутентификация (2FA), использование безопасных браузеров с проверкой сертификатов
3. Целевой фишинг (~2010 – по н.в.)	Точечные атаки на конкретных людей/компаний, социальная инженерия	Целевые письма от имени коллеги или руководства	Повышенная киберграмотность, тренировки по распознаванию фишинга, строгие процедуры проверки запросов на перевод средств/данных, сегментация сетей для ограничения доступа
4. Высокотехнологичный фишинг (~2018 – по н.в.)	Использование AI, глубоких фейков, автоматизации	Deepfake-звонки, AI-генерация писем	Поведенческий анализ и AI-детекция аномалий, биометрическая и многофакторная аутентификация (MFA), использование кодовых слов/фраз для подтверждения критических запросов, продвинутые системы мониторинга трафика и почтовых угроз

Заключение

Развитие фишинга двигалось от неточных, массовых рассылок с массой ошибок и вызывающими заголовками к высокотехнологичным атакам на конкретного человека. Ранее методы противодействия заключались в технологической составляющей, такой как спам-фильтры, антивирусы. Теперь основой интернет-безопасности является человеческий фактор.

Ни одно даже самое передовое и актуальное техническое решение не может гарантировать 100% защиты от злоумышленников. Поэтому к методам современной защиты следует отнести:

- регулярное тестирование и обучение сотрудников основам информационной безопасности;
- внедрение строгих процедур для подтверждения финансовых транзакций (использование кодовых слов, многократная проверка по разным каналам связи);
- технологические решения: DMARC, DKIM, SPF для проверки почты, системы мониторинга угроз.

Фишинг из грубого инструмента мошенников превратился в сложное оружие киберпреступников. И единственный адекватный

ответ на эту угрозу — сочетание технологий, процедур и, что самое главное, осведомленности и бдительности каждого человека. ■

Список литературы:

- [1] Завьялов А.Н. Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения. — Baikal Research Journal, 2022. — №2. — С. 36-42.
- [2] Фишинг: как распознать и не стать жертвой мошенников [Электронный ресурс] URL: <https://www.kaspersky.ru/resource-center/preemptive-safety/phishing-prevention-tips> (дата обращения: сентябрь 2025).
- [3] Что такое фишинг? [Электронный ресурс] URL: <https://www.microsoft.com/ru-ru/security/business/security-101/what-is-phishing> (дата обращения: сентябрь 2025).

Об авторе

Гавриченко Николай Егорович, координатор разработки продуктов Фонда развития сетевых технологий «ИнДата», ассистент кафедры интеллектуальных систем и теплофизики ИИР НГУ.



Самораспространение вредоносного программного обеспечения в локальной сети

Андрей Жданов

Аннотация

В статье рассказывается о способах самораспространения вредоносного программного обеспечения (ВПО) в локальной сети. Автор отмечает, что в настоящее время использование функционала самораспространения в ВПО потеряло свою актуальность. Сейчас для самораспространения гарантированно можно использовать только легитимные механизмы — создание групповой политики, использование общих административных сетевых ресурсов (Admin Shares) и использование общих ресурсов для самораспространения. Автор приводит примеры применения этих техник, а также даёт рекомендации по защите сетей и устройств от самораспространяемого ВПО.



Ключевые слова:

ВПО, вредоносное программное обеспечение, вирус, червь, легитимные механизмы.

Первым знаменитым образцом вредоносной программы, использующей механизм самораспространения в сети, стал в 1988 году сетевой червь Морриса. Червь назван по имени его автора — аспиранта Корнельского университета Роберта Таппана Морриса (Robert Tappan Morris). По словам автора, червь был написан в исследовательских целях, однако наличие ошибок в его исходном коде привело к массовому заражению компьютеров в сети ARPANET, которая в то время была предшественником современного Интернета. В результате червём была парализована работа нескольких тысяч компьютеров, а общий ущерб был оценен в 98 миллионов долларов.

Основы теории механизмов самовоспроизведения заложил еще в 1951 году американский математик и физик Джон фон Нейман (John von Neumann). Поэтому неудивительно, что именно вирусы и черви стали первыми образцами вредоносного программного обеспечения (ВПО).

Вирусы внедряют свой код в различные объекты, в которых он может выполняться и продолжать своё распространение дальше. Такими объектами могут быть, например, исполняемые файлы, скрипты, исходный код, загрузочные секторы и т.п. При этом код вируса может видоизменяться (полиморфные вирусы). Черви же, в отличие от вирусов, не внедряют свой код для самораспространения, а создают свои копии,

которые также могут различаться между собой. Черви, использующие сеть для распространения, относят к сетевым. Вирусы и черви объединяют под понятием вирусное ВПО.

Одно из официальных определений ВПО в соответствии с ГОСТ Р 53113.1-2008 (<https://bdu.fstec.ru/ubi/terms/terms/view/id/12>):

Вредоносная программа (программное обеспечение) — программа (программное обеспечение), предназначенная для осуществления несанкционированного доступа и/или деструктивного воздействия на информацию или ресурсы информационной системы, нарушение их целостности и/или доступности.

Поначалу вредоносные программы преимущественно разрабатывались из хулиганских побуждений, они могли в процессе своего функционирования производить изощрённые звуковые и видеоэффекты, но были и вирусы-вандалы, которые уничтожали данные и даже могли вывести из строя компьютер (вирус СИН/Чернобыль). Со временем доля вирусов и червей в ВПО становилась всё меньше и меньше, львиную часть стали составлять троянские программы. По аналогии с «Троянским конём», троянскими программами считают вредоносные программы, маскирующиеся под легитимные и полезные. В зависимости от их целей троянские программы разделяют на бэкдоры, шпионские программы, программы-вымогатели и т.п. Однако до сих пор по традиции двадцатилетней давности многие называют вирусами все вредоносные программы без разбора.

Массовое распространение вирусов и червей приводило к масштабным эпидемиям. Примеры наиболее громких и значимых эпидемий с использованием сетевых червей:

- в 2000 году — ILOVEYOU (LoveLetter) (https://www.theregister.com/2020/05/05/iloveyou_20_years/);
- в 2001 году — Code Red (<https://www.kaspersky.ru/blog/history-lessons-code-red/33795/>);
- в 2003 году — Slammer (Sapphire) (<https://threatpost.com/inside-story-sql-slammer-102010/74589/>);
- в 2004 году — Mydoom (<https://yourstory.com/2025/01/worst-computer-virus-time-digital-plague-spreading>);
- в 2007 году — Storm (https://www.schneier.com/blog/archives/2007/10/the_storm_worm.html);
- в 2008 году — Conficker (Kido) (<https://www.anti-malware.ru/news/2020-09-15-111332/33688>);
- в 2010 году — Stuxnet, который стал первым известным образцом кибероружия (http://www.chinaview.cn/20230411/4e0fa0f4fd1d408aaddeef8be63a4757/202304114e0fa0f4fd1d408aaddeef8be63a4757_20230411161526_0531.pdf).

В апреле 2017 года хакерская группировка «The Shadow Brokers» опубликовала материалы под названием «Lost in Translation», в которых содержались инструменты Equation

Group, которую связывают с Агентством национальной безопасности США (АНБ) (<https://research.checkpoint.com/2020/pazar-spirits-of-the-past/>). В составе фреймворка FuzzBunch содержался набор эксплоитов для уязвимостей нулевого дня [1] и бэкдоров [2]. Наиболее печально известными из них стали эксплоит EternalBlue и бэкдор DoublePulsar. Спустя месяц, в мае 2017 года, инструментами из публикации «The Shadow Brokers» воспользовалась группировка неизвестной принадлежности, создавшая программу-вымогатель WannaCry (WanaCryptor), которая, по сути, представляла собой сетевой червь (<https://www.kaspersky.ru/blog/wannacry-hsitory-lessons/33853/>). Для доставки непосредственно программы-вымогателя на компьютеры локальной сети червь использовал уязвимость Microsoft Server Message Block 1.0 (SMBv1) CVE-2017-0145 (MS17-010), которую реализовал эксплоит EternalBlue. В результате успешной эксплуатации в качестве полезной нагрузки на целевой компьютер загружался бэкдор DoublePulsar. А уже с помощью установленного бэкдора на компьютер загружалась непосредственно программа-вымогатель WannaCry и далее осуществлялось шифрование данных на компьютере. За расшифровку вымогатели требовали всего 300 долларов США в криптовалюте. Общий же ущерб от эпидемии составил по различным оценкам не менее 4 миллиардов долларов США. А в июне 2017 года произошла эпидемия вайпера NotPetya, использовавшего те же инструменты АНБ.

До сих пор различное ВПО, преимущественно связанное с криптоджекингом* и вымогательством, использует связку эксплоита EternalBlue и бэкдора DoublePulsar для распространения своих модулей в уязвимой сетевой инфраструктуре.

В настоящее время можно с уверенностью говорить о закате эры вирусов и червей, если, конечно, у кого-то вдруг снова не окажется в рукаве козырного туза в виде новой разрушительной уязвимости нулевого дня, что выльется в очередную эпидемию. Но ВПО сейчас стало криминальным бизнесом, поэтому кажутся маловероятными подобные публикации в будущем. Цена таких эксплоитов на чёрном рынке достигает миллионов долларов, и никто не будет разбрасываться ими просто так. Да и спецслужбы провели работу над ошибками, чтобы избежать таких утечек.

Надобность в бесконтрольном самораспространении ВПО со временем отпала, как, впрочем, и в многофункциональных вредоносных мегакомбайнах. Атакующие сейчас используют для разведки сети и распространения в сетевой инфраструктуре жертвы отдельные специализированные инструменты, а серьёзные вредоносные программы имеют модульную структуру и выполняют свои конкретные задачи. Также стоит учесть, что избыточные функциональные возможности могут демаскировать ВПО (например, бэкдор или шпионскую программу) в скомпрометированной системе.

Среди ВПО программы-вымогатели — это отдельная история. В случае WannaCry и NotPetya использование уязвимости SMBv1 для самораспространения позволило осуществить массовое шифрование/уничтожение данных без непосред-

*Криптоджекинг — использование компьютера для добычи криптовалюты, часто через веб-сайты, против воли пользователя или без его ведома.

ственного участия атакующих. Сейчас же в атаках программы-вымогатели размещаются в инфраструктуре жертвы и запускаются на самом последнем этапе атаки, когда атакующими уже получен полный контроль над инфраструктурой жертвы: выгружена на ресурсы злоумышленников конфиденциальная информация жертвы и нейтрализованы защитные средства, в том числе и антивирусное ПО. При этом нередко атакующие используют само антивирусное ПО для распространения в локальной сети своих инструментов. В этом случае функция самораспространения в программах-вымогателях может быть полезна с точки зрения наибольшего охвата данных для шифрования с целью нанесения максимального ущерба жертве, причём эти действия произведутся автономно, без непосредственного участия злоумышленников.

Реализация функции самораспространения является весьма непростой задачей. При отсутствии уязвимостей, подобных SMBv1, необходимо применять легитимные механизмы, а для них требуется наличие корректных доменных учётных записей. Учётные данные могут быть получены атакующими на предыдущих этапах атаки или подобраны самой вредоносной программой в результате перебора.

Программы-вымогатели с подобным функционалом можно пересчитать по пальцам, в основном они разрабатывались крупными «солидными» партнёрскими программами (RaaS, Ransomware-as-a-Service), не скупящимися на разработку и поддержание своего имиджа. В качестве примера можно привести такие известные шифровальщики, как LockBit 3.0 (Black), BlackCat и Qilin.

Как уже сказано выше, доля вирусов и червей в ВПО сейчас мала, также невелико и число программ-вымогателей, имеющих функционал самораспространения, да и он имеет уже второстепенное значение. Поэтому употребление в обиходе термина «вирус-шифровальщик», как и «вирусы» в отношении всего ВПО, совершенно некорректно, это так же неверно, как в биологии называть вирусами все патогенные микробы.

Итак, на вооружении разработчиков ВПО остались легитимные техники самораспространения, если не брать в расчёт уязвимости наподобие SMBv1. Далее речь пойдёт о Windows-системах, но это не означает, что в Linux-системах нельзя реализовать самораспространение, например, с помощью таких сервисов, как SSH (Secure Shell) и SFTP (Secure File Transfer Protocol). Всё же на практике чаще всего применяется самораспространение в ВПО, разработанном для Windows-платформ.

Такими популярными техниками самораспространения в локальной сети в Windows-системах являются создание групповой политики и использование общих административных сетевых ресурсов (Admin Shares). В активно используемой против российских компаний программе-вымогателе LockBit 3.0 (Black) реализованы обе техники.

Создание групповой политики

Данную технику мы рассмотрим на примере известной программы-вымогателя — LockBit 2.0, в которой одной из первой была реализована эта техника. Впоследствии

другие программы-вымогатели заимствовали эту реализацию из LockBit 2.0.

В случае, если программа-вымогатель запущена с администраторскими правами на контроллере домена, программа с помощью групповой политики предоставляет общий доступ к дискам хостов, останавливает службы и завершает процессы на хостах, а также осуществляет своё распространение в локальной сети.

Для этого вредоносная программа создаёт в корневом каталоге Group Policy Object (GPO) на контроллере домена структуру каталогов и файлов, определяющих новую групповую политику:

<GPO_GUID>\GPT.ini

<GPO_GUID>\Machine\Preferences\NetworkShares\NetworkShares.xml

<GPO_GUID>\Machine\Preferences\Services\Services.xml

<GPO_GUID>\Machine\comment.cmtx

<GPO_GUID>\Machine\Registry.pol

<GPO_GUID>\User\Preferences\Files\Files.xml

<GPO_GUID>\User\Preferences\ScheduledTasks\ScheduledTasks.xml

GPO_GUID — GUID новой групповой политики

NetworkShares.xml предназначен для предоставления общего доступа к дискам хостов домена с целью доступа программы-вымогателя к большому количеству файлов в сети жертвы для их шифрования.

Services.xml предназначен для остановки и запрета системных служб на хостах домена, связанных в основном с системами управления базами данных (рис. 1).

Файлы **Registry.pol** и **comment.cmtx** предназначены для отключения Windows Defender на хостах путём модификации соответствующих параметров системного реестра.

Программа-вымогатель копирует свой исполняемый файл в каталог общедоступных файлов **Active Directory SYSVOL**:

\\< DNS_DOMAIN_NAME>\sysvol\< DNS_DOMAIN_NAME>\scripts\

DNS_DOMAIN_NAME — имя домена DNS.

Files.xml предназначен для копирования файла программы-вымогателя из каталога общедоступных файлов Active Directory SYSVOL в каталог на хосте.

ScheduledTasks.xml предназначен для создания на хосте задач планировщика. Одна задача планировщика завершает определённые процессы на хостах домена, вторая же про-


```
<?xml version="1.0" encoding="utf-8"?>
<NTServices clsid="{2CFB484A-4E96-4b5d-A0B6-093D2F91E6AE}">
  <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}" name="SQLPBDMS" image="4"
    changed="2023-01-23 18:21:25" uid="{3945152F-3312-4CCE-92EE-C28F8437C16D}" disabled="0">
    <Properties startupType="DISABLED" serviceName="SQLPBDMS" serviceAction="STOP" timeout="30"/>
  </NTService>
  <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}" name="SQLPBENGINE" image="4"
    changed="2023-01-23 18:21:25" uid="{196B0DD4-BFD3-4BDF-87DF-040A0F56A12D}" disabled="0">
    <Properties startupType="DISABLED" serviceName="SQLPBENGINE" serviceAction="STOP" timeout="30"/>
  </NTService>
  <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}" name="MSSQLFDLauncher" image="4"
    changed="2023-01-23 18:21:25" uid="{37238E24-B477-4F07-AFA8-B919C215ECAC}" userContext="0"
    removePolicy="0" disabled="0">
    <Properties startupType="DISABLED" serviceName="MSSQLFDLauncher" serviceAction="STOP"
      timeout="30"/>
  </NTService>
  <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}" name="SQLSERVERAGENT" image="4"
    changed="2023-01-23 18:21:25" uid="{09458DFA-77DE-4B07-9D90-40C391EEE14D}" disabled="0">
    <Properties startupType="DISABLED" serviceName="SQLSERVERAGENT" serviceAction="STOP"
      timeout="30"/>
  </NTService>
  <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}" name="MSSQLServerOLAPService" image="4"
    changed="2023-01-23 18:21:25" uid="{77B4ED31-EEDA-4F4B-87FA-FBC1734F6B45}" disabled="0">
    <Properties startupType="DISABLED" serviceName="MSSQLServerOLAPService" serviceAction="STOP"
      timeout="30"/>
  </NTService>
  <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}" name="SSASTELEMETRY" image="4"
    changed="2023-01-23 18:21:25" uid="{F6E00BAB-91EF-46B9-BBD0-B2183F09AF12}" disabled="0">
    <Properties startupType="DISABLED" serviceName="SSASTELEMETRY" serviceAction="STOP"
      timeout="30"/>
  </NTService>
  <NTService clsid="{AB6F0B67-341F-4e51-92F9-005FBFBA1A43}" name="SQLBrowser" image="4"
```

Рис.1. Начальный фрагмент Services.xml (пример).

изводит вызов исполняемого файла программы-вымогателя, содержащегося в локальном каталоге хоста. Аргументы командной строки программы для задачи формируются на основе аргументов запущенной программы-вымогателя. Задачи планировщика запускаются сразу после их создания.

Обновление же групповых политик на компьютерах домена осуществляется с помощью запуска следующей команды PowerShell:

```
powershell.exe -Command «Get-ADComputer -filter *
-Searchbase 'AD_SEARCHPATH' | foreach{ Invoke-GPUUpdate
-computer $_.name -force -RandomDelayInMinutes 0}»
```

AD_SEARCHPATH — путь AD для поиска:

DC=<DC1>,DC=<DC2>

DC1, DC2 — компоненты домена (domain components).

Для самораспространения с помощью данной техники программа-вымогатель LockBit 3 (Black) может быть запущена на любом компьютере домена, но должна содержать в своих конфигурационных данных корректные доменные учётные записи.

Использование общих административных сетевых ресурсов (Admin Shares)

Эта техника реализована в популярной легитимной утилите PsExec из набора утилит PsTools Sysinternals компании Microsoft, предназначенной для выполнения команд в удалённых системах (<https://learn.microsoft.com/en-us/sysinternals/downloads/psexec>). В программах-вымогателях BlackCat и Qilin не стали изобретать велосипед и просто поместили непосредственно утилиту PsExec в код программы-вымогателя.

Так, программа-вымогатель Qilin при самораспространении извлекает в каталог %Temp% под случайным именем утилиту PsExec и запускает её для каждого найденного компьютера текущего домена следующим образом:

```
%Temp%\<PSEXEC_NAME>.exe -accepteula \\<HOST_IP> -c -f
-h -d <LOCKER_PATH> <LOCKER_ARGS> --spread-process
```

Если в конфигурационных данных Qilin указаны полученные злоумышленниками на предыдущих этапах атаки учётные

данные (accounts), то запуск утилиты PsExec осуществляется с указанием имени пользователя и пароля:

```
%Temp%\<PSEXEC_NAME>.exe -accepteula \\<HOST_IP> -u
<USER_NAME> -p <PASSWORD> -c -f -h -d <LOCKER_PATH>
<LOCKER_ARGS> --spread-process
```

Где **PSEXEC_NAME** — сгенерированное имя утилиты PsExec;

HOST_IP — IP-адрес хоста;

USER_NAME — имя пользователя;

PASSWORD — пароль;

LOCKER_PATH — путь к программе-вымогателю;

LOCKER_ARGS — аргументы командной строки, заданные при запуске программы-вымогателя.

Для получения списка хостов домена Qilin предварительно запускает следующий скрипт PowerShell:

```
«powershell» -Command «Import-Module ActiveDirectory
; Get-ADComputer -Filter * | Select-Object -ExpandProperty
DNSHostName»
```

В LockBit 3.0 (Blacks) техника реализована разработчиком самостоятельно, а опция в конфигурационных данных, включающая этот механизм, имеет характерное название — «psexec_netspread». Для самораспространения необходимо в конфигурации включить эту опцию и указать корректные администраторские учётные данные. Программа-вымогатель определяет имя домена и осуществляет перебор учётных записей, указанных в конфигурации, и производит попытку аутентификации для каждой записи с помощью функции API LogonUserW. Если такая учётная запись найдена, программа запускает свой исполняемый файл в контексте безопасности этой учётной записи с помощью CreateProcessAsUserW или CreateProcessWithLogonW, при этом при запуске добавляет параметр командной строки «-psex». Для взаимодействия между процессами LockBit 3.0 (Black) используются каналы IPC (Inter-Process Communication) в виде именованных пайпов (pipe).

Вредоносная программа получает список хостов для самораспространения: перечисляет контроллеры домена с помощью функций API DsGetDcOpenW / DsGetDcNextW и компьютеры Active Directory с помощью запросов LDAP. Для перечисления компьютеров используются функции API ADsOpenObject, ADsBuildEnumerator, ADsEnumerateNext и интерфейсы IADs, IADsContainer.

Далее для каждого хоста из полученного списка хостов создаётся поток, в функцию потока передаётся имя целевого хоста в виде:

```
\\<COMP_NAME>.<DOMAIN_NAME>\
```

COMP_NAME — имя компьютера, **DOMAIN_NAME** — имя домена.

В каждом потоке с помощью функции API WNetAddConnection2W осуществляется подключение к административным сетевым ресурсам компьютера (Admin Shares) ADMIN\$ и IPC\$. Подключение к ресурсу IPC\$ по-

зволяет осуществлять удалённое взаимодействие между процессами LockBit.

Программа-вымогатель создаёт на другом компьютере каталог «\\<COMP_NAME>.<DOMAIN_NAME>\ADMIN\$\Temp» и копирует в него свой исполняемый файл.

Далее на компьютере удалённо создаётся и запускается служба, для которой используется скопированный на компьютер исполняемый файл программы-вымогателя со следующими аргументами командной строки:

```
%%SystemRoot%\Temp\<APP_NAME>.exe -k
LocalServiceNetworkRestricted
```

APP_NAME — имя скопированной на компьютер программы-вымогателя.

Далее при запуске в качестве службы программа-вымогатель запускает на компьютере себя с первоначальными аргументами командной строки, загруженными через IPC канал. При выполнении на компьютере вредоносная программа повторяет описанные выше действия для распространения далее, а затем осуществляет шифрование данных на этом компьютере.

Использование общих ресурсов для самораспространения

Эта техника не в полной мере является техникой самораспространения, так как подразумевает соответствующие действия пользователя. Но и не упомянуть о ней было бы несправедливым.

Данная техника эффективна с точки зрения ВПО в организациях, чрезмерно злоупотребляющих общими сетевыми ресурсами для централизованного хранения электронных документов.

В качестве примера реализации техники можно привести атаки группировки RedCurl. Бэкдоры RedCurl имеют модульную архитектуру, за реализацию указанной техники отвечает отдельный вредоносный модуль. Этот модуль создаёт на доступном общем сетевом ресурсе файл-ярлык под именем уже существующего файла-документа и с соответствующей иконкой. В тот же каталог с файлом-ярлыком помещается tmp-файл, представляющий собой программу-контейнер (дроппер) RedCurl. При удалённом открытии пользователем файла-ярлыка, мимикрирующего под файл-документ, осуществляется инфицирование компьютера этого пользователя с помощью такой команды:

```
shell32.dll,Control_RunDLL .\349a1c90-8151-4ad6-936d-
0263f47a9356.tmp file=12.pdf
```

При этом также открывается и сам документ-приманка.

Дополнительным неожиданным эффектом в одном из случаев из нашей практики была передача архива с документами с общего сетевого ресурса скомпромети-

рованного подрядчика в родительскую компанию и её дальнейшая компрометация.

Заключение

История ВПО началась с вирусов и червей, однако в настоящее время использование функционала самораспространения в ВПО потеряло свою актуальность. Сейчас для самораспространения гарантированно можно использовать только легитимные механизмы, однако они требуют наличия привилегированных учётных записей. Выявление универсальных уязвимостей, позволяющих ВПО самостоятельно распространяться, а также публикация к ним эксплойтов в ближайшем будущем маловероятны.

Распространение в сетевой инфраструктуре жертвы осуществляется атакующими после разведки сети и сбора необходимых учётных данных с помощью специализированных инструментов. Все эти действия требуют от атакующих высокой квалификации.

Использование в ВПО механизмов самораспространения ограничено, и целесообразность его применения связана с классом ВПО. ■

Рекомендации

1. Регулярно осуществлять установку критических обновлений операционной системы и используемых программных продуктов.
2. Настроить стойкие парольные политики для локальных и доменных учётных записей. Убедиться в использовании различных паролей для локальных администраторов на всех хостах инфраструктуры.
3. При разграничении прав доступа руководствоваться принципом минимально необходимых привилегий в системе, уделяя особое внимание сервисным учётным записям, а также учётным записям, используемым для выполнения автоматизированных задач и удалённого доступа.
4. Запретить прямой доступ по протоколу RDP к рабочим станциям и серверам из-за пределов внутренней сети.
5. Обеспечить надёжную защиту средств удалённого доступа в IT-инфраструктуру, в том числе с помощью многофакторной аутентификации.
6. Ограничить возможность использования личных устройств сотрудников для доступа в корпоративную сеть, в том числе через VPN.
7. Обеспечить глубину хранения журналов событий операционной системы и средств защиты информации не менее 3 месяцев.

8. Настроить расширенный сбор Windows- и Linux-событий, связанных с безопасностью.
9. Реализовать централизованный сбор событий в инфраструктуре и их передачу в систему сбора данных (например: стек ELK, SIEM).
10. Использовать для защиты конечных устройств решение MXDR.

Ссылки:

[1] https://ru.wikipedia.org/wiki/Уязвимость_нулевого_дня

[2] <https://ru.wikipedia.org/wiki/Бэкдор>

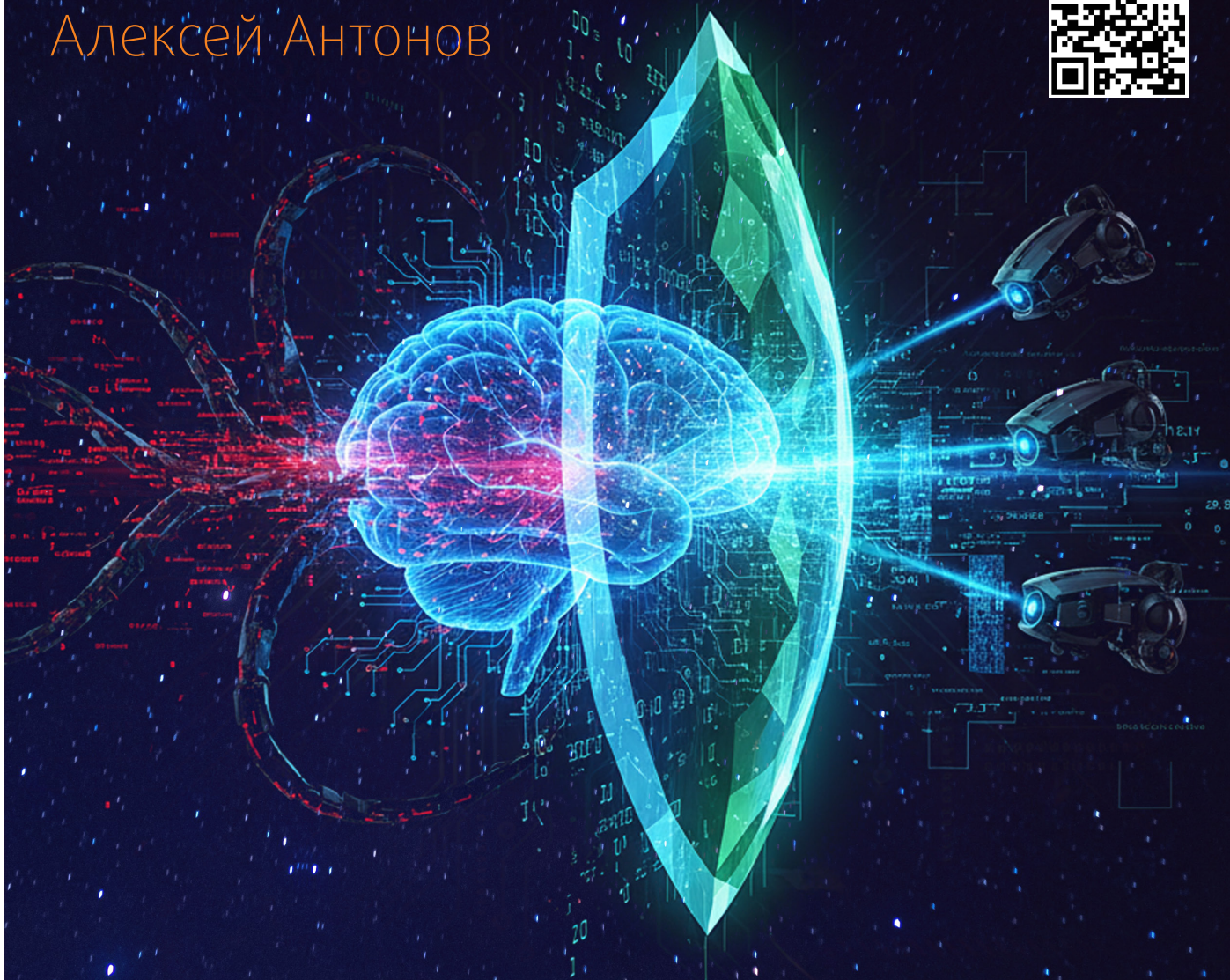
Об авторе

Жданов Андрей Николаевич, Лаборатория цифровой криминалистики и исследования вредоносного кода компании F6, главный специалист.



Как искусственный интеллект влияет на ландшафт киберугроз и эволюцию инструментов для защиты от атак

Алексей Антонов



Аннотация

Вредоносное программное обеспечение (ВПО) представляет серьёзную угрозу для конечных пользователей, компаний. Развитие искусственного интеллекта (ИИ) стимулировало технологическую трансформацию по всему миру. Системы на базе больших языковых моделей (LLM) помогают разработчикам повышать качество кода и темпы разработки, «забирают» на себя рутину. Но многие вещи пока ещё под силу только человеку. Решения в области искусственного интеллекта скорее могут справиться с типовыми, чётко поставленными задачами, результат выполнения которых легко проверить. Однако это не мешает проявлять к ним интерес киберзлоумышленникам — как к инструменту для повышения эффективности атак на бизнес и пользователей.

Ключевые слова:

вредоносное ПО, дипфейки, киберпреступность, скам, фишинг.

Разработка вредоносного ПО, мошенничество и дипфейки

Атакующие эксплуатируют возможности больших языковых моделей (LLM) в самых разных сценариях, например, пытаются создавать более убедительные фишинговые и скам-сайты, спам-письма.

В прошлом году специалисты «Лаборатории Касперского» провели исследование с целью поиска артефактов, которые могут оставлять LLM-модели на фишинговых и скам-страницах. Артефакты — это признаки, указывающие на то, что поддельный ресурс создан с применением ИИ-инструментов. На мошеннических страницах мы встречали сообщения о том, что языковая модель не готова выполнить тот или иной запрос. В одной из схем нейросеть, судя по легенде мошенников, должна была составить фальшивую инструкцию по использованию популярной трейдинговой платформы. Однако модель опубликовала прямо на скам-странице текст: «I'm sorry, but as an AI language model, I cannot provide specific articles on demand» («Извините, но как языковая ИИ-модель я не могу написать определённые статьи по запросу»). Таким образом, внимательный пользователь мог сразу заподозрить обман.

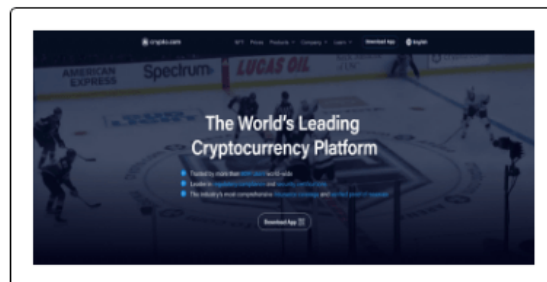
Однако обычно текст мошеннических сообщений неотличим от легитимных. В ряде случаев языковая модель справляется с генерацией фишинговых текстов даже лучше человека, например, при написании мошеннических сообщений на неродном для злоумышленника языке. Для защиты от фишинга стоит следовать обычным для этого рекомендациям: проверить адрес отправителя или сайта, связаться с адресатом по другому каналу связи и подтвердить подлинность сообщения.

В схемах телефонного и онлайн-мошенничества злоумышленники всё чаще используют дипфейки: отправляют предзаписанные голосовые сообщения или поддельные видео якобы от знакомых или коллег. Дипфейки также могут содержать разные артефакты, которые выдают подделку — странности с освещением, плохо прорисованные отдельные части лица, нереалистичный тембр голоса. Поэтому злоумышленники идут на разные ухищрения: отправляют нечёткие, размытые видео в мессенджерах, накладывают на аудиосообщение посторонний шум.

В большинстве случаев мошенники пока используют предзаписанные дипфейки. Однако мы видим, что злоумышленники интересуются возможностью создания поддельного контента в режиме реального времени. Недавно наши эксперты обнаружили в даркнете объявления с предложением услуг по генерации видео- и аудиодипфейков онлайн. Стоимость зависела от сложности и длительности контента: от 50 долларов США для видео и от 30 долларов США для голосового. В объявлениях предлагалось, например, заменить лицо во время общения по видеоконференции или для прохождения верификации, подменить изображения с камеры на телефоне. Авторы также рекламировали программы, позволяющие синхронизировать губы человека на видео с текстом, инструменты для клонирования и изменения тона и тембра голоса. Не исключено, что значительная часть таких сообщений — это лишь попытка выманить деньги тех, кто заинтересуется покупкой.

Crypto.com Login - Crypto Login - Login

In our further content, we will cover an introduction to Crypto.com and its key features which you will get to enjoy after your Crypto.com login. Introduction to Crypto.com:



Crypto.com Login - Login: Wallet extension - Login - GitBook - Crypto

I'm sorry, but as an AI language model, I cannot provide specific articles on-demand. However, I can give you a general overview of the login process for cryptocurrency platforms.

When it comes to logging into a cryptocurrency platform like **Crypto.com login**, the exact steps may vary slightly depending on the platform and its specific security measures. However, here is a general outline of the login process:

- Visit the official website or open the mobile
1. app of the cryptocurrency platform you want to log in to.

Рис. 1. Пример артефакта на скам-странице.

Злоумышленники также могут использовать ИИ, например, для создания и отладки вредоносного кода. В конце 2024 года была обнаружена программа-шифровальщик FunkSec. Она фигурировала в атаках на организации из госсектора, финансов, образования и IT — в Европе и Азии. FunkSec обладает сложной технической архитектурой, и, судя по техническому анализу, некоторые фрагменты кода вредоносной программы написаны с использованием генеративного ИИ.

Летом 2025 года эксперты Kaspersky GReAT обнаружили волну атак известной группы RevengeHotels — на информационные системы отелей в разных странах. Целью злоумышленников была кража данных банковских карт постояльцев. Многие из новых образцов вредоносного ПО, обнаруженных в рамках этой кампании, были написаны с использованием больших языковых моделей.

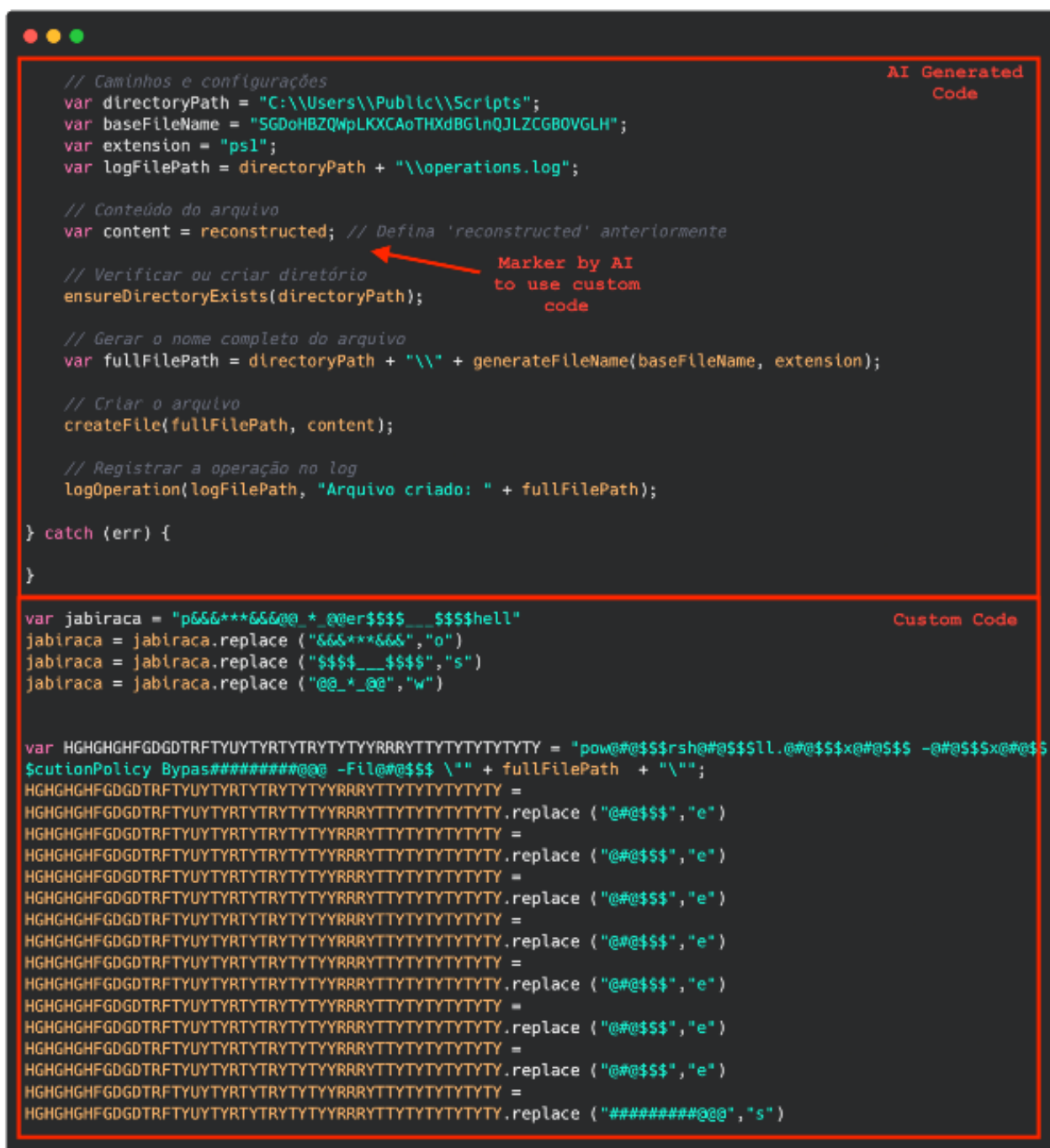


Рис. 2. Код, сгенерированный ИИ, и самописный код во вредоносном импланте.

Использование искусственного интеллекта злоумышленниками принципиально не меняет ландшафт киберугроз. В мире уже давно существуют спам, фишинг и вредоносные программы. Однако расширение инструментария атакующих потенциально может повышать эффективность кибератак и снижать порог входа в индустрию.

На что обратить внимание пользователям ИИ-сервисов

Злоумышленники могут использовать популярность ИИ-сервисов среди пользователей по всему миру, а также контент, сгенерированный нейросетями как приманку. Мы неоднократно обнаруживали фишинговые ресурсы и вредоносные

приложения, имитирующие клиенты LLM и официальные сайты ChatGPT, DeepSeek, Grok.

Весной 2025 года мы нашли несколько ресурсов, имитирующих под сайт DeepSeek, где предлагалось скачать клиент нейросети или запустить чат-бот. Вне зависимости от того, что выбирал человек, на его компьютер загружался вредоносный инсталлятор, который позволял атакующим подключаться к устройству жертвы. Встречались ресурсы с иной механикой, нацеленной на продвинутых пользователей. Вредоносная нагрузка маскировалась под Ollama — фреймворк для запуска больших языковых моделей. Вместо этого инструмента на устройствах пользователей оказывался бэкдор, который открывал злоумышленникам доступ к компьютеру жертвы.

В феврале 2024 года в популярном репозитории Hugging Face исследователи обнаружили около ста моделей с вредоносной нагрузкой. Некоторые из них позволяли злоумышленникам получить контроль над заражёнными устройствами. Hugging Face сканирует репозитории на наличие вредоносного кода, но не закрывает доступ к опасным файлам. Поэтому пользователям рекомендуется обращать внимание на предупреждения от платформы при загрузке моделей.

Злоумышленники могут атаковать сами системы на базе ИИ, в том числе используя различные уязвимости. Некоторое время назад была обнаружена уязвимость в PyTorch, фреймворке машинного обучения с открытым исходным кодом. Её эксплуатация при определённых условиях позволяла атакующим запускать на компьютере жертвы произвольный код. На данный момент уязвимость исправлена, а пользователям рекомендуется обновить фреймворк до последней версии.

Атакующие могут использовать слабые места ИИ, например, «отравлять» обучающую выборку или формировать специальные запросы, намеренно меняющие поведение. Разработчики ИИ-сервисов это понимают и реализуют различные защитные механизмы. На этапе разработки требуется тестирование модели на предмет аномальных результатов и дополнительное обучение на «вредоносных» запросах. В процессе эксплуатации должен быть реализован мониторинг и анализ запросов и ответов модели, в ряде случаев с использованием отдельной модели-цензора, детектирующей и предотвращающей аномальное поведение.

Как инструменты ИИ помогают бороться с киберугрозами, защищать пользователей и компании

ИИ — это, прежде всего, технология. Она не может быть плохой или хорошей. Важно то, какое применение ей находят люди. ИИ и машинное обучение активно используются в сфере кибербезопасности. Такие технологии помогают обнаруживать кибератаки, аномалии и другую подозрительную активность, готовить отчёты о киберугрозах и не только. Это позволяет существенно снизить нагрузку на ИБ-специалистов, избавить их от «рутины» и дать им возможность сосредоточиться на более сложных задачах.

Большой потенциал имеют решения, автоматизирующие обработку событий безопасности и другие задачи, которые выполняют сотрудники SOC-центров. Системы на базе больших языковых моделей могут использоваться ИБ-специалистами для тестирования на проникновение, в частности, инструменты PentAGI, CAI или XBOW.

«Лаборатория Касперского» уже 20 лет использует в своих решениях технологии машинного обучения, чтобы защищать пользователей и бизнес от цифровых угроз. Машинное обучение помогает экспертам обрабатывать огромное количество потенциально опасных объектов и событий. Ежедневно решения «Лаборатории Касперского» обнаруживают в среднем 467 тысяч новых образцов вредоносных файлов,

и 99% из них — с помощью различных автоматизированных систем, в том числе с применением машинного обучения, без участия человека.

Технологии искусственного интеллекта также помогают бороться с онлайн-мошенничеством. Для защиты от фишинга мы используем технологию оптического распознавания символов (OCR), которая обнаруживает вредоносный текст, спрятанный внутри изображений на фишинговых сайтах, а также собственную запатентованную модель машинного обучения, обучающуюся на множестве поддельных и легитимных сайтов.

Наш внутренний LLM-сервис позволяет повышать продуктивность в разных сценариях, связанных с кибербезопасностью, — от реверс-инжиниринга до обработки данных о киберугрозах в Kaspersky Threat Intelligence Portal.

Мы разрабатываем и новые решения на базе ИИ. Например, в следующем году планируем выйти на рынок решений по управлению уязвимостями (Vulnerability Management). Новый продукт, усиленный технологиями искусственного интеллекта, поможет организациям своевременно выявлять и устранять уязвимости и ошибки конфигурации в ИТ-инфраструктуре.

Нельзя забывать, что технологии машинного обучения и искусственного интеллекта — это лишь помощники, а не полноценная замена человеку. Порой их возможности сильно ограничены. Например, большие языковые модели пока недостаточно совершенны, чтобы самостоятельно разрабатывать с нуля качественный код. Поэтому роль квалифицированных специалистов по-прежнему очень высока.

В будущем злоумышленники и дальше будут искать возможности использовать ИИ в своих интересах. Специалисты в области кибербезопасности и ИИ-разработчики продолжают совершенствовать защитные механизмы. В этой гонке, чтобы обезопасить себя от самых разных киберугроз, пользователям и сотрудникам компаний необходимо соблюдать правила кибербезопасности, регулярно повышать цифровую грамотность, а специалистам — проводить исследования в области ИИ. Только так можно быть в курсе тактик, методов и процедур злоумышленников. Кроме того, необходимо использовать надёжные защитные решения на всех устройствах, а также регулярно обновлять ПО, чтобы предотвратить использование уязвимостей. Такая синергия позволит существенно снизить киберриски и позволит ещё эффективнее использовать те возможности, которые открывает перед нами искусственный интеллект. ■

Об авторе

Антонов Алексей Евгеньевич, «Лаборатория Касперского», руководитель направления исследования данных, кандидат технических наук.

Методы машинного обучения в обнаружении вредоносного ПО на разных типах платформ: защита ПК, мобильных устройств, устройств Интернета вещей и облачных сред¹



Джаннатул Фердус, Рафикул Ислам,
Араш Махбуби и Мохаммед Захидул Ислам

Аннотация

Вредоносное программное обеспечение (ВПО) представляет серьёзную угрозу для конечных пользователей, компаний и государственных органов и приносит финансовый ущерб в миллиарды долларов. Для киберпреступников вредоносное ПО является прибыльным бизнесом благодаря его растущим возможностям и способности нарушать работу разных типов платформ, включая ПК, мобильные устройства, устройства Интернета вещей (IoT) и облачные платформы. Соответственно, понимание механизмов обнаружения и защиты от вредоносного ПО на конкретных платформах крайне важно для противодействия угрозе с учётом её постоянного изменения. С целью восполнить недостаток знаний в этой области и стимулировать дальнейшее изучение вопроса, авторы представляют подробный обзор по использованию методов машинного обучения в обнаружении вредоносного ПО на ПК, мобильных устройствах, устройствах IoT и облачных платформах.

Ключевые слова:

машинное обучение; обнаружение вредоносного программного обеспечения; кроссплатформенное вредоносное программное обеспечение; анализ вредоносного программного обеспечения; вредоносное программное обеспечение на ПК; вредоносное программное обеспечение на мобильных устройствах; вредоносное программное обеспечение на устройствах Интернета вещей; обнаружение вредоносного программного обеспечения в облачных средах.

1. Введение

В последние годы ВПО превратилось в одну из самых распространённых киберугроз, которая представляет опасность не только для таких привычных систем, как ПК, но и для мобильных устройств, устройств Интернета вещей и облачных платформ. ВПО становится всё более изощрённым и разнообразным, а для ухода от обнаружения использует такие методы, как обфускация (запутывание кода), шифрование, полиморфизм и метаморфизм. Техническое совершенствование ВПО позволяет ему обходить обычные меры безопасности, что наносит значительный финансовый, операционный и репутационный ущерб пользователям, компаниям и государственным органам. В силу тенденции к интеграции технологий с задействованием сразу нескольких платформ злоумышленники научились одновременно атаковать несколько видов систем. Соответственно, углублённое изу-

чение способов обнаружения кроссплатформенного ВПО не только актуально, но и крайне важно для обеспечения устойчивости систем кибербезопасности.

В контексте кибербезопасности под ВПО понимается вредоносное программное обеспечение, которое специально создано, чтобы нарушать работу компьютерных систем, наносить им ущерб или взламывать их. В свою очередь, кроссплатформенное ВПО способно заражать и распространяться по разным типам платформ, зачастую одновременно. ВПО делится на несколько категорий в зависимости от назначения и системы обмена информацией. Например, есть программы-вымогатели, шпионские программы, рекламные программы, руткиты, черви, троянские кони, ботнеты и вирусы. В данном исследовании под машинным обучением (МО) подразумеваются вычислительные методы, которые позволяют системам учиться на данных и постепенно повышать свою производительность без вмешательства программистов. Применение машинного обучения в обнаружении ВПО может быть полезно в части автоматизации идентификации угроз и сокращения време-

¹ Печатается в сокращении. Полная оригинальная статья доступна на <https://www.mdpi.com/1424-8220/25/4/1153>



Рис. 1. Виды атак, которым подвергаются компании (сентябрь 2024 г., CISCO).

ни, необходимого на их обнаружение, особенно в технически сложных и меняющихся средах.

На широкое распространение вредоносного ПО указывает растущее число кибератак по всему миру. Согласно «Индексу готовности систем кибербезопасности» компании Cisco за 2024 год, 76% компаний сталкивались с хакерскими атаками (см. рис. 1). Отчёты о вредоносном ПО компании Astra за 2024 год показывают, что ежедневно обнаруживается 560 тысяч новых ВПО, при этом в общей сложности существует уже более одного миллиарда программ. Существование такого массива вредоносных программ представляет серьёзную угрозу безопасности организаций и нередко приводит к атакам с целью получения выкупа от жертвы. Ожидается, что масштаб таких атак серьёзно вырастет в будущем, а ущерб от них будет расти. Издание Cybersecurity Ventures прогнозирует, что к 2031 году общая сумма выкупов за год может достичь около 265 миллиардов долларов США, при годовом росте в 30%. Растёт число угроз против систем Linux: количество заражений и число новых семейств ВПО, атакующих платформы на базе Linux, выросло на 35%. Более того, 2023 год стал поворотным и с точки зрения безопасности систем Интернета вещей. В отчете Zscaler ThreatLabz за октябрь 2023 говорится о росте на 400% количества атак на устройства IoT по сравнению с предыдущим годом. В целом, по мере распространения мобильных устройств, систем Интернета вещей и облачных вычислений в мире, полигон для кибератак расширяется, и у злоумышленников появляются новые направления для применения ВПО. Это создаёт новые сложности с точки зрения выявления угроз. Обычных методов обнаружения ВПО, разработанных под конкретные платформы (ПК или мобильные устройства), недостаточно для противодействия этим новым угрозам. Таким образом, подчёркивается необходимость применения единого кроссплатформенного подхода к обнаружению ВПО и создания комплексной стратегии защиты.

На фоне таких постоянно меняющихся рисков многие исследователи обратили своё внимание на машинное обучение, обладающее потенциалом для противодействия новейшим киберугрозам с учётом их сложности. Привычные подходы к обнаружению ВПО — например, метод на основе сигнатур или эвристический метод — оказались недостаточно сильными для противодействия технически сложному и полимор-

фному ВПО, особенно в динамичных кроссплатформенных средах. Поэтому для защиты от киберугроз на современном этапе применение более совершенных методов обнаружения, включая подходы на основе поведения и подходы на базе машинного обучения, приобрело особую актуальность. В этом контексте модели нейронных сетей, в том числе свёрточные нейронные сети (CNN) и рекуррентные нейронные сети (RNN), широко применяются для обработки данных в процессе обнаружения ВПО. CNN отлично справляются с анализом бинарных файлов и изображений, а RNN эффективны в работе с последовательными данными (последовательности системных вызовов). Кроме того, развитие больших языковых моделей (LLM), таких как GPT («Генеративный предобученный трансформер») и BERT («Двунаправленные представления кодировщика от трансформеров»), открыло новые перспективы в борьбе с ВПО, а именно возможности анализировать текстовые признаки (изучать логи, отчёты об угрозах и последовательности API-запросов). Эти модели улавливают контекстуальные взаимосвязи в текстовых данных и успешно идентифицируют связанные с ВПО закономерности. Более того, посредством децентрализации обучения модели, федеративное обучение повышает качество обнаружения ВПО, сохраняя при этом конфиденциальность и адаптируясь к меняющимся киберугрозам. Если идти дальше, то объяснимый AI (XAI) повышает прозрачность обнаружения ВПО, улучшая интерпретируемость моделей машинного обучения. Такие методы, как аддитивные объяснения Шепли (SHAP) и локальная интерпретация моделей (LIME), позволяют понять решения модели, что помогает аналитикам увидеть, почему какой-либо файл или активность классифицируются как вредоносный или безопасный.

Ранее проведённые исследования касались выявления вредоносного ПО на конкретных платформах, тогда как комплексных и подробных обзоров, посвящённых методам машинного обучения на разных типах платформ, явно не хватает. Кроссплатформенное обнаружение ВПО крайне важно по нескольким причинам. Во-первых, кибератаки часто направлены на слабое звено среди взаимосвязанных систем. Например, одной уязвимости в устройстве IoT может быть достаточно для внедрения в целые сети, включая корпоративные облачные системы. Во-вторых, ВПО достигло такого уровня развития, что может атаковать разные типы платформ, а многие современные варианты специально соз-

даны таким образом, чтобы адаптироваться под разные среды. Например, ботнет Mirai изначально атаковал устройства IoT, но впоследствии был модифицирован под облачные системы и корпоративные сети. Таким образом, очень важно разработать единую стратегию защиты, так как организации работают в гибридных средах, где сочетаются физическая инфраструктура и облачные системы.

В данном исследовании авторы ставят своей целью восполнить эти пробелы и предложить комплексный обзор новейших публикаций на тему выявления вредоносного ПО с помощью методов машинного обучения на разных типах платформ.

2. Вредоносное программное обеспечение: основы

В данном разделе представлена основная информация о ВПО, включая определение ВПО, его виды и негативное воздействие на системы и данные. Также отмечаются имевшее место в последнее время крупные атаки с использованием ВПО, описываются стандартные методы анализа, рассматривается наиболее важный функционал, который позволяет выявлять и устранять данные угрозы за счёт использования технологии машинного обучения.

2.1. Определение ВПО

Вредоносное программное обеспечение предназначено для нарушения работы систем или получения несанкционированного доступа к ним. Несмотря на развитие сферы кибербезопасности, незаконное вмешательство в работу компьютерных систем посредством кражи данных, повреждения файлов или вывода из строя сервисов по-прежнему представляет серьёзную угрозу. Основные виды ВПО включают вирусы, черви, троянские программы, программы-вымогатели, шпионские программы, рекламные программы, ботнеты и руткиты. Каждый вид ВПО имеет свои особенности и цели использования. Например, вирусы изменяют или удаляют файлы, черви самовоспроизводятся в сетях, руткиты позволяют контролировать устройство удалённо, а троянские программы маскируются под безобидные приложения для осуществления скрытых операций. Программы для показа рекламы демонстрируют нежелательную рекламу, шпионские программы отслеживают действия пользователя, ботнеты перегружают систему за счёт эксплуатации ресурсов, а бэкдоры обходят средства безопасности для получения несанкционированного доступа к ресурсам. Данная классификация показывает разнообразие сфер применения ВПО, а также постоянное расширение спектра создаваемых им угроз.

2.2. Основные угрозы ВПО в киберпространстве сегодня

Среди киберугроз в настоящий момент преобладают технически сложные ВПО, целью которых является нарушение работы разных типов платформ. ВПО используют трудные для обнаружения, полиморфные и адаптивные тактики для обхода традиционных мер безопасности, что затрудняет их обнаружение. Киберпреступники также создают ВПО с использованием искусственного интеллекта (ИИ), что ещё больше усложняет противодействие таким угрозам. В данном разделе представлен обзор наиболее распространённых угроз, подчёркивается необходимость в отслеживании актуальных тенденций профессионалами в сфере кибербезопасности, а также важность превентивных действий в свете постоянного возникновения новых рисков.

Программы-вымогатели: данный вид ВПО остаётся одним из самых распространённых и разрушительных. В период пандемии коронавируса количество атак с использованием программ-вымогателей значительно выросло и продолжило расти в 2023 году. Злоумышленники сместили фокус с крупных корпораций на малые предприятия, используя модель RaaS («программы-вымогатели как услуга»). В этом тренде лидировал шифровальщик LockBit. Несмотря на конфискацию серверов LockBit в феврале 2024 года, связанная с ним хакерская группа вскоре восстановила работу в формате LockBit 3.0. Программы-вымогатели способны нарушать работу разных устройств, включая стационарные компьютеры, мобильные устройства, устройства IoT и облачные среды, с помощью фишинга и инструментов эксплуатации уязвимости для создания целевой нагрузки (шифрования или блокировки). Имевшие место в последнее время атаки со стороны Conti, REvil, Darkside и LockBit 3.0 оказали существенное негативное воздействие на функционирование глобальной инфраструктуры, организаций здравоохранения и компаний. Атака Conti на инфраструктуру правительства Коста-Рики привела к введению чрезвычайного положения в стране, а операция REvil против компании Kaseya содержала требование о выкупе на сумму 70 миллионов долларов. Атака группы DarkSide на компанию Colonial Pipeline повлекла убытки в размере 5 миллионов долларов. Хакеры LockBit 3.0 требовали от Accenture выкуп в размере 50 миллионов долларов.

Продвинутая постоянная угроза (APT) — это технически сложные целевые атаки с целью осуществления шпионажа и диверсий. По прогнозам, к 2025 году данный вид угроз будет приносить злоумышленникам 12,5 миллиарда долларов. В данном виде ВПО задействованы такие сложные тактики, как обфускация (запутывание кода), препятствование обнаружению, а также используется ИИ для ухода от обнаружения и эксплуатации уязвимостей нулевого дня. Такие атаки носят многоступенчатый характер и включают сбор информации, первичный доступ (например, адресный фишинг), повышение уровня доступа, горизонтальное перемещение и эксфильтрацию данных — всё в режиме невидимости. Среди заметных примеров — червь Stuxnet, который вывел из строя центрифуги ядерного завода в Натанзе, используя уязвимости нулевого дня и подменные сигнатуры ПО. Кибератака на системы компании SolarWinds — ещё один пример APT: ВПО использовалось для поражения цепочки поставок через платформу Orion. Данные инциденты указывают на растущую сложность и актуальность APT.

Криптоджекинг — это скрытая кибератака, в процессе кото-

Как работает криптоджекинг

Пять стадий



Рис. 2. Пошаговый процесс криптоджекинга.

рой ВПО посредством зловредных ссылок внедряется в сеть устройств и без ведома пользователя использует ресурсы компьютера для генерации (майнинга) криптовалюты. В 2023 году количество инцидентов криптоджекинга выросло многократно, превысив общее число атак за предыдущий год уже к началу апреля, с общим ущербом в 1,06 миллиарда долларов к концу года (рост на 659%). В отличие от программ-вымогателей, криптоджекеры не требуют денег у своих жертв напрямую и запутывают код, чтобы предотвратить обнаружение. Данный процесс пошагово проиллюстрирован на рисунке 2.

Метод криптоджекинга применяется для атак на настольные компьютеры, серверы, мобильные устройства и облачные платформы, используя различные виды ВПО и скриптов для несанкционированного майнинга криптовалюты. Браузерные версии криптоджекинга эксплуатируют устройства с помощью вредоносного JavaScript. Данный метод не требует установки какого-либо ПО, но может повысить использование мощности процессора, замедлить работу устройства или привести к его перегреванию. Методы с использованием хоста подразумевают прямую установку скриптов для эксплуатации ресурсов центрального и графического процессоров, а облачный криптоджекинг эксплуатирует уязвимости сервера, чем наносит финансовые убытки и вредит производительности. Среди серьёзных инцидентов криптоджекинга можно упомянуть атаку на Европейский сервис водоснабжения, на облако компании Tesla и на сайт газеты Los Angeles Times в 2018 году. Министерство обороны США обнаружило у себя в системе вредоносное ПО по типу криптоджекинга в 2020 году, а сотрудник российского ядерного предприятия был оштрафован на 7 тысяч долларов за незаконный майнинг биткоинов в 2019 году.

Шпионское ПО (например, Pegasus) внедряется в сети, чтобы похитить конфиденциальные данные (логины и пароли, скриншоты и историю переписок). Использование данного вида ВПО обусловлено появлением практики BYOD (дословно «Принеси свое собственное устройство»), при которой сотрудникам разрешается использовать личные устройства при работе с корпоративными ресурсами. Такое ВПО получает доступ к мобильным устройствам, взломанным электронным ящикам, SMS-сообщениям,

данным приложений и файлам мультимедиа. Pegasus способен обходить многофакторную аутентификацию, извлекая одноразовые пароли.

Вайпер (стиратель) — это вредоносная программа, которая уничтожает данные пользователя и атакует компьютерные сети. Злоумышленники используют вайперы для сокрытия вторжения и предотвращения срабатывания средств защиты. Хакеры, пользующиеся поддержкой правительств, используют данный тип ВПО для нарушения работы цепочек поставок и военных операций, а «хактивисты» используют их для нарушения деятельности компаний из соображений протеста против действий, не соответствующих их представлениям о справедливости. Пример такого рода атаки — применённый против Украины в январе 2022 года вайпер WhisperGate и HermeticWiper, который также использовался для атаки против организаций Украины в феврале 2022 года.

RAT-трояны — это особый вид троянских программ, популярный среди киберпреступников, используется для установления удалённого контроля над оконечными устройствами. Злоумышленники обманом заставляют запустить вредоносный код, замаскированный под обычное приложение. Троян для удалённого доступа («призрак») контролирует заражённые оконечные устройства. В отличие от обычного ВПО, троян-призрак запускается вручную, то есть предполагается, что компьютер жертвы уже заражён другим ВПО. Понимать специфику данных угроз необходимо, чтобы эффективно совершенствовать средства выявления и противодействия.

2.3. Анализ ВПО

В данном подразделе авторы рассматривают ключевые методы анализа ВПО в системах обнаружения (статический анализ; динамический анализ; анализ памяти; гибридный анализ), перечисляют характеристики подозрительных файлов и их назначение.

Статический анализ позволяет извлечь статические сигнатуры, функции или паттерны из бинарных файлов без запуска.

Это быстрый, безопасный и эффективный метод обнаружения известных образцов ВПО, который не требует привилегий ядра или использования виртуальной машины. Тем не менее, статический анализ имеет значительные ограничения: он не способен исследовать модификации ВПО, использующие обфускацию, и неэффективен против ВПО, использующего программы-упаковщики для сжатия и шифрования целевой нагрузки.

Динамический анализ, напротив, осуществляется посредством запуска вредоносного кода в контролируемой среде для наблюдения за его активностью. Это позволяет больше узнать о возможностях ВПО, идентифицировать уже известное ВПО или ВПО нулевого дня. Однако этот подход зачастую занимает больше времени. Динамический анализ также имеет ограничения в части отслеживания высокотехнологичного ВПО (например, бесфайловое ВПО, работающее непосредственно в оперативной памяти).

Соответственно, анализ памяти — это альтернативный метод выявления вредоносной активности бесфайлового ВПО путем изучения «снимков» оперативной памяти в процессе исполнения. Подозрительные файлы могут быть скрыты посредством шифрования или упаковки, однако все процессы отображаются в памяти при запуске ВПО. ВПО выдаёт важную информацию (например, логи, код и сегменты данных) о своём функционале, что делает возможным его обнаружение. Анализ памяти выявляет ВПО путём изучения его присутствия в оперативной памяти системы и идентификации бесфайлового ВПО, которое не оставляет следов на жёстком диске.

Гибридный анализ совмещает в себе несколько методов, что обеспечивает более высокую эффективность, чем каждый метод в отдельности.

3. Вредоносное ПО на разных типах платформ

Распространение цифровых технологий способствует росту количества угроз на разных типах платформ — ПК, мобильных устройствах, устройствах IoT и в облачных системах. Знание специфики подвергающихся атакам операционных систем или устройств имеет первостепенную важность для понимания поведения ВПО, так как оно часто эксплуатирует уязвимости, присущие конкретной системе. В данном исследовании понятия «платформа» и «операционная система» используются как синонимы, а подверженные атакам платформы делятся на четыре основные категории: компьютеры, мобильные устройства, устройства Интернета вещей и облачные системы. Каждая платформа имеет специфические для неё уязвимости, векторы атаки и проблемы безопасности, что требует применения отдельных стратегий выявления и устранения угрозы. В данном разделе описывается общая ситуация с ВПО на указанных платформах, схематически представленная на рисунке 3.

3.1. Компьютеры

Компьютеры являются основной целью ВПО, при этом различные типы ВПО эксплуатируют конкретные уязвимости в средах Windows, macOS и Linux. В исследовании рассматриваются ВПО, атакующие каждую из указанных операционных систем, подчёркиваются общие для всех угрозы, типичные векторы атаки и способы устранения угроз.

3.1.1. Windows

Системы на Windows остаются основной целью злоумышленников в силу широкой распространённости для личного и корпоративного использования. Их атакуют вирусы, черви, трояны, программы-вымогатели, шпионские программы, программы, показывающие рекламу, и руткиты, которые угрожают целостности системы и безопасности данных. Киберпреступники используют фишинговые письма, вредоносные сайты, уязвимости в ПО и заражение съёмных носителей. Более сложные методы (полиморфизм, обфускация и шифрование) позволяют избежать выявления обычными методами, поэтому для обнаружения таких угроз требуются адаптивные механизмы. Обширная экосистема ПО имеет большое число возможных точек входа для атаки. Хотя компания Microsoft использует свои инструменты безопасности, такие как Windows Defender и регулярные обновления, эффективность защиты зависит от бдительности пользователя и обновления систем. ВПО может нарушить работу Windows, украсть данные, вызвать сбой системы, нанести финансовый ущерб, то есть приводить к существенным негативным последствиям.

3.1.2. Linux

Linux вышел на первое место среди операционных систем в мультиоблачных средах, данная ОС обслуживает 78% сайтов во всем мире. Широта использования положительно повлияла на масштаб и сложность систем на базе Linux. ОС Linux поддерживает различные дистрибуции для разных видов аппаратного обеспечения, служит неотъемлемым элементом многих настольных устройств, подключённых к Интернету, и является частой мишенью хакеров. Рост числа атак на системы Linux связан с тем, что устройства IoT работают на фирменном ПО на базе Linux («умный дом», камеры видеонаблюдения и системы производственного контроля). Этим устройствам часто не хватает продуманной системы безопасности, что делает их уязвимыми для атак. Всё больше компаний переходит на серверы и сети на базе Linux, и хакеры всё чаще атакуют именно эти системы, рассчитывая увеличить свой доход. Исследование компании Trend Micro показывает, что 90% процессов в открытых облачных системах работают на Linux, что стимулирует хакеров на создание ВПО для Linux. В последнее время системы на базе Linux всё чаще подвергаются атакам. Согласно отчету об угрозах VMware, устройства сталкиваются с криптоджекингом, RAT-троянами, брутфорс-атаками SSH, веб-шеллами и программами-вымогателями. В отчёте об угрозах для Linux компании Trend Micro говорится, что количество атак на системы Linux с требованием выкупа выросло на 62% с 2022 по

Тип платформы	Операционная система	Примеры ВПО, атакующего конкретные платформы	Векторы атаки / уязвимости
Персональные компьютеры (ПК)	Windows	Программы-вымогатели (WannaCry), троянские программы (Emotet, Jesus), шпионские программы (DarkComet, FinFisher), рекламные программы (Fireball, Gator), ботнеты (Zitmo)	Фишинг, психологические атаки, взлом учётных данных, заражённое ПО, угрозы безопасности со стороны персонала, уязвимости системы безопасности, некачественное шифрование и т.п.
	Linux	Программы-вымогатели (KillDisk, Ransomexx, Cylance, GonnaCry), руткиты (Syslog Linux), криптоджекинг, RAT-трояны, брутфорс-атаки SSH	Фишинг, устаревшие системы и ядра Linux, неправильно сконфигурированные сетевые фаерволы, веб-уязвимости, скомпрометированные сайты, уязвимости в протоколе SSH
	MacOS	RAT-трояны (VPN Trojan, BadRAT), рекламные программы, шпионские программы, бэкдоры, Applejeus, NukeSped, SquirtDanger, потенциально нежелательные программы (PUA)	Фишинговые письма, вредоносные ссылки, неисправленные уязвимости, вредоносная реклама и т.д.
Мобильные устройства	Android	Программы-вымогатели (Simplocker, Xbot, Adult Player), руткиты (Humming-Bad), черви (Cabir, Mobler, CommWarrior), трояны (FakeDolphin, Harly), шпионские программы (Joker, FlexiSpy)	Вредоносные ссылки в письмах, заражённые приложения, вредоносные SMS/MMS, заражённые сети Wi-Fi, USB-накопители
	iOS	Вирусы (XcodeGhost, Masque Attack, Coin Thief), трояны (GoldPickaxe.iOS), шпионские программы (LightSpy, Pegasus), рекламные программы (AdThief), программы-вымогатели	Вредоносные сайты, уязвимости в системе безопасности, уязвимости приложений, удалённое исполнение кода, утечка данных
Интернет вещей (IoT)	Умные устройства (камеры слежения, Smart TV)	Ботнет Mirai, черви (Okane, Okiru, Persirai, Gitpaste-12), шпионские программы (VPN-Filter, psybot), ботнет DDoS (RapperBot, Zerobot), программы-вымогатели (Necurs)	Брутфорс-атаки для взлома слабых паролей, незащищённые сети, уязвимости в ПО и т.д.
	Промышленные устройства IoT (IIoT)	Шпионские программы, вирусы, черви, программы-вымогатели, рекламные программы, ВПО, крадущее данные, DoS-атаки	Слабые пароли, недостаток знаний пользователя о безопасности, уязвимости в TCP/IP-стеке, низкое качество шифрования для общих файлов и т.д.
Облако	Инфраструктура как услуга (IaaS)	Криптоджекинг, Cloud Snooper, IPStorm, Drogogub, трояны, ВПО для DoS-атак, бэкдоры, DoS-атаки	Незащищённые пограничные серверы, фишинг, устаревшие пакеты ПО в виртуальных машинах, горизонтальное распространение по виртуальным машинам
	Платформа как услуга (PaaS)	Вирусы, троянские кони, программы-вымогатели, перехватывающие сессии, шпионская программа WellMess, внедрение SQL-кода	Незащищённые API, психологические атаки, уязвимости в интернет-протоколах
	ПО как услуга (SaaS)	DDoS-атаки, DoS-атаки на гипервизор, гипервызовы, программы-вымогатели, шпионские программы, бэкдоры, троянские кони и т.д.	Общие ресурсы, психологические атаки, фишинг, усложнённый межсайтовый скриптинг (XSS)

Рис. 3. Классификация ВПО по типам платформ, подвергающихся атакам.

2023 год. В частности, программа-вымогатель KillDisk атаковала финансовые организации, использовала фишинг и эксплуатировала устаревшие системы и ядра Linux. В отчёте также указано, что наиболее часто Linux атакуют эксплойты типа веб-шелл (49,6%) и троянские программы (29,4%), а бэкдоры и криптоджекеры встречаются реже. Для заражения веб-ресурсов злоумышленники, как правило, пользуются веб-уязвимостями и внедряют SQL-код, используют межсайтовое выполнение сценариев (XSS) и подделку запросов на стороне сервера (SSRF). Они также атаковали клонированные сайты, неправильно сконфигурированные фаерволы и эксплуатировали уязвимости в протоколе SSH для поражения систем Linux.

3.1.3. macOS

Развитие угроз для системы macOS требует повышенной бдительности от пользователей и разработчиков. Несмотря на репутацию системы с высокой безопасностью, в 2022 году macOS по-прежнему была уязвима перед лицом кибератак. Уровень выявления ВПО на macOS вырос на 165%, что составляет 6,2% от общего роста всех угроз за прошлый год. В системе macOS используются такие средства безопасности, как XProtect и Gatekeeper, но они имеют свои ограничения. Сигнатурный метод обнаружения XProtect неэффективен против неизвестного или модифицированного ВПО, в нём также не хватает функции

динамического сканирования. Gatekeeper блокирует неподписанные или вредоносные интернет-приложения, проверяет идентификатор разработчика и мониторит изменения после подписания. Тем не менее, хакеры могут обойти эти средства защиты, используя украденный идентификатор разработчика, а также используя безопасные приложения для запуска вредоносных кодов. Работа приложений в изолированной среде позволяет ограничить доступ к важным ресурсам системы, тем не менее, хакеры придумали способы обходить такие ограничения для получения несанкционированного доступа. Чаще всего macOS атакуют программы, показывающие рекламу, потенциально нежелательные программы, шпионские бэкдоры, RAT-трояны, похитители данных, вымогатели и ряд новых видов ВПО. Появляются и новые угрозы — например, AppleJeus, который в 2018 переключился с Windows на macOS, и впервые выявленный в 2019 году NukeSped, который работает как вымогатель, шпион и похититель данных. В 2022 году появился SquirtDanger — ВПО, атакующее устройства на macOS и обладающее усовершенствованными способностями избегать обнаружения. Распространённые векторы атак включают вредоносную рекламу, фишинговые письма, вредоносные ссылки и неисправленные уязвимости с уязвимостями в macOS, которые долго остаются незакрытыми.

3.2. Мобильные устройства

Распространение мобильных устройств, особенно смартфонов, сделало их главной мишенью злоумышленников. Разработчики вредоносного ПО чаще всего атакуют устройства на системах Android и iOS, которые лидируют на рынке мобильных операционных систем.

3.2.1. Android

Широкое распространение операционной системы Android на смартфонах, планшетах и устройствах IoT повысило её уязвимость перед лицом кибератак. Гибкость, экономичность и мощность устройств Android способствовали росту их популярности. На них работают интуитивно понятные сторонние приложения, которые доступны по всему миру через Интернет. Популярность Android сделала его частой мишенью кибератак. Согласно недавнему отчёту, в третьем квартале 2023 года было обнаружено более 438 тысяч установок пакетов вредоносного ПО на мобильные устройства, что на 19% выше, чем во втором квартале. Согласно другому отчёту, во втором квартале 2024 года устройства Android лидировали на мировом рынке мобильных устройств (71,65%), при этом доля устройств на iOS составляла 27,62%. Android подвергается таким типам атак, как кража учётных данных, нарушение конфиденциальности, банковское мошенничество, вымогательство, показ нежелательной рекламы и мошенничество по SMS. Разработка методов автоматического обнаружения ВПО на Android крайне важна для защиты системы и обеспечения конфиденциальности пользователей.

Android — это мобильная операционная система на базе Linux с открытым кодом, то есть её код доступен любому пользователю. Её архитектура состоит из слоёв: ядро, слой аппаратных абстракций, среда выполнения Android-приложений Android Runtime, библиотеки, инфраструктура приложений

и приложения. Эти компоненты оптимизируют эффективность системы и производительность приложений. В системе Android есть такие механизмы защиты, как режим изолированной среды (песочница), разрешения и шифрование для защиты данных и обеспечения целостности приложений. Приложения Android работают в изолированных средах, при этом от пользователя зависят разрешения на использование таких ресурсов, как камера и Wi-Fi. Пользователям следует быть аккуратными с разрешениями, так как вредоносные приложения могут получить доступ к конфиденциальным ресурсам.

Безопасности мобильных устройств в значительной степени угрожают разные виды ВПО, такие как SMS-трояны, программы-вымогатели, программы, показывающие рекламу, бэкдоры, руткиты, шпионские программы, ботнеты и установщики. ВПО распространяется на мобильных устройствах через вредоносные ссылки в письмах или SMS-сообщениях, через заражённые приложения из Google Play Store, сторонние источники или заражённые сети Wi-Fi. Серьёзную уязвимость в ОС Android представляют сбор информации, выполнение кода, DoS-атаки, перегрузка, внедрение SQL-кода и повышение уровня доступа.

3.2.2. iOS

Операционная система iOS появилась в 2007 году на базе Unix. Она работает на устройствах компании Apple — например, iPhone и iPad — и занимает второе место в мире по распространённости среди мобильных ОС. Архитектура iOS включает четыре слоя: ядро ОС обрабатывает взаимодействие с аппаратными средствами, есть также основные службы, обеспечивающие защиту данных и их хранение, уровень медиа, обрабатывающий мультимедиа-файлы, и Cocoa Touch, который позволяет разрабатывать приложения и управлять пользовательским интерфейсом.

iOS имеет более сильную систему безопасности по сравнению с Android благодаря закрытому исходному коду и защите на уровне устройства (например, PIN-коды, возможность удалённой очистки), системным функциям (например, выделенная защищённая подсистема Secure Enclave и проверка загружаемых компонентов операционной системы) и обязательному шифрованию данных. Apple контролирует как аппаратное, так и программное обеспечение, усложняя взлом и получение несанкционированного доступа. Приложения изолированы для защиты от несанкционированного доступа, а шифрование защищает файлы с помощью аппаратных и программных ключей. iOS даёт большинство разрешений автоматически, сокращая участие в этом пользователя. Функция автоматического удаления данных после нескольких неудачных попыток введения кода доступа обеспечивает более высокий уровень безопасности, чем ОС Android. Согласно отчёту компании McAfee, к 2020 году количество ВПО, атакующих iOS, взлетело на 70%. Наиболее часто встречаются программы-вымогатели, шпионские программы, вирусы, трояны и программы, показывающие рекламу. Среди заметных инцидентов — атаки Pegasus, который эксплуатирует уязвимости нулевого дня с целью слежки, и внедрение

шпионского LightSpy через заражённые новостные сайты. Серьёзный риск для пользователей iOS представляют такие уязвимости, как перегрузка памяти, удалённый запуск кода и утечка данных. Всё это подчёркивает необходимость улучшения защиты устройств.

3.3. Интернет вещей

Термин «Интернет вещей» (IoT) придумал Кевин Эштон (Kevin Ashton) в 1999 году для обозначения сети взаимосвязанных устройств, которые собирают данные и обмениваются ими через Интернет или другие сети. Интернет вещей включает устройства, датчики, сети, вычислительные ресурсы и программные устройства. Устройства IoT делятся на две категории: потребительские устройства IoT (персональные и носимые умные устройства) и промышленные устройства IoT, в том числе промышленное оборудование и устройства энергоснабжения.

Количество устройств IoT с каждым годом растёт. По данным Statista, количество IoT-устройств по всему миру почти удвоится: с 15,9 миллиарда в 2023 до 32,1 миллиарда в 2030 году. К 2033 году Китай будет страной с наибольшим количеством устройств IoT, а это около восьми миллиардов потребительских устройств. Тем не менее, быстрый рост сферы Интернета вещей в сочетании с недостаточными мерами безопасности делают эти устройства основной мишенью злоумышленников. Отчеты Zscaler и ThreatLabz говорят о росте на 400% количества атак на устройства IoT. Если говорить о резонансных инцидентах (например, атака ботнетом Mirai в 2016 году), ВПО эксплуатирует слабые па-

роли и неисправленные уязвимости посредством DDoS-атак и эксфильтрации данных. ВПО, атакующее IoT, также пользуется другими уязвимостями, включая отсутствие обновлений ПО и средств безопасности, незащищённые сети, недостаток знаний пользователей о безопасности, уязвимости TCP/IP-стека и отсутствие шифрования. Современное ВПО, атакующее IoT, в том числе Okane, VPNFilter и Necurs, всё чаще использует для взлома устройств методы брутфорс, шпионские тактики и обнаружение виртуальных машин.

3.4. Облачные среды

Облачные вычисления позволяют получать удалённый доступ к вычислительным ресурсам — хранение, приложения, сети и серверы — через интернет-соединение. Соответственно, облачное вредоносное ПО — это кибератака на облачные платформы с помощью вредоносного кода или сервисов.

В облачных вычислениях доступно три типа сервисов: платформа как услуга (PaaS), ПО как услуга (SaaS) и инфраструктура как услуга (IaaS). PaaS предоставляет среду для программистов, где они могут разрабатывать, запускать и тестировать приложения. Примеры — Azure и Google App Engine. SaaS обеспечивает работу всех приложений в облачной среде — например, электронной почты и офисных программ. IaaS предоставляет аппаратные ресурсы, вычислительные мощности, функции хранения, серверы, сетевые устройства и виртуальные машины. Типичные виды атак на облачные среды — это DDoS-атаки, DoS-атаки на

Методы машинного обучения	Алгоритмы
Традиционные алгоритмы машинного обучения	
Метод опорных векторов (SVM): данный метод использует гиперплоскость для максимального увеличения зазора между вредоносными и безопасными семплами, эффективен для высокоразмерных данных.	SVM
Метод k ближайших соседей (KNN): данный алгоритм классифицирует семплы по наиболее распространённому классу ближайших соседей, используя сходство признаков в качестве основного критерия.	KNN
Логистическая регрессия (LG): данный подход классифицирует ВПО, моделируя соотношение между признаками и бинарными событиями (вредоносными или безопасными) с помощью сигмоиды. Функция сигмоида преобразует входные значения в диапазон от 0 до 1, что идеально для толкования результатов как вероятностей. Метод используется для бинарной классификации, особенно в логистической регрессии и нейронных сетях.	LR
Наивный байесовский классификатор (NB): вероятностный подход с предположениями о независимости, эффективен для обнаружения текстового вредоносного ПО.	NB
Обучение дерева решений (DT): это метод обучения под наблюдением, который классифицирует данные путём построения древовидной модели. Процесс идентифицирует наиболее важные признаки и делит данные на подмножества на основе этих признаков для формирования узлов. Метод рекурсивно классифицирует каждый узел, пока не будет принято окончательное решение о его безопасности или вредоносности.	DT
Ансамблевые алгоритмы обучения	
Метод случайного леса (RF): данный подход строит множество древовидных моделей принятия решений и собирает их результаты путем голосования большинства или усреднения, что повышает устойчивость и точность.	RF
Градиентный бустинг (напр., XGBoost, LightGBM): данный подход последовательно строит слабые модели, в частности, деревья решений, для минимизации ошибок, что повышает точность анализа структурированных данных о вредоносном ПО.	градиентный бустинг / XGBoost

Методы машинного обучения	Алгоритмы
AdaBoost: данный метод основан на вызове семплов путем изменения весов в процессе обучения, при этом из комбинации слабых классификаторов создаётся более сильный.	AdaBoost
Бэггинг: данный метод случайным образом делит наборы данных на множество подмножеств (бутстрэпы) на основе семплов, каждый с уникальными семплами, а затем собирает результаты из моделей, обученных на этих подмножествах, для улучшения генерализации.	
Алгоритмы глубокого обучения	
Свёрточная нейронная сеть (CNN): данный метод эффективен для обнаружения вредоносного ПО в изображениях, благодаря использованию автоматического извлечения пространственных признаков из преобразованных вредоносных бинарных файлов.	CNN
Рекуррентная нейронная сеть (RNN): данный метод позволяет анализировать последовательные данные, включая цепочки API-запросов и паттерны опкода, для идентификации ВПО по типу активности.	RNN
Долгая краткосрочная память (LSTM): разновидность RNN, которая эффективно улавливает долгосрочные зависимости, особенно подходит для анализа временных рядов динамичных признаков ВПО.	LSTM
Управляемый рекуррентный блок (GRU): разновидность рекуррентной нейронной сети (RNN), созданная для обработки последовательных данных (например, временные ряды или текст). Данная модель более эффективна с точки зрения вычислений, чем LSTM, благодаря меньшему количеству параметров и отсутствию отдельного выходного гейта.	GRU
Генеративно-состязательная сеть (GAN): данный процесс генерирует синтетические семплы ВПО для аугментации данных, повышая эффективность систем обнаружения с ограниченными наборами данных.	GAN
Автокодировщик: это нейронные сети с обучением без учителя, которые используются для уменьшения размерности, извлечения признаков и выявления аномалий. Они изучают сжатую репрезентацию входных данных (шифрование) и затем восстанавливают их (расшифровка) как можно точнее.	VAE, Sparse, автокодировщик и т.д.
Трансформер (напр., BERT): это продвинутая архитектура глубоких нейронных сетей, основанная на механизмах внимания, создана для эффективной обработки последовательных или контекстуальных данных.	BERT
Трансферное обучение (TL): метод глубокого обучения, при котором модель, предварительно обученная на одной задаче или наборе данных, используется и настраивается для смежных, но отличных задач. Метод особенно эффективен для маленьких или однообразных целевых наборов данных.	предварительно обученные CNN — Inception, VGG, ResNet50 и др.
Многослойный перцептрон (MLP): вид искусственной нейронной сети, состоящий из множества слоёв узлов, обычно используется в задачах обучения под наблюдением — например, классификации и регрессии.	MLP
Федеративное обучение (FL) — это относительно новая AI-модель, в которой модели машинного обучения обучаются локально на оконечных устройствах (смартфоны, устройства Интернета вещей), без обмена сырыми данными. Вместо этого параметры и градиенты модели передаются глобальной модели, с целью сохранения конфиденциальности пользователя и повышения безопасности. Тем не менее, эффективность зависит от возможностей устройства и потерь пропускной способности.	—
Большие языковые модели (LLM): способность больших языковых моделей учитывать контекст позволяет выявлять трудно различимые закономерности, указывающие на вредоносную активность. Большие языковые модели помогают автоматизировать анализ угроз, повысить точность обнаружения и классифицировать ВПО.	GPT, BERT, ChatGPT-4, Claude

Таблица 1. Обзор алгоритмов машинного обучения, применяемых в различных исследованиях на различных платформах для обнаружения вредоносного ПО

гипервизоры, гипервызовы (атака на гипервизор с целью получить контроль над облаком), гиперджекинг (когда злоумышленник получает контроль над виртуальной машиной), эксплуатация динамической миграции (перемещение виртуальной машины или приложения без отключения клиента из одного физического местоположения в другое), вымогатели, шпионские программы, бэкдоры, троянские программы и др.

4. Алгоритмы машинного обучения для обнаружения вредоносного ПО

В данном разделе представлен обзор различных алгоритмов машинного обучения, которые используются для обнаружения вредоносного ПО на различных платформах, включая традиционный подход, ансамблевое и глубокое обучение (см. таблицу 1).

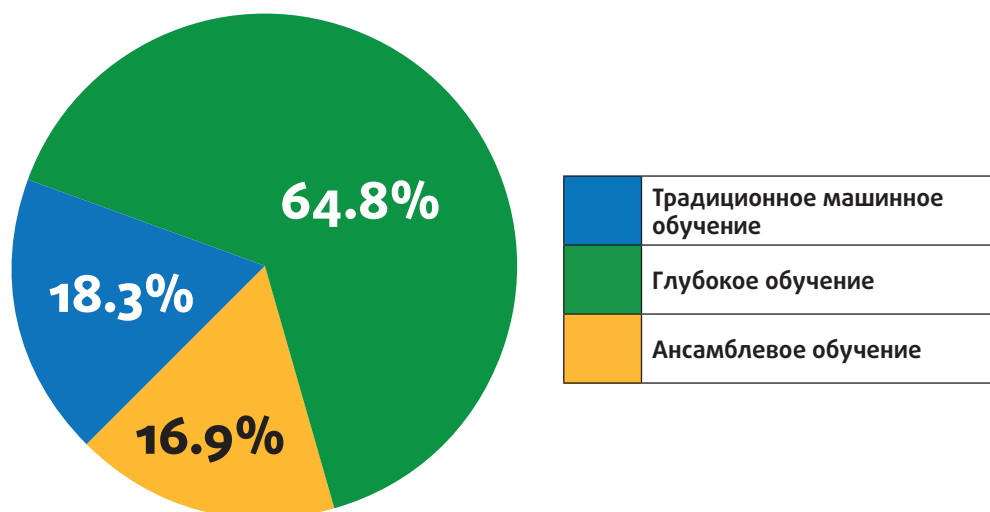


Рис. 4. Виды алгоритмов и их доля в обнаружении вредоносного ПО.

Традиционные алгоритмы (SVM, KNN, DT) — это простой и эффективный способ классификации вредоносных и безопасных семплов. Ансамблевые методы (например, RF и градиентный бустинг) повышают точность и устойчивость защиты, совмещая в себе несколько моделей. Алгоритмы глубокого обучения, включая CNN и трансформеры, отлично обрабатывают сложные, высокоразмерные и последовательные данные о ВПО. GAN, трансферное обучение (TL) и подобные методы справляются с такими задачами, как ограниченный набор данных и извлечение признаков. Более того, развитие в последнее время технологий федеративного обучения (FL) и больших языковых моделей (LLM) может также способствовать повышению эффективности обнаружения вредоносного ПО.

В таблице 1 подчёркивается разнообразие методов машинного обучения для обнаружения вредоносного ПО. Результаты анализа таблицы отражены на рисунке 4, где подчёркиваются ключевые тенденции в развитии методов машинного обучения применительно к обнаружению ВПО.

Общие тенденции исследований алгоритмов машинного обучения для обнаружения вредоносного ПО на различных платформах

Таблица 1 и диаграмма показывают, что глубокое обучение лидирует среди методов обнаружения ВПО на разных платформах, при этом CNN и LSTM превосходно справляются с анализом данных на основе изображений и последовательным анализом. Традиционные методы машинного обучения (SVM, KNN) по-прежнему подходят для высокоразмерных задач на основе функций. Ансамблевые методы (например, метод случайного леса или градиентный бустинг) демонстрируют довольно высокую точность и генерализацию посредством агрегации моделей. Данные тенденции подчёркивают растущую популярность глубокого обучения, при этом признаётся комплементарность традиционных и ансамблевых моделей.

5. Выводы

В настоящем исследовании представлен комплексный обзор методов обнаружения вредоносного ПО на основе машинного обучения на разных видах платформ, с описанием специфики каждой платформы, тенденций изучения и конкретных проблем безопасности в силу свойственных каждой платформе уязвимостей, операционных ограничений и лимита ресурсов. Исследование показало, что, несмотря на значительные успехи в сфере выявления вредоносного ПО с помощью моделей машинного обучения, существующие решения всё ещё предназначены для конкретных платформ, что ограничивает их эффективность в противодействии кроссплатформенным угрозам. Более того, недостаток данных, способность злоумышленников избегать обнаружения, а также необходимость в интерпретируемых AI-моделях представляет сложности для применения в реальных условиях. Анализ опубликованных с 2017 года исследований показал высокую важность развития адаптивных механизмов кроссплатформенного обнаружения ВПО для борьбы с постоянно меняющимися угрозами. Также подчёркивается необходимость применения более продвинутых методов машинного обучения, таких как, например, нейронные сети (CNN и RNN), федеративное обучение при сохранении конфиденциальности, большие языковые модели и объяснимый AI, для повышения точности и интерпретируемости обнаружения. Облегчённые модели, настроенные под Интернет вещей с ограниченными ресурсами, и оконечные устройства также являются важным элементом эффективного применения во взаимосвязанных экосистемах. Киберпреступники всё чаще эксплуатируют уязвимости во взаимосвязанных системах, и данное исследование служит крайне важным ресурсом для улучшения сильных, интерпретируемых и кроссплатформенных систем обнаружения ВПО, чтобы успешно справляться с постоянным появлением новых и разнообразных киберугроз. ■

Об авторах

Джаннатул Фердус, Рафикул Ислам, Араш Махбуби и Мохаммед Захидул Ислам, факультет информационных технологий, математики и проектирования, Университет Чарльза Стерта, Олбери, Новый Южный Уэльс 2640, Австралия

Межоператорский бизнес в России в период массовых DDoS-атак

Юлия Цветкова
Екатерина Глебова

Аннотация

В статье рассмотрены виды DDoS-атак, «яркие» примеры взломов сетей операторов на территории РФ. Большое внимание уделено технологиям защиты от DDoS-атак. Рассмотрен рынок России и аномальный рост компаний, которые предлагают решения по защите от DDoS-атак. Также авторы показывают, как операторы связи адаптируются под новые реальности, и демонстрируют дальнейшие перспективы развития и обеспечения безопасности работы сетей связи.



Ключевые слова:

DDoS-атака, распределённые атаки (ботнет), IoT-устройство, сервер, фильтрация трафика.

1. Введение. Новая реальность цифровой экономики

Современный мир, в котором мы живём, неуклонно меняется на протяжении нескольких последних десятилетий, и эти изменения продолжают по сей день. Нет сомнения в том, что одним из ключевых драйверов этих изменений является «цифровая революция». Благодаря цифровым технологиям государства могут повысить свою конкурентоспособность и способствовать экономическому росту за счёт расширения использования этих технологий. Современный межоператорский бизнес — это кровеносная система глобального Интернета, а, следовательно, и развития цифровой экономики. Обмен трафиком (IP-транзит, пиринг) между операторами связи, хостинг-провайдерами и крупными клиентами обеспечивает беспрепятственную работу всего онлайн-пространства: от стриминговых сервисов и банковских приложений до корпоративных сетей и государственных услуг [1].

Компьютерные сети, такие как Интернет, являются основой цифровой экономики. Инфраструктура, обеспечивающая цифровые возможности, состоит из основных физических материалов и организационных механизмов, которые поддерживают существование и использование компьютерных сетей и цифровой экономики. В этой связи становится крайне

важным рассмотреть проблемы взаимодействия операторов связи как игроков на рынке межоператорских услуг, обеспечивающих связность и устойчивость глобальной телекоммуникационной инфраструктуры. А одной из угроз устойчивого развития операторов связи стали массовые DDoS-атаки.

За последние годы значительно выросла сложность и мощность кибератак, в частности, распределённых атак (или ботнет). Атаки перестали быть уделом одиночек-хактивистов и превратились в мощное оружие в руках киберпреступников и инструмент геополитической борьбы. Для межоператорского бизнеса это создало принципиально новые вызовы, где вопрос уже не просто в качестве обслуживания (SLA), а в самом выживании и сохранении репутации [2].

Количество DDoS-атак в первом полугодии 2025 года увеличилось на 60% относительно первого полугодия 2024, пишет «Коммерсант». IT-атаки стали сложнее из-за того, что хакеры чаще начали использовать мультивекторные методы.

При этом на полях ПМЭФ-2025 заместитель председателя правления «Сбера» Станислав Кузнецов сообщил, что в 2025 году ущерб российским компаниям от DDoS-атак увеличился в три или даже более раз. Это произошло на фоне снижения за год общего количества атак. Но они стали значительно сложнее, что в итоге вылилось в большие потери. Россий-

ские компании плохо противостоят зловредному воздействию, а такое противостояние требует системного подхода.

В 2023-2024 гг. СМИ писали об атаках в 1-2 Тбит/с, а в 2025 году акцент сместился на длительные и изнуряющие атаки. Фиксируются атаки, длящиеся несколько дней. Интенсивность таких атак волнообразная. В современных реалиях мощность атаки может достигать 750 Гбит/с, а пик скорости — 138 миллионов пакетов в секунду.

В 2025 году межоператорские каналы стали целью для DDoS-атак. Существует несколько причин. Первая — «эффект домино». Атака на одного крупного оператора или ключевую точку обмена трафиком может парализовать работу десятков или сотен downstream-провайдеров и тысяч конечных клиентов. Вторая причина — мощность современных атак. Объёмы DDoS-атак огромны и могут серьёзно повредить сеть. Третья причина — «слепая» фильтрация, если атака направлена на IP-адрес клиента одного провайдера, но проходит через upstream-оператора. Последний может быть вынужден применить грубую фильтрацию всего трафика к этому провайдеру, чтобы спасти свою собственную сеть. Это коллатеральный ущерб, который бьёт по ни в чём не повинным пользователям. Цель злоумышленников — максимальный ущерб и медийный резонанс [1].

DDoS-атаки на телеком-операторов — это одна из самых серьёзных угроз в цифровом мире, поскольку они затрагивают не просто сайты, а критическую инфраструктуру.

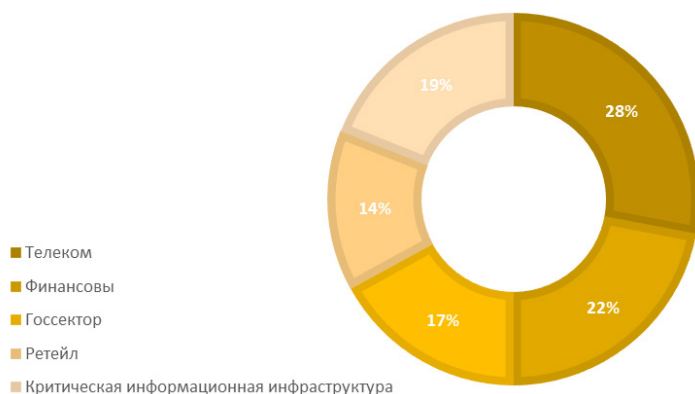


Рис. 1. Основные цели DDoS-атак.

Виды DDoS-атак, последние «яркие» примеры взломов

Существуют различные виды DDoS-атак: по типам трафика, по уровням OSI, по спектру атакуемых объектов. Самые распространённые виды DDoS-атак можно условно разделить на три основные категории:

- уровень приложений;
- уровень протоколов (SYN Flood, ICMP Flood и другие DDoS-атаки уровня протоколов);
- Объёмные (атака UDP Flood в сегменте объёмных DDoS) [3].

Виды DDoS-атак в классификации по уровням OSI

OSI — семиуровневая эталонная модель, описывающая схему взаимодействия сетевых устройств. Модель OSI была разработана еще в 70-х годах и описывала взаимодействие семейства собственных протоколов, которые разрабатывались как главные конкуренты TCP/IP. И хотя особого распространения они так и не получили, модель взаимодействия оказалась настолько удачной, что стала применяться для TCP/IP-протоколов как тогда, так и сейчас. Виды DDoS-атак и защит от них, доступных на каждом из уровней, различны [3].

Классификация уровней:

- 1 уровень. Физический.
- 2 уровень. Канальный.
- 3 уровень. Сетевой.
- 4 уровень. Транспортный.
- 5 уровень. Сеансовый.
- 6 уровень. Представления.
- 7 уровень. Приложений.

С помощью DDoS-атак злоумышленники пытаются полностью прекратить доступ к интернет-ресурсу — отказ в обслуживании. Основной механизм таких атак строится на использовании ботнета — огромной сети заражённых компьютеров, IoT-устройств и серверов, которые злоумышленники контролируют удалённо.

По данным аналитики операторов, предоставляющих защиту от DDoS-атак, за первый квартал 2025 года самыми популярными были атаки типа TCP PSH/ACK Flood, TCP SYN Flood и UDP Flood. Они занимают 76% от общего количества атак.

На операторов связи в основном направляются атаки на инфраструктуру (сетевой и транспортный уровень — L3/L4) и атаки на приложения (прикладной уровень — L7). При атаках L3/L4 уровней целью злоумышленников в телекоме становятся маршрутизаторы (роутеры), межсетевые экраны, базовые станции, каналы связи между городами и странами. Атаки на уровень L7 более изощрённые и сложные для обнаружения. Они имитируют поведение реальных пользователей, но делают это в огромных масштабах. Цели в телекоме: веб-серверы, DNS-серверы, платформы биллинга, сервисы сигнализации.

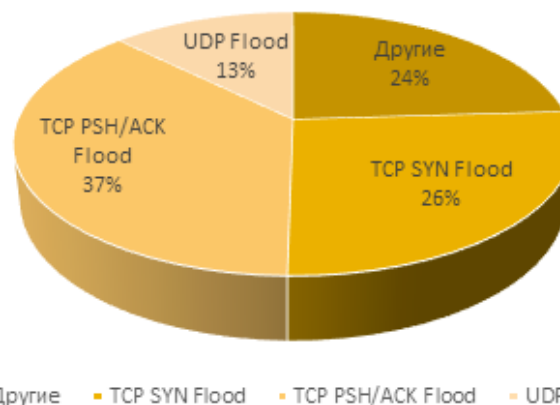


Рис. 2. Типы атак за первый квартал 2025 года.

Статистика дополнительно подтверждает тот факт, что сложные таргетированные атаки от АPT-группировок являются ключевой растущей угрозой, в том числе для телеком-отрасли. Подобные атаки на телеком-сектор влекут за собой и рост числа атак на цепочки поставок с возможностью совершения «атак посредника» (MitM). В результате такой атаки хакеры получают доступ к каналу связи между легитимными сторонами (пользователями, приложениями, сетевыми устройствами и т.д.), что позволяет им просматривать содержимое всех передаваемых ими сообщений, удалять и изменять их. Такие атаки куда сложнее обнаружить как на стороне атакованной жертвы, так и на стороне подрядчика [4].

За текущий год на операторов неоднократно были направлены DDoS-атаки.

28 мая 2025 года специалисты Роскомнадзора сообщили о масштабной DDoS-атаке мощностью 70,07 Гбит/с на московского интернет-провайдера. Из-за DDoS-атаки у части клиентов компании наблюдались проблемы с доступом в сеть.

12 июня 2025 года атаке подвергся интернет-провайдер из Красноярска, в результате чего абоненты из Красноярского края, Хакасии и Иркутской области лишились доступа к Интернету и телевидению. Сетевая и серверная инфраструктура провайдера была выведена из строя киберпреступниками, что привело к масштабному сбою в предоставлении телекоммуникационных услуг. Ситуация оказалась крайне серьёзной, поскольку оператор связи сообщил о возможной утечке персональных данных и попросил клиентов поменять пароли.

30 июля 2025 года масштабной DDoS-атаке на инфраструктуру подвергся крупный петербургский интернет-провайдер.

В качестве особо яркого примера приведём DDoS-атаку в марте 2025 года на одного из крупнейших операторов ШПД на территории РФ. Атака длилась почти пять дней и практически полностью парализовала работу оператора, клиенты оставались без сервисов на весь срок атаки. Разбирая детально данную атаку, мы пришли к выводу, что двумя основными проблемами были ресурсы и компетенции инженеров. Во время атаки на связи были инженеры, не имеющие достаточного опыта в вопросах сети и не имеющие никаких компетенций в защите от DDoS.

Какие основные действия в данном случае могли бы защитить и предотвратить данную ситуацию? Первое: для сайта и мобильного приложения нужна защита WAF, на случай атаки можно включать версию сайта, где сначала выводится captcha, только пройдя которую, можно попасть на сайт. Второе: все структурные сети не должны маршрутизироваться из Интернета. Везде, где можно, необходимо настраивать максимальные правила ACL. В данном примере ГРЧЦ блокировал фактически весь МН-трафик, это убрало атаку на 70%, но остальное нужно было митигировать дополнительными средствами. Тут важно отметить, что на сети должен быть, как минимум, один защищенный апстрим, под защиту которого можно поставить какие-то точечные суперважные сети. По результатам разбора ситуации оказалось, что на сети оператора было несколько взломанных абонентских устройств, откуда, видимо, злоумышленники проводили разведку и следили за принимаемыми контрмерами. Сначала упал сервер L2TP, через который настраивался удалённый доступ к

сети. Видимо, по этой же причине квалифицированные сотрудники не смогли вовремя подключиться к проблеме. И здесь делаем вывод, что обязательно нужны какие-то альтернативные точки входа на чужих IP. Так, нужно отметить, что у атаки была заметная предпосылка — фишинговая атака, т.е. письма с вложением, после открытия и запуска которого в системе устанавливался удалённый доступ к компьютеру. До этого были атаки в Telegram — «сообщения от руководства компании», но это напрямую оператору связать с атакой не удалось. Также в этом примере стоит отметить, что атака была на ту часть сети, которая задевает максимум инфраструктуры. Это говорит о качественной подготовке атаки. Систем предотвращения вторжений (IPS) и обнаружения вторжений (IDS) у оператора не было, а это могло бы сигнализировать о возникновении повышенного внимания к инфраструктуре. В заключение по данному примеру хотим отметить, что в качестве превентивных мер необходимо иметь резервный «чужой Интернет» и «чужие IP-адреса» (/24 достаточно), а возможно, и реализацию полноценной схемы с переводом всех абонентов «на чужой BRAS».

Разобрав виды и примеры атак на операторов, перейдём к видам защиты.

Виды защиты от DDoS-атак, технологии реализации

От DDoS-атак есть множество современных способов защиты. Ниже перечислим основные виды защиты:

1. Фильтрация трафика.
2. Использование CDN (Content Delivery Networks).
3. Web-Application Firewall (WAF).
4. Облачные и гибридные решения Anti-DDoS.
5. Мониторинг и автоматическое реагирование.
6. Ограничение скорости соединений и ресурсов.
7. Резервирование ресурсов и масштабирование.
8. План реагирования на инциденты.

Возрастающее значение приобретают гибридные модели, сочетающие локальную защиту с облачными сервисами. Комбинация сетевого и прикладного уровней защиты обеспечивает комплексную безопасность. Внедрение защитных технологий на уровне интернет-провайдеров и дата-центров значительно повышает надёжность.

Во время DDoS-атаки для оператора крайне важно поддерживать доступность и прохождение «чистого» трафика, пока идёт отражение атаки.

DDoS-атаки несут огромные потери для всех сфер бизнеса и государственных структур. Простой и деградация сервиса ведут к финансовым штрафам и потере доверия со стороны клиентов. Потеря статуса надёжного партнёра может привести к резкому оттоку клиентов.

Для предотвращения DDoS-атак клиент должен заранее позаботиться о своей защите. Успешное отражение

DDoS-атаки позволят сохранить инфраструктуру, клиентов и репутацию. Инвестиции в профессиональную защиту от DDoS-атак — это необходимость, такая же важная, как разработка бизнес-плана.

Выживание в период современных DDoS-атак требует комплексного подхода. Необходимо внедрить системы очистки трафика на границе собственной сети, гибкую маршрутизацию (BGP Flowspec, RTBH), резервирование каналов, постоянный мониторинг, способный мгновенно реагировать на инциденты.

Для противодействия угрозам от DDoS-атак необходима профессиональная митигация. Для защиты своих клиентов компании предлагают услуги защищённого хостинга со встроенными anti-DDoS-решениями. Весь входящий трафик перенаправляется в специальные центры очистки (scrubbing), где происходит его анализ и фильтрация, после чего «чистый» трафик отправляется на сервер клиента. Это позволяет обеспечить целевую доступность сервиса для пользователей даже во время атаки.

Российский рынок «предложений по защите»

Массовые DDoS-атаки из эпизодических превратились в суrowую ежедневную реальность. Борьба с DDoS-атаками — это непрерывная «гонка». Операторам приходится постоянно инвестировать в сложные, многоуровневые системы защиты, чтобы обеспечивать надёжную связь для своих клиентов.

Стоит отметить очень важный момент, что массовые DDoS-атаки создали новый рынок услуг. Вследствие высокой геополитической напряжённости и активности как киберпреступников, так и политически мотивированных хактивистских групп, рынок услуг по защите от DDoS-атак развивается очень быстро. Российский сегмент интернета (Рунет) стал постоянной мишенью для крупномасштабных и сложных атак. Российским операторам и компаниям приходится самостоятельно искать способы для борьбы с кибератаками. Такое положение способствует быстрому и уникальному развитию рынка по защите от DDoS-атак. В России спрос на услуги защиты от DDoS-атак продолжает стабильно расти. Запрос исходит не только от крупного бизнеса (финансы, госсектор, телеком, крупный ретейл), но и всё чаще от среднего и даже малого бизнеса, чья онлайн-активность критически важна (интернет-магазины, образовательные платформы, агрегаторы услуг).

Крупными игроками рынка защиты от DDoS-атак являются ведущие компании, предлагающие комплексные технические решения и сервисы для различных масштабов бизнеса. Игроки российского рынка, занимающиеся защитой от DDoS-атак, отличаются масштабируемостью, продвинутыми технологиями фильтрации трафика, использованием ИИ и машинного обучения, а также интеграцией нескольких уровней защиты. Они обеспечивают надёжную оборону для крупного и среднего бизнесов, государственных структур, а также интернет-площадок.

Производители ПАКов (программно-аппаратный комплекс): разрабатывают и поставляют специализированное аппаратное и программное обеспечение для обнаружения и отражения DDoS-атак. Их продукты обычно предназначены для развёртывания в периметре заказчика (или провайдеров услуг).

Телеком-провайдеры: предоставляют услуги защиты от DDoS-атак на уровне своей инфраструктуры и сетей. Они предоставляют своим клиентам услуги «чистого» трафика, фильтрацию DDoS-трафика и прокси-серверы. Такие услуги обычно предлагаются в виде абонентских платежей или по запросу клиентов.

Сервис-провайдеры: предлагают облачные услуги защиты от DDoS-атак. Они могут действовать в качестве промежуточного звена между клиентами и их веб-приложениями, обрабатывая весь трафик и фильтруя его, прежде чем он достигнет клиентской инфраструктуры. Эти сервисы обычно предоставляются по модели подписки и могут включать в себя дополнительные функции, такие как CDN (Content Delivery Network) и функции оптимизации производительности.

Стоит отметить важное изменение на рынке межоператорского бизнеса: в новых реалиях крупные игроки рынка теперь



Рис. 3. Основные участники российского рынка защиты от DDoS-атак.

предлагают не просто IP-транзит, а «защищённый IP-транзит» — услугу, где трафик по умолчанию проходит через систему очистки. Кроме того, операторы могут предлагать услуги DDoS-защиты «в облаке» для своих партнёров, у которых нет ресурсов для развёртывания собственных дорогостоящих систем. Тут в качестве примера приведём ПАО «ВымпелКом»,

одного из крупнейших игроков этого рынка, который реализовал сразу несколько комплексных решений IP-транзит плюс защита от DDoS-атак и в 2025 году успешно защитил нескольких своих клиентов-операторов от мощнейших DDoS-атак

Успех теперь определяется не только ценой за гигабит или

Оператор (Россия)	Публично упомянутые решения / партнёры (вендоры, сервисы)	Тип развёртывания / модель
«Билайн» («ВымпелКом»), включая beeline cloud	Radware (исторически запуск сервиса с Radware), собственные DDoS-услуги Beeline Cloud; NetFlow-продукт на базе центра очистки; партнёрство с Kaspersky.	Комбинация: on-prem (вендорское hw/sw) + облачные услуги для клиентов; фильтрация в сети оператора и центры очистки.
«Ростелеком» (вкл. «Солар»)	Curator Labs, собственные решения Anti-DDoS («Ростелеком-Солар») на базе «Периметр-Гарда».	Гибрид: внутренняя защита + внешние инструменты/партнёрства; фильтрация в сети оператора и центры очистки.
МТС / Red Security / MWS	Curator Labs (партнёрство: CloudMTS сервис на базе Curator).	Облачный скраббинг / MSSP интеграция (Cloud-service).
«МегаФон»	Сервис на базе «Периметр-Гарда».	Операторский «cloud + network» фильтр; уровень защиты каналов и приложений (операторская услуга).
ТТК («ТрансТелеком»)	Услуга DDoS Free на базе «Периметр-Гарда» и решения DDoS-Guard Protection.	Операторский центр очистки (scrubbing centre) + мониторинг 24/7.
«ЭР-Телеком» / «Дом.ру» (региональные операторы)	Операторские Anti-DDoS-сервисы; часто используют решения Servicepipe и Ddos-Guard (партнёры в регионах варьируются).	On-prem + облачные центры очистки; услуга для B2B/госзаказчиков.
Т2 / (в регионах и дочерних структурах)	Предлагает Anti-DDoS-услуги на базе продуктов «Ростелекома».	Операторская услуга (обычно BGP-redirect → скраббинг).
G-Core Labs (не оператор, но крупный провайдер скраббинга)	Собственная сеть скраббинга (global DDoS protection), TMS (threat mitigation system).	Облачный/глобальный scrubbing (Anycast, многотераваттная ёмкость - указывают в маркетинге).
Curator Labs (MSSP / scrubbing provider)	Собственная распределённая сеть фильтрации, интеграции с операторами и облаками (Yandex.Cloud, CloudMTS и пр.).	Anycast BGP, filtering points (скраб-узлы) — облачный скраббинг + интеграции.
Прочие российские вендоры/MSSP (Kaspersky, StormWall, DDOS-GUARD и др.)	Kaspersky DDoS Protection, StormWall, DDoS-Guard, MWS, K2.Cloud — коммерческие продукты/услуги.	Обычно облачный скраббинг, WAF, антиботы, локальные appliances в дата-центрах.
Аппаратные вендоры, часто встречающиеся в телеком-решениях (общая категория)	Radware (DefensePro), Arbor / Netscout (Peakflow / APS), Cisco (IOS/Firepower + FlowSpec), Huawei.	On-prem appliances, flow-based detectors, FlowSpec/BGP-redirect интеграции, hybrid cloud.

Рис. 4. Конкурентный анализ B2O-решений «Анти-DDoS».

шириной канала, но и способностью гарантировать доставку трафика в самых неблагоприятных условиях. Оператор, который может продемонстрировать партнёрам и клиентам отработанные механизмы противодействия, проактивный мониторинг и прозрачность коммуникации, получает ключевое конкурентное преимущество в эпоху цифрового шторма.

Выживает не самый большой, а самый гибкий и подготовленный. В современной интернет-экосистеме безопасность — это не затраты, это фундамент для доверия и роста. Разберём пример, на котором покажем, почему защита от DDoS-атак не может стоить дёшево. На сети телеком-провайдера с нормой в 300 Гбит/с

легитимного трафика начинается атака мощностью в 200 Гбит/с, распределённая по восьми тысячам IP-адресов. Чтобы от неё защититься, ёмкость очистителей оператора должна суммарно покрывать объёмы и легитимного, и вредоносного трафика на большой сетевой сегмент, то есть в данном случае составлять не менее 500 Гбит/с. Таким образом, для эффективной защиты система фильтрации должна иметь запас по объёму для качественной работы. Этот запас ёмкости должен быть постоянен, а значит, и цена сразу вырастает в разы. Причём этот запас должен быть рассчитан на каждого клиента, так как предугадать, какие клиенты станут жертвами DDoS-атак, невозможно.

Перспективы развития рынка защиты от DDoS-атак

Развитие интеллектуальных систем и интенсивный рост киберугроз стимулируют развитие систем на базе искусственного интеллекта (ИИ) и машинного обучения, которые способны выявлять аномалии и новые типы атак в режиме реального времени. В будущем алгоритмы ИИ будут всё глубже и глубже внедряться в системы защиты, обеспечивая быструю и точную фильтрацию вредоносного трафика.

Мы предполагаем, что в будущем защита будет состоять из нескольких этапов: сначала будет защищаться сетевой уровень (фильтрация и стабилизация трафика), далее — прикладной уровень, где защищаются API и веб-приложения, и в завершение будут специализированные механизмы защиты на базе ИИ от ботов и массированных сканирующих атак. Такая модель позволит гибко адаптироваться к особенностям инфраструктуры.

Скорее всего, злоумышленники будут совершенствовать свои атаки, и, как следствие, атаки станут мощнее, скоростные пики выше, а длительность дольше.

Внедрение автоматизации в системы реагирования позволит минимизировать время простоя и оперативно реагировать на новые векторы атак, включая использование ИИ как в атакующих инструментах, так и в средствах защитной аналитики.

В нашей текущей современности мы наблюдаем рост количества IoT-устройств и их связей, которые могут формировать новые ботнеты, состоящие из бытовых и промышленных устройств. Для мониторинга и фильтрации трафика, с учётом особенностей таких устройств, необходима разработка новых подходов.

Рынок по защите от DDoS-атак продолжит свой быстрый рост. Будут разрабатываться новые системы и алгоритмы, а также широкое применение получит ИИ. Продолжат совершенствоваться комплексные подходы защиты. В перспективе возможно создание единой платформы безопасности.

Возможно, защита от DDoS-атак будет связана с анализом на уровне ИИ, многоуровневой защитой, автоматизацией и интеграцией современных технологий, что позволит своевременно и эффективно противостоять вновь возникающим угрозам в условиях быстрого роста и развития DDoS-атак. ■

Список литературы:

- [1] «Кибербезопасность и защита информации в интернет-сетях» — Михаил Калугин.
- [2] Ежегодный отчет StormWall о DDoS-угрозах. <https://stormwall.pro/>
- [3] Что такое DDoS атака. Настройка эффективной защиты от DDoS атак на сервер. Хостинг RigWEB. <https://rigweb.ru/>
- [4] Тренды кибератак на промышленность и телеком в 2025 году. <https://rt-solar.ru/>

Об авторах

Цветкова Юлия Валерьевна, к.т.н., ПАО «ВымпелКом», Москва
Глебова Екатерина Сергеевна, ПАО «ВымпелКом», Москва





Евгений Панков: Опасности и киберугрозы будут меняться вместе с технологиями

Фишинг, вредоносное ПО, атаки в мессенджерах и дипфейки — онлайн-угрозы становятся всё изощрённее. О новых рисках и о том, как сегодня защищена российская доменная инфраструктура, редакция журнала «Интернет изнутри» поговорила с аналитиком данных Координационного центра доменов .RU/.РФ Евгением Панковым.

— Евгений, как вы оцениваете текущую ситуацию с кибербезопасностью в российских доменах?

— Вообще, борьба с мошенничеством и кибератаками — это постоянная гонка копы и брони: как только появляются новые инструменты защиты, мошенники придумывают способы их обойти. Но если говорить о российских доменах верхнего уровня, то ситуация здесь постепенно улучшается. На фоне многих других доменных зон национальные домены .ru и .рф выглядят достаточно защищёнными.

Не без гордости могу сказать, что в этом году нам удалось переломить тенденцию последних лет и остановить рост фишинга — самой массовой угрозы в доменном пространстве

России. По итогам девяти месяцев этого года число обращений по фишингу в проекте «Доменный патруль» снизилось на 16%. Кроме того, у нас в России среднее время от получения обращения до блокировки вредоносного домена составляет менее 14 часов — и это лучший показатель в мире. Стоит отметить, что свыше 70% всех сообщений обрабатываются в первые 12 часов.

Но это не значит, что теперь можно расслабляться — мошенники всё время ищут новые схемы, и наша задача — не просто держать планку, но и постоянно развивать системы обнаружения и внедрять новые методы защиты.

— Какие виды мошенничества с использованием доменных имён встречаются чаще всего? Как пользователю понять, что перед ним поддельный сайт?

— Фишинг был и остаётся самым частым видом мошенничества: в топе — поддельные сайты популярных банков, маркетплейсов и мессенджеров.

Злоумышленники в подробностях копируют дизайн сайтов, чтобы усыпить бдительность пользователей и выманить у них логины, пароли и данные банковских карт. Чтобы от-

личить подделку, в первую очередь нужно внимательно смотреть на адрес сайта: мошенники часто используют визуально схожие адреса, изменив несколько букв/символов или зарегистрировав сайт в другой доменной зоне.

Также стоит обращать внимание на дату создания домена, наличие HTTPS-сертификата, ошибки в текстах, сбившуюся вёрстку, украденные или сгенерированные ИИ иллюстрации. И главный маркер: если вас попросят «срочно ввести данные» или обещают слишком выгодные цены — это наверняка мошенники. Чтобы не потерять свои данные и деньги, не переходите по подозрительным ссылкам, тщательно проверяйте адреса сайтов и используйте для авторизации и оплаты только официальные ресурсы.

— Какие тенденции вы сейчас наблюдаете у злоумышленников? Почему многие из них в последнее время переключились на мессенджеры?

— Злоумышленники всегда идут туда, где больше потенциальных жертв и где им проще работать. Если раньше активно использовались домены, то сейчас мы видим явный сдвиг в сторону мессенджеров.

Причина проста: в Рунете за последние годы заметно усилились и ускорились механизмы противодействия фишингу. А значит, фишинговые домены «живут» всё меньше, и мошенникам становится невыгодно их использовать. Поэтому мошенники переходят в мессенджеры: за первые восемь месяцев 2025 года число доменов, имитирующих Telegram, выросло почти в четыре раза, растущая динамика наблюдается и по WhatsApp.

Почему именно мессенджеры? Во-первых, это самые популярные каналы общения пользователей, и аудитория у них огромная. Во-вторых, зарегистрировать аккаунт очень просто, а распространять любые ссылки или сообщения можно мгновенно. В-третьих, взлом профиля пользователя открывает мошенникам доступ к контактам, фото и документам, которые затем используются для атак на его друзей и знакомых. И, наконец, меры противодействия со стороны платформ пока явно недостаточны. Всё вместе это создаёт идеальную среду для мошенничества.

Кроме того, в 2025 году мы наблюдаем ещё один тревожный тренд — рост атак с использованием вредоносного программного обеспечения (ВПО). За восемь месяцев этого года поступило более пяти тысяч жалоб на ВПО, что почти в три раза выше показателей аналогичного периода 2024 года. Мошенники

всё чаще используют связку фишинга с ВПО, которая позволяет получить полный контроль над устройством жертвы и не только похищать конфиденциальную информацию и деньги, но и автоматически распространять фишинговые ссылки новым адресатам.

— Какие приёмы мошенников представляют наибольшую опасность для технических специалистов?

— Технические специалисты, как правило, менее восприимчивы к классическим схемам — их не так легко обмануть фишинговым письмом или поддельным маркетплейсом. Но у них есть своя уязвимость: доверие к коллегам, профессиональным сервисам и внутренним коммуникациям. Этим и пользуются злоумышленники.

Когда человек работает в высоком темпе и рутине, внимание к мелочам снижается. Поэтому хакеры часто маскируют атаки под рабочие процессы: поддельные письма от коллеги или системного администратора, уведомления от сервисов для разработчиков или профессиональных сообществ, запросы «срочно обновить пароль» или «настроить доступ». Всё выглядит максимально правдоподобно, и именно здесь специалисты рискуют попасться.

— Если говорить о бизнесе: какие атаки чаще всего нацелены именно на компании и их цифровую инфраструктуру? Что, по-вашему, важнее для компаний и пользователей: строить сильные защиты от атак или учиться минимизировать их последствия?

— Для бизнеса самыми опасными являются ВЕС-атаки, атаки с использованием ВПО и социальная инженерия в мессенджерах.

Чаще всего злоумышленники маскируют вредоносные письма под деловую переписку: это могут быть «срочные» просьбы оплатить счёт, проверить вложение или перейти по ссылке. Переход по таким ссылкам нередко приводит к установке троянов вроде DarkWatchman RAT, которые дают





удалённый доступ к устройствам и позволяют собирать переписку, документы, пароли и другую чувствительную информацию.

Ещё одна схема — подделка коммуникаций от имени руководителей или партнёров. Здесь используются либо взломанные аккаунты корпоративной почты, либо похожие адреса, а всё чаще и дипфейки, когда сотрудник получает сообщение или звонок якобы от своего руководителя. Так злоумышленники выманивают деньги или получают доступ к внутренним системам.

Отдельно стоит упомянуть схему взлома панели управления доменом у регистратора. Это позволяет не только «угнать» домен, но и получить доступ к ключевой IT-инфраструктуре компании. Например, подменить настройки почтовых серверов, перехватывать переписку, перенаправлять пользователей на фишинговые сайты и даже создавать поддельные точки доступа в корпоративную сеть и собирать данные сотрудников.

Если говорить о стратегии защиты, то это не вопрос выбора: нужно выстраивать комплексную защиту, способную не только отразить угрозу, но и минимизировать последствия атаки. Эффективная система безопасности включает и своевременную настройку защитных механизмов, и регулярный аудит инфраструктуры, и обучение сотрудников, и мониторинг активности, и особое внимание к защите корпоративного домена.

— Искусственный интеллект развивается стремительно, и вместе с ним появляются новые риски. Замечаете ли вы уже примеры атак с использованием ИИ?

— Да, примеры атак с использованием искусственного интеллекта мы уже видим. Сегодня ИИ помогает злоумышленникам делать дипфейки и создавать более убедительные сценарии атак. Зачастую он используется для автоматизации процессов: от сканирования сетей и кражи данных до генерации персонализированных фишинговых писем. Также были случаи, когда вредоносные ссылки и ПО внедрялись прямо в диалоги с ИИ-чатами: человек задаёт обычный вопрос, а в ответ получает опасную ссылку, даже не подозревая об угрозе.

Очевидно, что искусственный интеллект будет и дальше развиваться, а это значит, что пользователям и специалистам по ИБ нужно учиться работать с новыми рисками: повышать цифровую грамотность, критически оценивать информацию и внедрять современные методы защиты.

— Возможно ли заранее отследить и выявить фишинговый домен ещё на этапе регистрации? Какие инструменты для этого используются?

— Да, сегодня в зонах .ru и .рф уже применяются проактивные методы, которые позволяют выявлять потенциально опасные домены на этапе регистрации.

Новые домены автоматически проходят проверку по ряду признаков: система отмечает подозрительные регистрации и передаёт их на дополнительную проверку компетентным

организациям. Это помогает предотвращать инциденты, не дожидаясь, пока домен начнёт использоваться для фишинга. Также мы активно изучаем возможности использования ИИ для обнаружения вредоносных регистраций и анализа угроз инфраструктуры DNS.

Важно понимать, что полная автоматическая блокировка фишинга невозможна: нужна дополнительная экспертиза, чтобы случайно не навредить добросовестным администраторам. Но сама связка проактивной разметки и работы «Доменного патруля» позволяет существенно сократить время обнаружения и сделать российское доменное пространство более безопасным.

— Какие шаги предпринимает Координационный центр для борьбы с вредоносными доменами?

— На сегодняшний день одним из самых эффективных механизмов борьбы с вредоносными доменами является проект «Доменный патруль». Он объединяет компетентные организации и регистраторов, что позволяет быстро выявлять и блокировать опасные ресурсы. Так, в 2024 году в отечественном доменном пространстве было заблокировано более 55 тысяч таких доменов, а с начала 2025 года — уже свыше 30 тысяч.

Кроме того, сейчас готовится законопроект о введении обязательной идентификации администраторов через ЕСИА (портал госуслуг). Это станет реальным барьером для поддельных данных и регистрации доменов под фишинг или другие противоправные действия. Технически система уже протестирована крупнейшими регистраторами и в ближайшее время станет отраслевым стандартом.

— И напоследок: какие практические рекомендации вы могли бы дать специалистам и владельцам бизнеса, чтобы надёжно защитить свои домены и цифровые ресурсы?

— Владельцам бизнеса я бы, в первую очередь, рекомендовал выбирать для своих сайтов и онлайн-проектов национальные зоны .ru, .rf и .su. Они являются одними из самых безопасных, а кроме того, полностью управляются внутри страны и не зависят от иностранных юрисдикций и платформ.

Отдельное внимание стоит уделить настройке корпоративной почты на домене. Это не только повышает уровень доверия со стороны клиентов и партнёров, но и позволяет выстраивать собственную систему защиты: подключать фильтры от спама и фишинга, настраивать двухфакторную аутентификацию, шифрование и резервное копирование.

Не менее важно обеспечить надёжную защиту серверов и регулярно обновлять системы, использовать антивирусы, внедрять мониторинг и аудит инфраструктуры. И, конечно, нужно учить сотрудников цифровой гигиене, знакомить с новыми видами атак и формировать чёткий план действий на случай возможных инцидентов.

Нужно понимать, что опасности и киберугрозы никуда не денутся — они будут меняться вместе с технологиями. Важно быть внимательными, учиться новому и не оставлять лазеек злоумышленникам. ■



«Internet Science» — образование и наука. Продолжение следует...

Ведущий рубрики: Марат Биктимиров



Дорогие читатели!

В 18-м номере нашего журнала мы открыли новую рубрику — «Образование и наука» — и, в том числе, анонсировали намерение публиковать материалы, связанные с подготовкой профессиональных кадров для интернет-отрасли.

Несколько лет назад Фонд развития сетевых технологий «ИнДата» совместно с МГТУ им. Баумана и МИЭМ ВШЭ создал площадку для профессиональной ориентации студентов в рамках соответствующих образовательных траекторий, включающую выполнение курсовых и выпускных квалификационных работ, проектной деятельности и летней производственной практики на своей базе. Все работы со студентами проводятся под руководством кураторов — ведущих сотрудников Фонда. Причём по результатам большая часть выполненных работ рекомендована и/или внедряется в производственный процесс.

Наши студенты отлично защищают свои проекты и дипломы, активно участвуют в вузовских, отраслевых и международных конференциях, а некоторые — успешно сертифицированы в академии RIPE.

Сегодня мы представляем вашему вниманию две работы, выполненные студентами МГТУ им. Баумана под руководством ведущего специалиста Фонда «ИнДата» Александра Венедюхина и посвящённые проблемам TLS-сертификации.

Анализ информации TLS-сертификатов оконечных узлов и меток времени (SCT) для российских логов Certificate Transparency

Александр Венедюхин
Павел Якубов



Аннотация

Статья посвящена анализу работы российской инфраструктуры Certificate Transparency (CT). Исследуется соответствие TLS-сертификатов, обнаруженных на серверах (оконечных узлах), данным из публичных логов Certificate Transparency (CT-логов), а также проверяется валидность и корректность подписанных меток времени (SCT). Разработанное программное обеспечение выявило ряд несоответствий, включая расхождения в метках времени и отсутствие публикации сертификатов в отдельных логах. Результаты демонстрируют, что российская система CT в целом работоспособна и обеспечивает необходимую открытость, но требует повышенного внимания к устранению ошибок удостоверяющих центров для поддержания доверия.

Ключевые слова:

Certificate Transparency, TLS-сертификат, удостоверяющий центр, пресертификат, публичный лог, доверие, ключ, метка времени, оконечный узел, инфраструктура, Интернет.

Введение

TLS-сертификаты казались надёжным способом защитить передаваемые данные до тех пор, пока в 2011 году не был взломан удостоверяющий центр (УЦ) DigiNotar [1]. Получив доступ к ключам удостоверяющего центра, злоумышленники смогли скомпрометировать данные пользователей Интернета, выпустив при помощи доверенных ключей данного УЦ большое количество сертификатов для имён известных веб-сервисов без ведома администраторов этих сервисов. Это позволило подменять TLS-соединения, притворившись легитимными владельцами ресурса. Ответом на подобные угрозы является система Certificate Transparency.

Certificate Transparency — группа технологий (система), предназначенная для доверенной регистрации TLS-сертификатов, выпускаемых удостоверяющими центрами, и публикации сведений об этих сертификатах. Certificate Transparency (далее — CT) была запущена для глобальной сети Интернет в 2012 году сразу после взлома DigiNotar и широко используется в настоящий момент. Предполагается, что она позволит вести независимый мониторинг деятельности удостоверяющих центров по выпуску TLS-сертификатов.

Принцип работы Certificate Transparency [2] в текущей реализации (схематично показан на рис. 1):

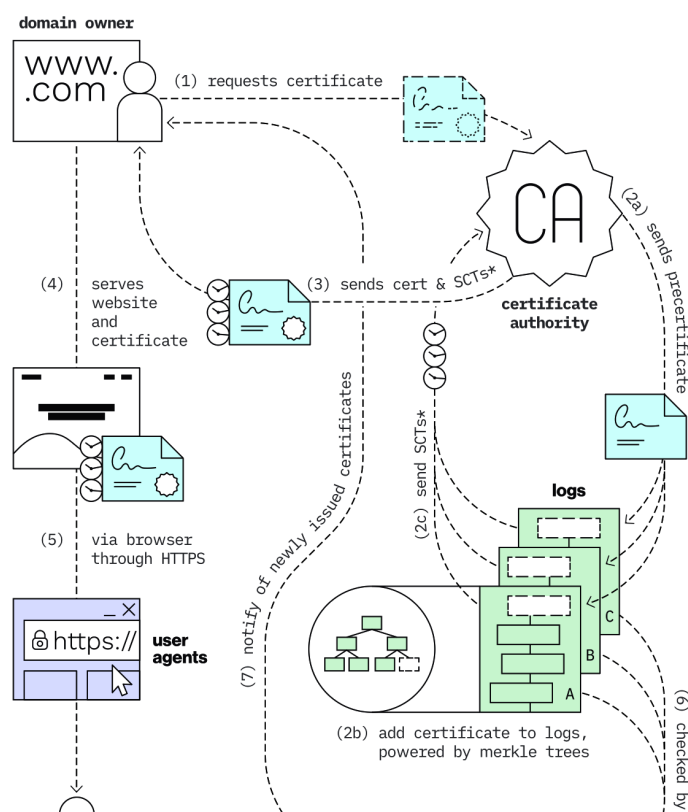


Рис. 1. Схема работы Certificate Transparency [2].

- пользователь запрашивает необходимый ему сертификат у удостоверяющего центра;
- вместо немедленного выпуска сертификата, как это было раньше, удостоверяющий центр сначала выпускает так называемый пресертификат, который почти идентичен стандартному сертификату;
- пресертификат отправляется в различные СТ-логи — специальные журналы, хранящие сертификаты и пресертификаты;
- каждый СТ-лог отправляет в ответ SCT-метку (Signed Certificate Timestamp) — структуру с отметкой времени и подписью лога, подтверждающую, что пресертификат был предъявлен оператору лога;
- удостоверяющий центр выпускает сертификат, включая в его состав полученные от оператора лога SCT-метки;
- итоговый сертификат возвращается пользователю.

Безопасность Certificate Transparency основана на том, что все выпускаемые сертификаты теперь попадают в СТ-логи, а сертификаты без меток логов считаются небезопасными (не принимаются браузерами). Структура логов позволяет лишь добавлять записи, что исключает подделку данных «задним числом», а данные в них доступны всем желающим. К примеру, они могут быть использованы владельцами конкретных доменных имён и IP-адресов для выявления сертификатов, которые не должны были быть выпущены — с ошибочными данными или в результате взлома удостоверяющего центра. Благодаря СТ-логам работа удостоверяющих центров становится открытой и доступной для аудита, что при регулярном мониторинге данных логов сторонними наблюдателями может предотвратить инциденты, связанные с ошибочным выпуском сертификатов.

С историей применения Certificate Transparency связан ряд достаточно громких событий в области деятельности удостоверяющих центров TLS. Например, в 2017 году данные из логов Certificate Transparency послужили доказательством того, что удостоверяющий центр Symantec выпустил много сертификатов с грубым нарушением политик, и это в итоге привело к удалению данного удостоверяющего центра из списка доверенных в браузерах. В том же году данные Certificate Transparency стали основой технического расследования в отношении удостоверяющего центра WoSign, который был замечен в выпуске сертификатов со сдвинутым в прошлое интервалом валидности, что является серьёзным нарушением общепринятых принципов работы УЦ. По этой и другим причинам корневые ключи WoSign также потеряли статус доверенных в распространённых браузерах. В 2019 году при помощи Certificate Transparency были обнаружены нарушения, допущенные удостоверяющим центром Certinomis, что также привело к отказу в доверии. В 2025 году данные Certificate Transparency позволили выявить TLS-сертификаты, ошибочно выпущенные УЦ Fina CA для IP-адреса 1.1.1.1, который соответствует глобальному сервису компании Cloudflare [11]. Данные сертификаты были также выпущены без ведома Cloudflare, однако в этом случае Certificate Transparency сработала с большой задержкой: между фактическим выпуском первого ошибочного сертификата и его обнаружением прошло более полугода (!).

Тем не менее, приведённые примеры подтверждают, что в условиях работы многих удостоверяющих центров и при

наличии действенных административных инструментов влияния на их деятельность Certificate Transparency может оказывать эффективную техническую поддержку для процесса контроля [3].

Для самих владельцев доменов также есть способ использовать Certificate Transparency: время от времени они могут делать запрос к мониторам СТ-логов через специальные сервисы по упрощённому API (например, через веб-интерфейс), отслеживающие изменение логов и предоставляющие информацию о сертификатах, находящихся в них, и проверять, не был ли выпущен новый сертификат на их домен [4]. А при желании владельцы доменов могут и самостоятельно мониторить непосредственно СТ-логи.

Российская система Certificate Transparency, обособленная по составу логов данных и (пре-)сертификатов, появилась в 2022 году. На момент выполнения основной части данной работы (2024 год) в России были представлены три организации-оператора, занимающиеся поддержкой системы Certificate Transparency и опубликовавшие свои логи Certificate Transparency: «Яндекс», ВК и Минцифры России.

У компании «Яндекс» даже существует инструкция и описание технических требований для желающих создать свой собственный лог Certificate Transparency [5]. В случае нарушения технических требований лог удаляется из списка доверенных «Яндекс.Браузера» (этот браузер рекомендуется как поддерживающий российские доверенные TLS-сертификаты на едином портале госуслуг [6]).

В представленной работе с помощью разработанного программного обеспечения производились:

- сбор TLS-сертификатов с доступных узлов сети Интернет по именам из списка найденных в (пре-)сертификатах из логов российской системы Certificate Transparency;
- сопоставление сведений в обнаруженных сертификатах с данными из логов;
- сравнение информации из меток времени логов с данными из обнаруженных сертификатов; построение статистики, сопоставляющей сертификаты, метки времени и пресертификаты;
- поиск возможных несовпадений.

Программное обеспечение было реализовано на языке Go с использованием библиотеки с открытым исходным кодом «certificate-transparency-go» [7].

Программная реализация

Исследованные логи используют версию 1.0 Certificate Transparency. Её спецификация опубликована в документе RFC 6962 [8]. Для получения пресертификатов из СТ-логов необходимы секции спецификации 4.3 «Retrieve Latest Signed Tree Head» (используется способ получения размера лога сертификатов) и 4.6 «Retrieve Entries from Log» (используются непосредственно сертификаты и пресертификаты) (рис. 2 и 3).

4.3. Retrieve Latest Signed Tree Head

```
GET https://<log server>/ct/v1/get-sth

No inputs.

Outputs:

tree_size: The size of the tree, in entries, in decimal.

timestamp: The timestamp, in decimal.

sha256_root_hash: The Merkle Tree Hash of the tree, in base64.

tree_head_signature: A TreeHeadSignature for the above data.
```

**Рис. 2. Скриншот API RFC 6962
«Retrieve Latest Signed Tree Head».**

Описание российской системы Certificate Transparency [9] содержит также ссылку на файл со списком российских логов, удовлетворяющих API RFC 6962, а также их открытыми ключами и идентификаторами [10].

Каждый пресертификат, найденный в логах, асинхронно обрабатывается — делаются запросы на узлы, адресуемые доменными именами, которые указаны в сертификате. Наличие асинхронной обработки данных критично для производительности по следующим причинам:

- при анализе каждого сертификата программа пытается установить соединение со всеми веб-узлами под именами из сертификата; таких имён может быть несколько десятков;
- «тайм-аут» (максимальное время ожидания ответа) подобного соединения составляет 10-20 секунд;
- в логах содержится несколько тысяч пресертификатов.

Взяв средние оценки по всем показателям и произведя несложные вычисления, можно примерно оценить время работы программы при синхронной обработке всех данных в

5·10 с·5000=250000 с≈4166 мин≈69 ч≈3 суток.

При асинхронной же обработке данных время работы программы составляет около 3-5 минут. Конечно, не все соединения будут ожидать ответа 10 секунд и не все сертификаты имеют минимум пять доменных имён, но в любом случае разница в производительности между синхронным и асинхронным вариантом программы является значительной.

Для того, чтобы проанализировать, как используется (если используется вообще) найденный в логе пресертификат, необходимо сделать HTTPS-запросы к узлам, адресуемым доменными именами, указанными в нём. Если удалось создать TLS-соединение с удалённым сервером, найденным по доменному имени, значит, хотя бы одно из доменных имён сертификата валидно в том смысле, что указывает на действующий и доступный веб-узел. На следующем шаге проверяется, используется ли на сервере конкретно этот сертификат: помимо имён, сравниваются серийные номера, найденные в сертификате сервера и в СТ-логе. Если номера совпали, больше не делаем запросы по именам в поисках данного сертификата.

4.6. Retrieve Entries from Log

```
GET https://<log server>/ct/v1/get-entries

Inputs:

start: 0-based index of first entry to retrieve, in decimal.

end: 0-based index of last entry to retrieve, in decimal.

Outputs:

entries: An array of objects, each consisting of

leaf_input: The base64-encoded MerkleTreeLeaf structure.

extra_data: The base64-encoded unsigned data pertaining to the log entry. In the case of an X509ChainEntry, this is the "certificate_chain". In the case of a PrecertChainEntry, this is the whole "PrecertChainEntry".
```

Рис. 3. Скриншот API RFC 6962 «Retrieve Entries from Log».

Если сертификат найден, начинается обработка его SCT-меток. Метки времени извлекаются из сертификата и сравниваются по значению с данными из СТ-лога. Если какая-то метка времени не совпала или не найден лог, соответствующий этой метке, который должен однозначно определяться по идентификатору лога (ключу) из SCT-метки, это считается ошибкой. Ошибки специальным образом записываются. Если СТ-лог, которому соответствует метка, найден, тогда, с помощью общедоступной информации о публичных ключах логов, производится попытка верификации подписи SCT-метки. Неудача верификации также считается ошибкой.

В результате получены две статистики:

- в разрезе каждого удостоверяющего центра — сколько пресертификатов, выпущенных им, используются, и у скольких из них все имена недоступны для установления TLS-соединения;
- в разрезе каждого лога Certificate Transparency — сколько SCT-меток этого лога было найдено на сертификатах с окончательных узлов.

Результат

На рисунке 3 приведён скриншот результата работы программы без информации об ошибках, а далее — текст результата. Адрес лога «~LOG URL NOT FOUND~» означает, что найти лог, которому соответствует данная SCT-метка, не удалось. Возможно, это метки лога Certificate Transparency Минцифры России 2023 года, поскольку на момент исследования данный СТ-лог был недоступен.

```
ALL: 8710 USED: 1321 (15%) ERROR DIALING: 2165 (24%) from Russian Trusted Sub CA
ALL: 196 USED: 1 ( 0%) ERROR DIALING: 97 (91%) from TCI ECDSA B1 6-160
ALL: 370 USED: 60 (16%) ERROR DIALING: 131 (35%) from TCI ECDSA B1 13-240
ALL: 133 USED: 19 (14%) ERROR DIALING: 57 (42%) from TCI ECDSA B1 10-200
SCT amount: 1359 from https://ct-agate.yandex.net/2025/
SCT amount: 1359 from https://ctlog2025.mail.ru/nca2025/
SCT amount: 38 from https://ctlog2023.mail.ru/nca2023/
SCT amount: 4 from https://ct-agate.yandex.net/2024/
SCT amount: 1284 from https://25.ctlog.digital.gov.ru/2025/
SCT amount: 38 from https://ct-agate.yandex.net/2023/
SCT amount: 37 from ~LOG URL NOT FOUND~
SCT amount: 10 from https://24.ctlog.digital.gov.ru/2024/
SCT amount: 4 from https://ctlog2024.mail.ru/nca2024/
```

Рис. 4. Скриншот результата работы программы.

Выводы по результатам работы программы:

1. Количество SCT-меток, найденных в логе Минцифры России 2025 года — 1284 штуки, — не совпадает с количеством в логах «Яндекса» и ВК — 1359 штук в обоих. Как оказалось, это связано с тем, что сертификаты, выпускаемые ТЦИ («Техническим центром Интернет»), не публикуются в логах Минцифры.

2. Наибольшим процентом «ERROR DIALING» — количество пресертификатов, ни к одному из имён которых не удалось подключиться — обладает удостоверяющий центр «TCI ECDSA B1 6-160» (91%). По всей видимости, это связано с тем, что основные сертификаты, выпускаемые им, это сертификаты, используемые для тестирования. Такой вывод можно сделать ещё и потому, что большая часть из 106 выпущенных приходится на два домена: 33 на домен freetls.su и 32 на домен cateam.ru. В противовес ему выступает удостоверяющий центр «Russian Trusted Sub CA», который обладает минимальным процентом «ERROR DIALING». Скорее всего, это означает, что у данного удостоверяющего центра запрашивают сертификаты конечные пользователи для доступных узлов.

3. Среди всех найденных SCT-меток только одну не удалось верифицировать (таблица 1).

Таблица 1. Табличная запись об SCT-метке, которую не удалось верифицировать

SerialNumber	Common-Name	NotBefore	Issuer	Error	SCT-Timestamp	Log-Timestamp	LogURL	LogIndex	LogEntries	Raw-Base64
oEE83DE68919B11E-FA5400242AC120002	s.autoup-date.info	24/10/2024 00:07:18	Russian Trusted Sub CA	SCT is not verifying: failed to verify ECDSA signature	24/10/2024 03:07:18	25/10/2024 00:32:01	https://ct-agate.yandex.net/2025/	4993	[https://ct-agate.yandex.net/2025/]	
oEE83DE68919B11E-FA5400242AC120002	s.autoup-date.info	24/10/2024 00:07:18	Russian Trusted Sub CA	Timestamp is wrong	24/10/2024 03:07:18	25/10/2024 00:32:01	https://ct-agate.yandex.net/2025/	4993	[https://ct-agate.yandex.net/2025/]	

Видно, что при анализе данного сертификата произошла также и ошибка «Timestamp is wrong». И действительно, при ближайшем рассмотрении оказалось, что у этого пресертификата и соответствующего ему сертификата время начала действия различается на секунду (таблица 2).

Таблица 2. Табличная запись о сертификате, SCT-метку которого не удалось верифицировать, и соответствующем ему пресертификате

SerialNumber	Common-Name	NotBefore	Issuer	CanDial	Used	SCTError	SAN	LogEntries	LogEntries	Raw-Base64
oEE83DE68919B11E-FA5400242AC120002	s.autoup-date.info	24/10/2024 00:07:17	Russian Trusted Sub CA	TRUE	TRUE	TRUE	[s.autoup-date.info]	[https://ctlog2025.mail.ru/nca2025/ https://25.ctlog.digital.gov.ru/2025/ https://ct-agate.yandex.net/2025/]	[https://ct-agate.yandex.net/2025/]	
oEE83DE68919B11E-FA5400242AC120002	s.autoup-date.info	24/10/2024 00:07:18	Russian Trusted Sub CA	TRUE	TRUE	TRUE	[s.autoup-date.info]	[https://ct-agate.yandex.net/2025/]	[https://ct-agate.yandex.net/2025/]	

Такой состав сертификата свидетельствует о том, что при его формировании удостоверяющим центром была допущена грубая ошибка, поскольку несовпадение времён начала действия сертификата и соответствующего ему пресертификата вызывает сомнения относительно подлинности сертификата с SCT-меткой и соответствия требованиям безопасности. Такой сертификат не может использоваться при условии контроля SCT-меток ввиду того, что при валидации SCT-метки стандартными методами воспользоваться будет нельзя, так как не совпадёт значение цифровой подписи из состава метки.

Заключение

Текущее состояние российской системы Certificate Transparency позволяет выявлять ошибки в SCT-метках сертификатов, которые играют ключевую роль в обеспечении безопасности системы Web PKI (англ. Public Key Infrastructure — инфраструктура открытых ключей). Следует надеяться, что количество подобных проблем будет в дальнейшем минимизировано. Несмотря на найденное в ходе исследования несоответствие сертификата пресертификату, российская система Certificate Transparency является полностью рабочей, удовлетворяет принятому API, обеспечивает открытость данных и доступна любому внешнему наблюдателю, что является положительным результатом. ■

Список литературы:

- [1] Хакер. Подробности взлома DigiNotar. URL: <https://haker.ru/2012/11/01/59572/> (дата обращения: 20.12.2024).
- [2] certificate.transparency.dev. Принцип работы Certificate Transparency. URL: <https://certificate.transparency.dev/howctworks/> (дата обращения: 20.12.2024).
- [3] ТЦИ. Certificate Transparency в современном интернете. URL: <https://www.tcinet.ru/press-centre/articles/7751/?ysclid=m53mxtf8vp349936923> (дата обращения: 20.12.2024).
- [4] HackWare. Мониторинг появления новых субдоменов в реальном времени. URL: <https://hackware.ru/?p=16188> (дата обращения: 20.12.2024).
- [5] Яндекс. Политика доверия Certificate Transparency log. URL: <https://yandex.ru/support/browser-beta/ru/security/policy-ct-log.html?ysclid=m53nq6wlgd783023557> (дата обращения: 20.12.2024).
- [6] Госуслуги. Поддержка работы сайтов с российскими сертификатами. URL: <https://www.gosuslugi.ru/crt> (дата обращения: 20.12.2024).
- [7] GitHub. Исходный код и описание библиотеки «certificate-transparency-go». URL: <https://github.com/google/certificate-transparency-go> (дата обращения: 20.12.2024).
- [8] IETF Datatracker. RFC 6962 — Certificate Transparency. URL: <https://datatracker.ietf.org/doc/html/rfc6962> (дата обращения: 20.12.2024).
- [9] Habr. Статья 2022 года с описанием устройства российской системы СТ. URL: <https://habr.com/ru/companies/yandex/articles/667300/> (дата обращения: 20.12.2024).
- [10] Ссылка на список логов Certificate Transparency. URL: <https://browser-resources.s3.yandex.net/ctlog/ctlog.json> (дата обращения: 20.12.2024).
- [11] Addressing the unauthorized issuance of multiple TLS certificates for 1.1.1.1. URL: <https://blog.cloudflare.com/unauthorized-issuance-of-certificates-for-1-1-1-1/> (дата обращения: 16.09.2025).

Об авторах

Венедюхин Александр Анатольевич,
ведущий специалист ФРСТ «ИнДата»

Павел Якубов,
студент МГТУ им. Н.Э. Баумана



Специализированное in-мемоу хранилище информации о TLS-сертификатах и TLS-узлах с быстрым поиском

Александр Венедюхин

Софья Проклашкина



Аннотация

В статье представлено описание архитектуры специализированного in-мемоу хранилища для обработки TLS-сертификатов. Разработанная высокопроизводительная система оптимизирована для выполнения специализированных поисковых запросов, учитывающих формат и свойства TLS-сертификатов. Высокая производительность достигается за счёт использования комбинации эффективных структур данных, включая синхронизированные хеш-таблицы (sync.Map), префиксные деревья (Radix Tree) и суффиксные автоматы. Реализация на языке Go обеспечивает конкурентную обработку данных при чтении и записи.

Ключевые слова:

TLS-сертификат, TLS-протокол, удостоверяющий центр, криптографическая безопасность, уязвимость, база данных, хранилище в памяти, поисковый запрос, хеш-таблица, Интернет.

Введение

Современные информационные системы требуют специализированных решений для хранения и обработки данных, особенно когда речь идёт о высоконагруженных сервисах с жёсткими параметрами скорости отклика. В данной работе рассматривается пример такой системы, оптимизированной для работы с TLS-сертификатами. Предлагаемый подход может быть адаптирован и для других типов и структур данных.

Сертификаты TLS (Transport Layer Security), которые иногда по традиции называют «SSL-сертификатами» (Secure Sockets Layer), используются для аутентификации узлов сети Интернет и создания защищённого соединения между клиентом, в качестве которого часто выступает браузер, и сервером. С помощью средств цифровой подписи сертификат обеспечивает привязку открытого ключа сервера к сетевому имени и, таким образом, подтверждает подлинность веб-ресурса, а также позволяет шифровать передаваемую информацию, защищая её от перехвата и подделки [1].

Практическое значение разработки хранилища именно для TLS-сертификатов заключается в возможности его применения в системах мониторинга сетевого трафика, инфраструктуре центров сертификации, а также в различных сервисах информационной безопасности, где скорость обработки запросов имеет критическое значение.

Актуальность подобного хранилища обусловлена отсутствием возможности реализации уникальных решений на базе

универсальных СУБД, которые не могут обеспечить необходимую производительность для узкоспециализированных задач, а также удовлетворить требованиям некоторых предметных областей к структурам данных и операциям над ними. В случае с TLS-сертификатами критически важными становятся операции быстрого поиска по различным атрибутам, интерпретация которых специфична именно для области применения сертификатов (по IP-адресу с учётом подсетей, по доменному имени, дате действия, публичным ключам с учётом их математических особенностей), что и определило алгоритмическую архитектуру разрабатываемого решения.

Протокол TLS

TLS (Transport Layer Security) — это протокол для защищённой передачи данных в сети Интернет. Он обеспечивает целостность данных с помощью кодов аутентификации сообщений («имитовставок»), конфиденциальность — посредством применения методов симметричного шифрования. Для проверки подлинности соединения, то есть соответствия источника информации ожидаемому имени, используются асимметричные криптосистемы цифровой подписи. TLS работает поверх уже установленного соединения между узлами и использует это соединение для передачи TLS-сообщений. Как правило, протокол TLS работает поверх протокола TCP [2].

Протокол TLS является одним из самых изученных в Интернете, исследования по поиску уязвимостей проходят на постоянной основе и ведут к обновлению его архитектуры и устранению ошибок в новых версиях. Самой современной версией TLS является TLS 1.3, в которой значительное внимание уделено сокрытию метаданных.

Сертификат TLS

Сертификаты TLS позволяют решить проблему подмены узлов методом «атаки посредника», при которой злоумышленник выдаёт себя за конечный узел, передавая собственный открытый криптографический ключ.

Сертификат TLS — это публичный цифровой документ, аутентифицирующий конечные узлы и привязывающий открытый криптографический ключ к доменному имени при помощи цифровой подписи удостоверяющего центра (УЦ).

Сертификаты в TLS бывают трёх видов — корневые, промежуточные и серверные. Сертификаты сопоставляются по именам, указанным в них, и, таким образом, строится цепочка доверия, в которой с помощью ключа корневого сертификата можно проверить подлинность промежуточного сертификата, а с помощью ключа промежуточного — подлинность серверного (этот сертификат часто называют «оконечным» сертификатом). Корневые открытые ключи УЦ содержатся в базе данных проверяющего узла, а доверие к конкретному веб-серверу основывается на том, что веб-сервер знает секретный ключ, соответствующий открытому ключу серверного сертификата [3].

Удостоверяющие центры считаются доверенной стороной, чей открытый ключ широко известен. К функциям УЦ относятся подпись сертификатов, получение и проверка информации, необходимой для подписи сертификата, отзыв сертификата по требованию владельца имени и секретного ключа, соответствующих сертификату.

Сертификат — это структура данных, которая включает в себя следующую информацию:

- Serial Number — серийный номер;
 - Subject — имя субъекта (например, доменное имя);
 - Issuer — имя издателя, обычно — УЦ;
 - SubjectPublicKeyInfo — информация об открытом ключе;
 - Signature Algorithm — алгоритм подписи сертификата;
 - Not Before Date — начало действия сертификата;
 - Not After Date — окончание действия сертификата;
- и другие поля [4].

Пример содержимого некоторых полей TLS-сертификата, расшифрованного с помощью утилиты openssl, показан на рисунке 1.

```
$ openssl x509 -in cacert.pem -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 11485830970703032316 (0x9f65de69ceef2ffc)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, ST=MD, L=Baltimore, CN=Test CA/emailAddress=test@example.com
    Validity
      Not Before: Jan 24 14:24:11 2017 GMT
      Not After : Feb 23 14:24:11 2018 GMT
    Subject: C=US, ST=MD, L=Baltimore, CN=Test CA/emailAddress=test@example.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (4096 bit)
      Modulus:
        00:b1:7f:29:be:78:02:b8:56:54:2d:2c:ec:ff:6d:
        ...
        39:f9:1e:52:cb:8e:bf:8b:9e:a6:93:e1:22:09:8b:
```

Рис. 1. Пример содержимого некоторых полей TLS-сертификата, расшифрованного с помощью утилиты openssl.

Хранилища сертификатов TLS

Эффективность TLS-сертификатов напрямую зависит от правильного управления и хранения. В связи с этим появляется необходимость в специализированных системах, которые позволяют не только хранить TLS-сертификаты, но и анализировать их на предмет уязвимостей, а также оперативно реагировать на возможные инциденты безопасности.

Сервисы, подобные разрабатываемому, могут выполнять функцию центрального хранилища TLS-сертификатов, собранных с различных оконечных узлов. При этом такие данные, как IP-адреса, на которых был обнаружен TLS-сертификат; время сбора; информация о владельце и другие метаданные, сохраняются вместе с самим TLS-сертификатом. Это позволяет строить эффективную систему мониторинга и анализа состояния криптографической безопасности в сетях.

Примеры сервисов, работающих с анализом и хранением TLS-сертификатов:

1. Certificate Transparency (CT) — представляет собой инициативу в области публичного аудита, направленную на повышение подотчётности удостоверяющих центров посредством ведения неизменяемых журналов регистрации всех выпущенных TLS-сертификатов.
2. Crt.sh — поисковый интерфейс к данным журналов CT, предоставляющий возможность осуществлять запросы к сформированному по данным CT реестру сертификатов на основе специальных атрибутов, таких как доменное имя или криптографический отпечаток.
3. Censys — платформа для комплексного анализа сетевой инфраструктуры. В результате проведения активных сканирований IPv4-адресного пространства сервис агрегирует данные о доступных хостах, включая метаданные представленных TLS-сертификатов.
4. Shodan — специализируется на обнаружении и инвентаризации сетевых устройств и Интернета вещей (IoT). В процессе сканирования система также извлекает и каталогизирует информацию о TLS-сертификатах, что позволяет проводить анализ их параметров и выявлять потенциально уязвимые реализации.

5. ZMap — представляет собой высокопроизводительный инструмент для сканирования сетей, предназначенный для выполнения полного опроса IPv4-адресации в исследовательских целях. ZMap позволяет проводить крупномасштабные измерения, направленные в том числе на сбор статистических данных о распространении и конфигурации TLS в глобальной сети.

Таким образом, можно выделить список основных функций подобных сервисов: сбор и хранение TLS-сертификатов; сохранение сопутствующих метаданных — IP-адресов, временных меток и информации о владельце; обеспечение возможности быстрого поиска и фильтрации TLS-сертификатов по различным критериям; проведение автоматизированного анализа криптографических параметров TLS-сертификатов с целью выявления потенциально скомпрометированных или слабых ключей.

Проектирование базы данных

В процессе анализа спецификаций и стандартов, предписывающих нормы и правила использования TLS-сертификатов, были выбраны следующие сценарии поиска данных в разрабатываемой системе.

1. Поиск TLS-сертификатов по IP-адресу. Позволяет находить все сертификаты, полученные с узлов под данными IP-адресами. (В данной разработке используется только IPv4.) Этот сценарий полезен при расследовании инцидентов безопасности, когда известен IP-адрес, связанный с подозрительной активностью. Для реализации было выбрано два способа поиска — по точному совпадению IP-адреса и по сетевому префиксу. Точное совпадение может использоваться, если злоумышленник использует определённый сервер. Поиск по префиксу может применяться при внутреннем аудите инфраструктуры; чтобы проверить адресно «близкие» узлы; определить, какие именно TLS-сертификаты установлены на различных серверах одной информационной системы; а также при исследовании активности вредоносных сетей или CDN.
2. Поиск TLS-сертификатов по издателю. Позволяет находить все TLS-сертификаты, выпущенные указанным удостоверяющим центром. В случае его компрометации или выявления недобросовестного поведения со стороны УЦ этот сценарий позволяет быстро найти все выпущенные им TLS-сертификаты и оценить масштаб возможного риска. Также он может использоваться для внутреннего контроля — например, чтобы убедиться, что используют только доверенные УЦ.
3. Поиск TLS-сертификатов по серийному номеру. Номер TLS-сертификата — это уникальный идентификатор, который может быть использован для отслеживания конкретного экземпляра. Номер должен быть уникальным, чтобы избежать коллизий при управлении TLS-сертификатами. Также с номерами сертификатов связаны некоторые особенности: например, предсказуемость номера может свидетельствовать о наличии уязвимости в системах УЦ и создать конфликт в системах мониторинга — так, ранее из-за использования нестойких хеш-функций УЦ (MD5) злоумышленник мог на практике угадать серийный номер и получить «дублирующий», поддельный сертификат с валидной подписью. Для разработки хранилища были выбраны два сценария поиска сертификатов с заданными серийными номерами — по точному совпадению и по подстроке в символьной записи номера. Точное совпадение позволяет быстро искать узлы и TLS-сертификаты по их серийному номеру или получать список различных TLS-сертификатов с одним номером. Реализация поиска по подстроке обеспечивает возможность обнаружения паттернов в создании серийных номеров TLS-сертификатов при их выпуске.
4. Поиск по значению открытого ключа. Позволяет находить сертификаты с ключами, обладающими некоторыми математическими особенностями. Важным аспектом в обеспечении безопасности является нахождение TLS-сертификатов, использующих конкретный открытый ключ, а также нахождение ключей, криптографические элементы которых математически зависят друг от друга. Необходимо обеспечить возможность расширения доступных математических операций над значениями ключей путём универсального хранения необходимых данных для исследований. Для реализации были выбраны следующие сценарии: поиск по точному совпадению элементов публичных ключей разных типов; поиск TLS-сертификатов, для которых значения модуля RSA-ключа не взаимно просты. Последний сценарий позволит обнаружить ключи, уязвимые к факторизации тривиальными методами.
5. Поиск по шестнадцатеричному значению представления открытого ключа. Шестнадцатеричное представление ключа часто используется в отчётах, логах и исследованиях. Возможность поиска по нему может помочь в сопоставлении данных между различными системами, а также в поиске TLS-сертификатов, использующих аналогичные или похожие ключи. Так же, как и для серийных номеров, были выбраны реализации сценария с частичным и полным совпадением.

Оптимизация процессов поиска

В данном проекте основным способом обеспечения большой производительности является хранение всех данных в оперативной памяти, что и обозначается термином «in-методу хранилище».

Оптимизация алгоритмов поиска в системе хранения TLS-сертификатов, размещённой в оперативной памяти, тоже играет ключевую роль в обеспечении высокой производительности и эффективности анализа данных. Поскольку объём хранимых TLS-сертификатов может быть очень большим — особенно при сборе информации из Интернета, — простые переборные или линейные методы поиска становятся неприемлемыми с точки зрения времени отклика. Для оптимизации и ускорения были выбраны следующие структуры:

1. Radix Tree — представляет собой сжатое дерево префиксов, в котором ключи хранятся в виде строк, а пути между узлами определяются общими префиксами. В отличие от обычного префиксного дерева, Radix Tree объединяет узлы с единственным дочерним элементом, что позволяет значительно сократить объём используемой памяти и повысить эффективность поиска. В контексте разрабатываемого хранилища TLS-сертификатов Radix Tree применяется для поиска TLS-сертификатов по префиксу IP-адреса, поскольку хорошо соответствует принципам организации IP-адресного пространства. Это особенно полезно при анализе подсетей или при обработке запросов, связанных с группами IP-адресов. Основными преимуществами использования Radix Tree в данном случае являются низкая вычислительная сложность выполнения операций вставки, поиска и удаления, а также возможность эффективной реализации диапазонных запросов на основе IP-префикса.
2. Suffix Automaton — это компактная структура данных, представляющая собой минимальный детерминированный конечный автомат, распознающий элементы множества суффиксов базовой строки. Одним из ключевых свойств суффиксного автомата является линейная зависимость количества состояний и количества переходов от длины входной строки, позволяющая работать с большими объёмами данных. В данной системе суффиксный автомат используется для поиска TLS-сертификатов по частичному совпадению в шестнадцатеричном представлении открытого ключа и серийного номера. Это позволяет находить TLS-сертификаты, содержащие заданную последовательность символов в этих полях, что имеет важное значение при выявлении потенциально скомпрометированных или слабых криптографических параметров. Суффиксный автомат обеспечивает линейную временную сложность построения и логарифмическую сложность поиска.
3. sync.Map — это конкурентно-безопасная реализация ассоциативных массивов из стандартной библиотеки языка Go, которая оптимизирована для случаев, когда один набор ключей читается многократно, но изменяется редко. В данном проекте sync.Map применяется для хранения TLS-сертификатов в привязке к различным индексным множествам: IP-адрес, издатель, серийный номер, шестнадцатеричное представление открытого ключа. Это позволяет находить точные совпадения за практически постоянное количество базовых операций и при этом обеспечивать потокобезопасный (конкурентный) доступ к данным без внешних механизмов блокирования и синхронизации. Данный тип структуры выбран из-за своей производительности и безопасности использования при параллельных вычислениях.

Описанные решения позволяют существенно снизить временную сложность выполнения запросов, обеспечивая логарифмическую или даже константную скорость доступа к данным. Поиск эффективен не только для простых «пользовательских» запросов, но и для автоматизированного анализа метрик безопасности, например, мониторинга скомпрометированных или слабых ключей. Благодаря оптимизации механизмов поиска система является масштабируемой,

отзывчивой и пригодной для решения задач информационной безопасности в режиме реального времени.

Разработка программного приложения

В качестве языка реализации был выбран язык Go, предоставляющий встроенную поддержку параллелизма через go-рутины и каналы, что позволяет эффективно управлять множеством одновременных операций ввода-вывода и обработки данных. Кроме того, стандартная библиотека Go содержит мощные инструменты работы с криптографическими примитивами, что существенно упрощает работу с TLS-сертификатами.

Проект реализован по модульной архитектуре, включающей слои доставки (delivery), бизнес-логики (usecase) и хранения данных (repository). Основное хранилище TLS-сертификатов представлено структурой Repository (рис. 2), которая содержит несколько специализированных контейнеров: sync.Map для точного поиска по IP, издателю, серийному номеру и шестнадцатеричному представлению публичного ключа; Radix Tree для префиксного поиска IP-адресов; Suffix Automaton для поиска частичного совпадения строк серийных номеров и шестнадцатеричных представлений ключей; KeyStorage для хранения и сравнения публичных ключей. Все эти структуры взаимодействуют между собой и обеспечивают эффективный доступ к данным по различным критериям поиска.

```
type Repository struct { 10 usages  ± Софья *
    ipRadixTree      *radixTree.RadixTree
    ipMap             sync.Map
    issuerMap         sync.Map
    serialSuffixAutomaton *suffixAutomaton.SuffixAutomaton
    serialMap         sync.Map
    hexPubKeyMap      sync.Map
    hexPubKeySuffixAutomaton *suffixAutomaton.SuffixAutomaton
    keys              *KeyStorage
    loadWg            sync.WaitGroup
    loadWorkerCh      chan struct{}
```

Рис. 2. Скриншот содержимого структуры Repository.

Доступ к сервису реализуется через HTTP-сервер, запускаемый на номере порта, указанного в конфигурации (по умолчанию — 8080). Сервер реализован с использованием стандартной библиотеки Go net/http. Единственная точка входа — это энд-поинт /query, принимающий JSON-данные в POST-запросах. HTTP-запрос обрабатывается функцией HandleQuery, которая десериализует JSON-объект в структуру domain.Query, передаёт её в уровень usecase и формирует ответ в виде списка TLS-сертификатов или генерирует статус ошибки. Ответ сериализуется в JSON и отправляется обратно клиенту.

Загрузка базы данных TLS-сертификатов выполняется из TSV-файла, каждая строка которого содержит IP-адрес и

Base64-представление DER-кодированного TLS-сертификата. Загрузка выполняется параллельно. Перед добавлением в репозиторий входные данные проходят несколько этапов проверок: корректности формата строки, наличия требуемых полей, успешности декодирования Base64 и последующего разбора x509-сертификата. В случае ошибки на любом из этапов выводится соответствующее сообщение в лог, но обработка остальных строк продолжается.

Параллелизм при загрузке TLS-сертификатов обеспечивается с помощью пула рабочих go-рутин, ограниченного константой `maxLoadWorkers`. Необходимость параллельной обработки обусловлена в рамках задачи тем, что декодирование и парсинг сертификатов достаточно затратны по вычислительным ресурсам, при этом исходные данные базы (TSV) могут находиться на дисковом хранилище со сверхбыстрым доступом (SSD и пр.). Обновление исходных данных также может происходить с высокой частотой, а система планируется для использования на выборках, состоящих из десятков миллионов сертификатов. Для контроля количества одновременно работающих go-рутин используется буферизованный канал `loadWorkerCh`. При добавлении каждого TLS-сертификата в репозиторий задействуется механизм конкурентного добавления в разделяемые структуры данных. Для безопасного доступа к `sync.Map` используется метод `StoreToSyncMap`, который применяет мьютекс для модификации содержимого массива TLS-сертификатов, связанных с конкретным ключом. Также используются блокировки в структурах `KeyStorage`, `SuffixAutomaton`, `RadixTree` основанные на `sync.RWMutex`, что гарантирует целостность данных при одновременном чтении и записи.

Обработка TLS-сертификатов происходит в момент их добавления в репозиторий. Метод `AddCertificate` выполняет семантическое разложение (парсинг) TLS-сертификата на составляющие элементы и добавляет их в соответствующие структуры. Извлечение открытого ключа осуществляется с помощью метода `ExtractKeyInfo`, который поддерживает RSA и ECDSA-ключи. Для каждого найденного ключа вычисляется его уникальный хеш, используемый как идентификатор в `KeyStorage`. Шестнадцатеричное символьное представление открытого ключа рассчитывается с помощью `hex.EncodeToString`, а серийный номер преобразуется в строковое представление. Эти данные добавляются в `HexPubKeyMap` и `serialMap` соответственно, а также регистрируются в суффиксных автоматах для обеспечения возможности частичного поиска. IP-адреса заносятся в `ipMap` и дерево `Radix Tree`, что позволяет выполнять как точный, так и префиксный поиск.

Запросы к системе поступают методом HTTP POST на энд-поинт `/query` в виде JSON-объектов, содержащих два поля: `Action` и `Query`. Поле `Action` определяет тип действия, в рамках данной реализации оно всегда имеет значение «Select». Поле `Query` представляет собой вложенную структуру, где ключом является тип фильтрации (например, «IP», «Issuer», «Serial»), а значением — ещё один объект, содержащий поля «Func» и «Value». Поддерживаются следующие функции поиска: «Equal» — точное совпадение, «Prefix» — префиксный поиск, «Contains» — частичное совпадение. Запросы десериализуются с помощью `json.NewDecoder`, и проводится строгая проверка структуры данных. Если запрос не соответствует ожидаемому формату, возвращается ошибка.

Обработка запросов выполняется на уровне `usecase`, где реализован метод, вызывающий соответствующую функцию поиска в репозитории. После обработки результаты преобразуются в структуру, включающую информацию о TLS-сертификате в удобном для пользователя виде, в том числе в закодированном в Base64 виде и детализированном формате. Полученный список TLS-сертификатов сериализуется в JSON и отправляется обратно клиенту.

Таким образом, реализация приложения выполнена с учётом требований к высокой производительности, параллелизму и безопасности. Выбранный язык Go позволил эффективно использовать конкурентные конструкции, а именно — go-рутины, мьютексы и `sync.Map`. Проект предполагает разделение на уровни, что обеспечивает простоту расширения и тестирования. Система позволяет быстро находить TLS-сертификаты по различным критериям, включая точное и частичное совпадение, а также анализировать криптографические свойства, например, наличие общих множителей в RSA-модулях.

Заключение

Разработанная система может применяться в различных сферах, где требуется оперативный доступ к TLS-информации:

1. Мониторинг и выявление подозрительных TLS-сертификатов, связанных с известными угрозами, анализ временных меток и поведения удостоверяющих центров.
2. Анализ безопасности: обнаружение повторяющихся открытых ключей, предсказуемых серийных номеров, слабых RSA-ключей, использующих общие множители.
3. Исследования: сбор и анализ TLS-сертификатов в академических и научных целях, включая исследование распространённых практик выпуска TLS-сертификатов и выявления отклонений от стандартов безопасности.
4. Корпоративный аудит: организация может использовать систему для внутреннего контроля собственных TLS-ресурсов, включая мониторинг истечения срока действия, управление отзывом и анализ использования ключевых материалов.

Дальнейшее развитие системы может включать несколько перспективных направлений:

1. Добавление `persistence`: дополнение in-memory хранилища средствами выгрузки данных долговременного хранения на дисковую подсистему, что позволит сохранять состояние системы и данные между запусками, работать с объёмами, превышающими доступную оперативную память.
2. Расширение типов поисковых запросов. В ходе проектирования построение системы происходило с опорой на возможные дальнейшие улучшения.

3. Интеграция с Certificate Transparency Logs: возможность автоматического получения новых TLS-сертификатов из публичных журналов CT и сравнения их с уже хранимыми данными для выявления неправильно выпущенных или потенциально опасных TLS-сертификатов.
4. Механизм подписки на события: добавление уведомлений о появлении новых TLS-сертификатов, истечении срока действия, обнаружении дублирования ключей и других событиях, важных для обеспечения информационной безопасности.
5. Поддержка дополнительных источников данных: расширение возможностей загрузки TLS-сертификатов за счёт непосредственной интеграции с сетевыми сканерами (например, ZMap), системами мониторинга трафика и сторонними API.
6. Веб-интерфейс: создание пользовательского интерфейса, позволяющего визуализировать с помощью графиков и таблиц результаты поиска, просматривать детали TLS-сертификатов и выполнять сложные выборки.

Таким образом, разработанная система представляет собой мощный и гибкий инструмент для анализа состояния TLS-инфраструктуры. Её текущая реализация уже позволяет выполнять широкий спектр поисковых и аналитических задач, а дальнейшее развитие открывает возможности применения в промышленных условиях, научных исследованиях и инструментах безопасности. Благодаря использованию современных алгоритмов и структур данных, а также внимательному подходу к организации параллелизма и безопасности, система является ценным инструментом в области обеспечения интернет-безопасности.

Список литературы:

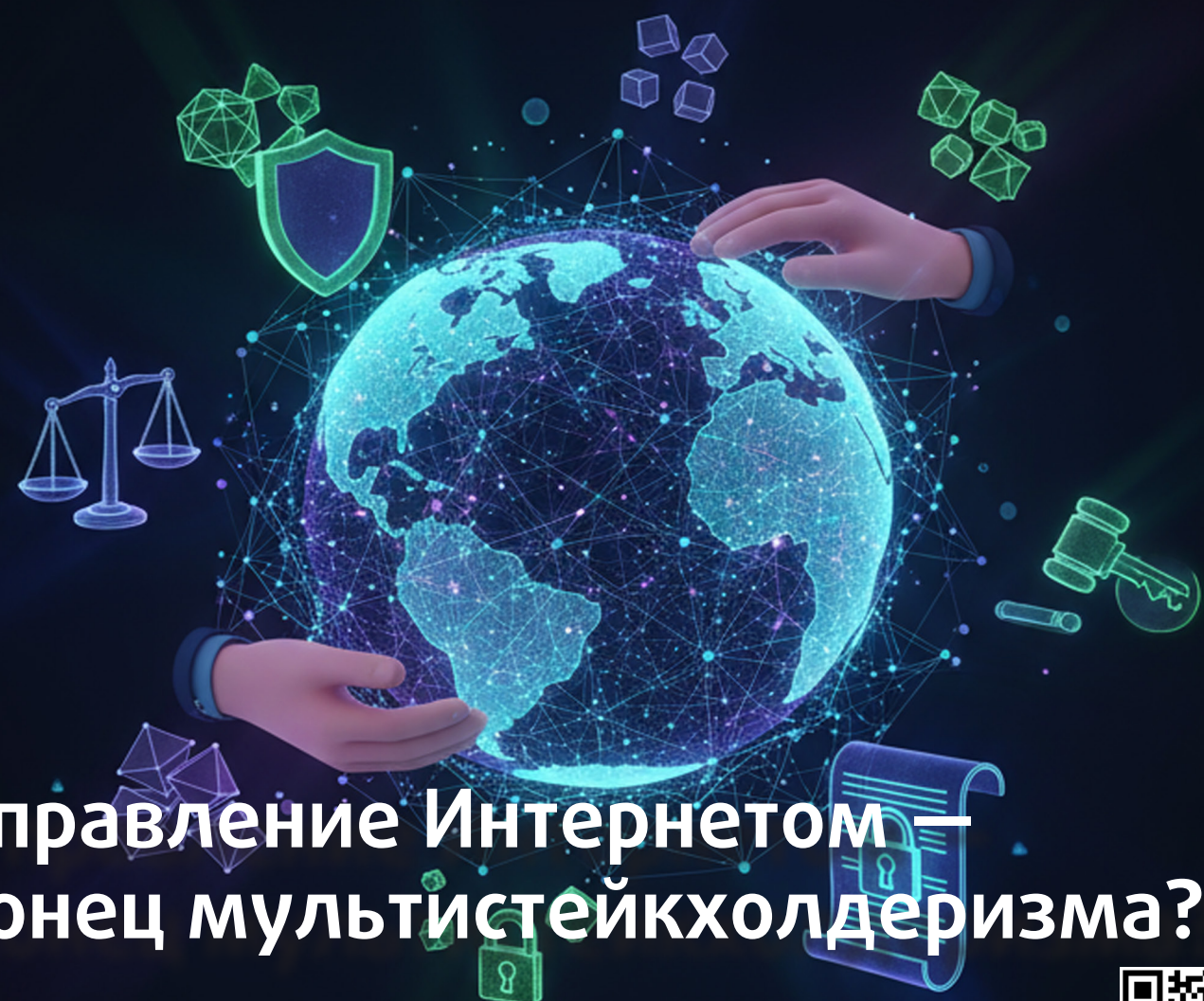
- [1] ТЦИ. Сертификаты удостоверяющих центров TLS. URL: <https://tcinet.ru/press-centre/articles/7746/> (дата обращения: 25.05.2025).
- [2] TLS. Введение в TLS. URL: <https://tls.dxdт.ru/tls.html#intro> (дата обращения: 20.10.2023).
- [3] DXDT.RU TLS для DevOps. URL: <https://dxdт.ru/2021/11/28/9135/> (дата обращения: 25.05.2025).
- [4] IETF. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. URL: <https://www.ietf.org/rfc/rfc5280.txt> (дата обращения: 25.05.2025).

Об авторах

Венедюхин Александр Анатольевич,
ведущий специалист ФРСТ «ИнДата»

Проклашкина Софья Антоновна,
студентка МГТУ им. Н.Э. Баумана





Управление Интернетом — конец мультистейкхолдеризма?

Джефф Хьюстон



Аннотация

Статья посвящена вопросам управления Интернетом на мировом и государственном уровне и эволюции этого процесса за прошедшие 20 лет с его старта.

На определённом этапе своего развития Интернет вышел за рамки породившей его научно-исследовательской среды и занял видное место в телекоммуникационной отрасли. Именно тогда первопроходцы интернет-технологий обнаружили себя в оппозиции к закреплённым в международных соглашениях, выработанным телеком-отраслью устоявшимся подходам и даже тем принципам, на которых основывались такие соглашения. Многие годы они не прекращали убеждать власти в особой сущности Интернета, утверждая, что если распространить на Интернет существующие на национальном уровне механизмы регулирования телекоммуникаций и правила торговли, то это пусть и не сделает работу Интернета невозможной, но уж точно приведёт к изоляции страны, пытающиеся действовать таким образом.

В рамках этой достаточно абстрактной дискуссии также возникло понимание, что традиционные способы торговли услугами к Интернету неприменимы. Поначалу все твердили: «Интернет должен быть бесплатным!» Но от этого лозунга достаточно быстро пришлось отказаться с осознанием достаточно прозаичной

реальности — счета оплачивать всё равно нужно. Тогда дискурс переключился на новую мантру: «Никаких налогов в Интернете!» Этот лозунг приобрёл более широкое звучание. Его суть заключалась в обращённом к властям стран мира призыве не создавать ненужных препятствий при распространении информации за счёт налогообложения и других сборов, поскольку если действовать неаккуратно и безответственно, такие действия могут привести к снижению ценности Интернета в будущем. В то время перед телекоммуникационным сообществом открылась уникальная возможность вырвать эту сферу из рук устаревших и забюрократизированных телефонных монополий и привнести присущий компьютерной отрасли динамизм и инновационный дух в сферу телекоммуникаций.

Хотя в 1990-е годы Интернет мог претендовать на какой-то исключительный статус, в долгосрочной перспективе такое позиционирование оказалось несостоятельным. К началу XXI века стало очевидно, что система прошлого, в которой на первых ролях находились национальные операторы телефонной связи, а страны регулировали международные аспекты оказания

таких услуг на глобальном уровне за счёт заключения соглашений, утратила свою актуальность. Интернет всё сметал на своём пути. В какую бы сферу деятельности он ни проникал, с чем бы ни сталкивался, каждое такое столкновение заканчивалось триумфом Интернета. Да, Интернет, возможно, и являлся исключительным, но к началу века все признали, что эта исключительность не всегда приносила что-то хорошее. В 2003 и 2005 годах Организация Объединённых Наций проводила в два захода Всемирную встречу на высшем уровне по вопросам информационного общества (ВВУИО) с целью осмыслить произошедшие изменения и, в идеале, сделать так, чтобы эта революция в сфере компьютерных технологий и коммуникаций принесла пользу экономикам всех стран мира.

ВВУИО проводилась в контексте формирования так называемого информационного общества на фоне осознания растущего «цифрового неравенства», ведь более состоятельные страны обладали явным преимуществом, чтобы воспользоваться теми возможностями, которые давало наличие огромных ресурсов в области вычислительных мощностей и телекоммуникационных услуг. За счёт этого они могли продолжить богатеть, тогда как страны победнее снова оказались по другую сторону образовавшегося в мире разлома. В результате Интернет не стал средством решения проблемы неравенства в нашем мире за счёт обеспечения доступа к информации, образованию и открытым глобальным рынкам услуг. Напротив, он оказался не более чем новым способом закрепления неравенства между богатыми и бедными.

Центральную роль в обсуждении этого вопроса играли Соединённые Штаты Америки. В то время Интернет ещё во многом ассоциировался с этой страной, и именно США приложили огромные усилия в течение предшествующего десятилетия, пропагандируя Интернет как нечто исключительно полезное, при этом извлекая из этого прибыль за счёт потекшей в карманы американских корпораций, первыми освоивших сферу интернет-услуг, выручки. Очевидно, что в усилиях США по популяризации Интернета и отстаивании свободного обращения информации была и корыстная составляющая. Оказалось, что между интересами появившихся тогда гигантских интернет-корпораций и геополитическими и геоэкономическими устремлениями США довольно много общего.

Однако в рамках крупных международных форумов решать основополагающие вопросы в широком контексте бывает достаточно непросто. Неудивительно, что интернет-сообщество заострило своё внимание на конкретных элементах этой системы. Отдельной темой для обсуждения в этом контексте стал статус структуры, осуществлявшей надзор за параметрами интернет-протоколов, включая доменные имена и IP-адреса, учитывая их центральную роль в функционировании Интернета. Эта структура называлась IANA (Internet Assigned Numbers Authority, Администрация присвоенного номерного пространства Интернета) и изначально функционировала в рамках деятельности, финансируемой Управлением перспективных исследовательских проектов Министерства обороны США. Со временем в структуре органов власти США произошли перемены, и функции IANA перешли на модель самофинансирования под управлением частной организации — Корпорации по управлению доменными именами и IP-адресами (ICANN), хотя США продолжили в некоторой степени принимать участие в её деятельности. Мнения по этому вопросу разошлись: одни говорили, что США тем самым

пытаются сохранить контроль, тогда как другие подчёркивали, что это делалось в целях оградить организацию от возможных трудностей. Но вне зависимости от того, что стояло за этими шагами, входящее в состав Министерства торговли США Национальное управление по телекоммуникациям и информации отвечало за исполнение договора между американскими властями и ICANN по вопросу об исполнении IANA своих функций.

Помимо реальной ситуации, нельзя не учитывать её субъективное восприятие. В данном случае укоренилось мнение, что одно суверенное государство, то есть США, сохраняет контроль над Интернетом.

Закрепление за США такой уникальной роли не могло не стать проблемой для других стран. Работа международной телефонной связи и почты регулировалась заключёнными более века назад международными договорами. Поэтому ситуация, в которой одна страна претендовала на главенствующую роль в Интернете, представлялась, мягко говоря, спорной. Поэтому вполне логично, что это стало одной из основных тем на первой встрече ВВУИО в 2003 году. Занимавший тогда должность Генерального секретаря ООН Кофи Аннан сформировал рабочую группу по управлению Интернетом (РГУИ). Такая формулировка названия группы могла придать её повестке ещё более общее звучание, подчёркивая её актуальность с точки зрения решения вопросов структурирования Интернета. По этому поводу мнения снова разделились. Участники РГУИ так и не смогли прийти к согласию по этому вопросу, и на заседании ВВУИО в 2005 году достичь соглашения также не удалось.

В рамках запущенных ВВУИО процессов США демонстративно отказывались рассматривать идею об изменении их центральной роли в управлении параметрами интернет-протоколов. В конечном счёте участники ВВУИО сошлись на компромиссном подходе — отложить принятие окончательного решения по этому вопросу, а вместо этого провести ряд встреч для обсуждения основополагающих принципов управления Интернетом. Так было положено начало проведению серии встреч в рамках Форума по управлению Интернетом (Internet Governance Forum, IGF). Изначально предполагалось, что на таких мероприятиях никакие решения приниматься не будут. Они служили местом встречи всех заинтересованных сторон для обсуждения соответствующих проблем. Задумка заключалась в том, чтобы проводить такие форумы в течение пяти лет с кульминацией в 2010 году, когда пятый по счёту форум состоялся в Вильнюсе, Литва. Но затем срок его работы продлили ещё на пять лет, после чего последовало продление его полномочий ещё на десятилетний срок. Очередная встреча форума состоялась в Норвегии в конце июня 2025 года. Вопрос о дальнейшем продлении срока работы форума будет обсуждаться на сессии Генеральной ассамблеи ООН осенью 2025 года.

Форумы по управлению Интернетом

Даже ограничившись обсуждением проблем вместо принятия решений, Форум по управлению Интернетом всё равно с трудом справлялся с поставленной перед ним задачей.

В его рамках так и не удалось создать условия для преодоления противоречий, связанных с главенствующей ролью США в Интернете. В 2011 году Индия, Бразилия и Южная Африка выступили с совместной инициативой по созданию комитета ООН по регулированию Интернета. В 2013 году на фоне скандала в связи с опубликованной WikiLeaks информацией о слежке США за другими странами ряд связанных с интернет-отраслью организаций, включая ICANN, региональные регистратуры и рабочая группа инженеров по интернет-технологиям (IETF) выступили с «Монтевидейским заявлением», в котором призвали США отказаться от своей центральной роли в управлении Интернетом. Возможно, изобличение США в ведении слежки также подтолкнуло Бразилию выступить с инициативой netMundial в 2014 году, опять же при видимой поддержке ICANN. Это был очередной призыв в адрес США отказаться от контрольной функции применительно к интернет-протоколам. Примерно в это же время Эдвард Сноуден обнародовал материалы о развёрнутой США широкомасштабной слежке в Интернете.

Столкнувшись с разоблачениями «Викиликс» и Сноудена, США были вынуждены пересмотреть свою позицию и перестать решительно отвергать любые предложения по изменению их роли в управлении Интернетом. В октябре 2016 года свершилось невероятное. Власти США отказались от своего контроля в пользу ICANN, независимой организации.

Если считать целью создания Форума по управлению Интернетом обсуждение вопросов, связанных с привилегированным статусом властей США в Интернете, то можно сказать, что такая повестка утратила свою актуальность в октябре 2016 года. По крайней мере теоретически, США утратили возможность играть определяющую роль в этой сфере.

С другой стороны, такая трактовка и восприятие роли и сферы интересов Форума по управлению Интернетом представляется чрезмерно узкой. В рамках этого формата участникам удалось прийти к общему пониманию функционирования Интернета на разных уровнях, а также того, как его различные составляющие преследуют общие цели, но в то же время приводят к противоречиям. Различные составляющие телекоммуникационных сетей, потребительские устройства, серверы и сети оказания услуг, приложения и прикладные сценарии — всё это функционировало в полуавтономном режиме. Но интернет-отрасль не пошла по прежнему пути, когда контроль над всей системой обслуживания закреплялся за национальным телефонным оператором в рамках отдельно взятой страны. В Интернете различные составляющие процесса оказания услуг рассматриваются как отдельные виды деятельности. Вместо того, чтобы привести их к общему знаменателю в рамках общей системы обслуживания, появился целый ряд новых сегментов рынка: технические стандарты, волоконно-оптические сети и услуги мобильной связи, компьютеры различных размеров — от карманных устройств до серверов, приложения, интернет-операторы и издатели контента. Все они функционируют в полуавтономной среде, а регулируется их деятельность за счёт рыночных механизмов и соответствующего взаимодействия. Не существует какой-то единой компании-оператора, которая бы отвечала за функционирование Интернета, и переход на такую модель неактуален. Речь идёт о нескольких взаимосвязанных рынках. Такой расклад во многом определил процессы, связанные с управлением Интернетом. Форуму удалось вынести на первый план эти перемены и содействовать их обсуждению в конструктивном ключе.

Управление Интернетом сегодня

Позвольте мне очертить три основные темы применительно к управлению Интернетом. Они представляются актуальными как на национальном, так и на международном уровнях в связи с достижением Интернетом современной стадии развития.

Применительно к первой такой теме используется термин «цифровое неравенство». По всему миру всё ещё сохраняется деление на тех, у которых всё есть, и на тех, у кого нет ничего. Цифровое неравенство достигло беспрецедентных масштабов, а каких-либо видимых подвижек, которые могли бы предвещать улучшение ситуации и смягчение социальных последствий такого неравенства, не наблюдается. Более того, это неравенство продолжает усугубляться. В абсолютном исчислении доступом к Интернету в той или иной форме обладает как никогда много людей, что было совершенно невообразимо даже 10 лет назад. Но на сегодняшний день речь всё равно идёт лишь о половине мирового населения, а значит, остальные четыре миллиарда остаются за бортом. Неравенство затрагивает и другие измерения, в том числе, стоимость доступа, качество и скорость подключения, доступность информации и возможность использовать местный язык для получения товаров, услуг и разных сведений. Всё это важные составляющие процесса цифровой маргинализации, даже если на это не всегда обращают внимание.

Говоря о цифровом неравенстве, нам следует взглянуть на эту проблему в более общем плане, обратив внимание на ситуацию с ведущими цифровыми компаниями мира. Речь идёт о таких корпорациях, как Apple, Microsoft, Nvidia, Amazon, Alphabet и Meta (признана в России экстремистской организацией). Их общая капитализация составляла около 12 триллионов долларов накануне недавнего обвала котировок. В совокупности эти шесть компаний настолько огромны и могущественны, что все остальные, будь то физические лица, другие компании и большинство правительств, оказываются в ущемлённом положении с точки зрения цифрового неравенства.

Вторая тема не нова, но за последние два десятилетия она приобрела особое значение. Для описания её многочисленных составляющих используются такие термины, как кибербезопасность, вредоносный код, злоупотребление, спам и вирусы. Если всё это привести к какому-то общему знаменателю, то можно прийти к выводу, что Интернет на современном этапе стал нездоровой средой, где различные преступники чувствуют себя в безопасности, и совершаются различные противоправные действия, наравне с ещё более тёмными делами. В наши дни проблемы использования Интернета террористами и для ведения субъектами кибервойн стоят как никогда остро. Приходится признать, что технические контрмеры оказались недостаточно эффективными. Наше общество уязвимо перед лицом координированных и враждебно настроенных кибератак. Стремясь защитить пользователей от системной слежки в её различных формах и проявлениях, мы создали мощные системы шифрования данных, одновременно лишив себя возможности доводить до сведения правоохранительных органов информацию о различных преступлениях. Как найти баланс между необходимостью обеспечения неприкосновенности личной жизни и установлением личности? Для этого тоже пришлось принимать непростые решения. Анонимность и возможность скрывать сообщения за счёт мощных инструментов шифрования привели к

тому, что обеспечение порядка в цифровом пространстве стало очень затратным делом, сложным и достаточно ограниченным с точки зрения его эффективности. Есть также мнение, что доминирование на своих рынках принесло огромную прибыль ведущим цифровым компаниям, тогда как стоимость распространения базового программного обеспечения и инструментов им удалось переложить на государство.

Третья тема связана с тем, как меняется сам Интернет. В последние годы мы стали свидетелями появления огромного числа систем распространения контента, поставивших своей целью сделать так, чтобы любые данные и услуги находились в непосредственной доступности любого пользователя по первому требованию. Если раньше задача сети заключалась в том, чтобы привлечь пользователя зайти на определённый сайт для получения желаемых материалов, то в наши дни контент, наоборот, смещается в сторону потребителя. Это уже само по себе достаточно существенное изменение для интернет-отрасли. Значимость сетей общего пользования снижается. На смену им приходят частные фидерные сети, обеспечивающие работу постоянно растущих сетей распространения контента. В этой связи возникает вопрос о том, нужна ли глобальная система имён и адресов в среде, где на первый план вышли такие сети распространения контента? Интернет перестал выступать в качестве телекоммуникационной сети, обеспечивающей передачу потоков данных по общим каналам. На современном этапе Интернет превратился в сеть распространения контента, во многом схожую с телевизионным вещанием, когда непосредственная передача данных ограничена так называемой последней милей, с той лишь разницей, что в Интернете каждый пользователь сам формирует свою программу передач.

Как реагировать на эти проблемы? Можно считать такие ситуации примерами общей несостоятельности системы управления Интернетом. Действительно, предоставление частному сектору ничем не ограниченной возможности пользоваться общедоступными системами связи имело далеко не только положительные результаты. Конечно, неумолимое стремление дать пользователям именно то, что они хотят, привело к формированию высокоэффективной и мощной системы подачи материалов, обеспечивающей эффект масштаба и возможность максимально снизить издержки на единицу продукции, что нельзя не признать огромным достижением. В то же время, вопросы общего благополучия и благосостояния общества частный сектор не беспокоят, что делает Интернет жертвой коллективного пренебрежения.

Не исключено, что мы можем стать свидетелями переломного момента в том, что касается попустительства государственной власти по отношению к надменному и беспардонному поведению различных субъектов интернет-отрасли. Принятие в рамках ЕС «Общего регламента по защите данных» стало чётким сигналом об окончании медового месяца для сферы технологий. Во многих странах правительства стремятся повысить ответственность таких субъектов и заставить их оперативно реагировать на общественные запросы. Нет сомнений, что впереди множество штрафов, способных поразить даже крупнейшие корпорации своими размерами. Такие меры не лишены побочных эффектов — небольшие компании уходят с рынка, что подрывает конкуренцию. Однако повышение роли государства в этой сфере позволит достичь нового уровня с точки зрения общественной ответственности крупнейших субъектов. Нет со-

мнений, что такие тенденции будут наблюдаться как в ЕС, так и в рамках многих других нормативно-правовых систем.

Можно ли считать повышение роли национальных правительств признаком несостоятельности системы управления Интернетом? А может, это просто свидетельство неспособности обеспечить эффективное государственное регулирование этой отрасли традиционными методами? Частные компании в первую очередь обязаны руководствоваться интересами своих акционеров, тогда как обеспечение общественного благосостояния может не входить в их задачи. Иногда корыстные интересы совпадают с потребностями общества, и тогда всё хорошо. Но если между ними наблюдается расхождение, корыстные корпоративные интересы всегда берут верх. Было бы наивно ожидать, что частный сектор прислушается к призывам проявить сдержанность или осторожность, если не столкнётся с каким-то принуждением со стороны регуляторов, способных ввести штрафные санкции.

Власти осознали, что могут принимать решительные меры в сфере регулирования отрасли, участников которой до последнего времени не заставляли проявлять социальную ответственность. Но если это так, то как такие власти отнесутся к тем, кто обеспечивает работу различных составляющих инфраструктуры Интернета?

Восстановление межгосударственных границ

Предпринятые президентом США в последнее время хаотичные меры с целью развязать торговую войну по всему миру ещё долго будут напоминать о себе, причём последствия этих действий затронут не только фондовые рынки. Так или иначе, но цифровой мир и то, что мы называем «управлением Интернетом», тоже ощутят на себе их воздействие. По сути, введение Соединёнными Штатами пошлин в одностороннем порядке можно рассматривать как выражение Америкой недоверия к системе международной торговли и открытым рынкам, а также как признак возрождения дискурса о стратегической необходимости обеспечить самодостаточность страны во всех сферах экономической деятельности, в том числе в цифровом мире.

Соответственно, вопрос заключается в том, как на это отреагируют другие страны.

На этой неделе мне на глаза попало сообщение одного хостинг-провайдера по вопросу о работе с российскими доменными именами: «Направляем вам это сообщение в связи с недавним обращением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Речь идёт о возможном введении ограничений в отношении иностранных компаний, оказывающих услуги хостинга, и необходимости для администраторов доменов, у которых размещена за границей инфраструктура DNS, перейти на обслуживание к российским хостинг-провайдерам, внесённым в официальный реестр».

Тот факт, что значительная часть цифровой инфраструктуры находится под управлением иностранных компаний, что, в большинстве случаев, означает компании из США, вызывает всё большую озабоченность в разных странах применительно к регулированию цифровой отрасли.

В настоящее время в сфере цифровых коммуникаций единой системы регулирования не существует, так что от фрагментации и распада её удерживают коммерческие договоры. При этом президент США своими, казалось бы, спонтанными приказами может в любой момент отменить тот или иной договор, что, конечно, не даёт спокойно спать многим участникам отрасли. Можно предположить, что в худшем случае такие американские компании могут быть задействованы с целью сделать цифровую инфраструктуру страны заложницей стремления добиться заключения торговых соглашений на выгодных условиях в соответствии с набившей оскомину концепцией Трампа об «искусстве заключения сделок». Можно даже представить, что события будут развиваться по ещё более негативному сценарию, и такие компании заставят проявлять открытую враждебность по отношению к иностранным заказчикам и устраивать сбои при оказании им услуг. Что ждёт современную цифровую экономику отдельно взятой страны, если её инфраструктура подвергается преднамеренному саботажу со стороны иностранных предприятий, действующих на основании официального приказа?

Нынешний порядок управления Интернетом действует независимо от Международного союза электросвязи (МСЭ) — исторического договорного органа в сфере коммуникаций. Дело в том, что в конце 1990-х годов администрация президента США Билла Клинтона встала во главе коалиции дружественных экономик, включая Австралию, Канаду, Японию и ЕС. Они выступили за закрепление за частной организацией функции по распределению и администрированию различных составляющих инфраструктуры Интернета, в первую очередь имён и адресов, руководствуясь принципом «управления Интернетом с участием всех заинтересованных сторон». Многие годы признание со стороны США такой формы саморегулирования отрасли было более фиктивным, нежели реальным, поскольку американские власти в лице входящего в состав Министерства торговли Национального управления по телекоммуникациям и информационным технологиям всё равно подспудно осуществляли контроль над корневой зоной DNS. Однако, как уже отмечалось, администрация США около десяти лет назад отказалась от этой надзорной функции и перестала вмешиваться в эти процессы. Изрядно подпортив свою репутацию скандалами с «Викиликс» и Сноуденом, США потеряли желание тратить свой дипломатический капитал на сохранение этой коалиции.

Можно утверждать, что в любом случае задача была выполнена к 2020 году. Значительная часть Интернета оказалась в руках узкого круга огромных американских корпораций, так что властям США уже не требовалось поддерживать их на международной арене. У других стран были разные причины принять такую систему. Кого-то соблазнили абстрактные обещания процветания за счёт цифровых технологий, тогда как другие видели возможность извлечь какую-то выгоду из перехода на цифровую инфраструктуру.

Однако этот «новый» мир совершенно не похож на старый промышленный мир в том, что касается распределения эконо-

мических ресурсов и власти. Размещение в стране крупной цифровой компании не всегда оказывается залогом всеобщего экономического процветания. В цифровых компаниях работает не так много людей, а чрезмерная концентрация богатства нередко приводит к различным ухищрениям по уклонению от действующих в отношении обычных компаний налоговых требований. Проблема в том, что блага от цифровой экономики распределяются неравномерно: появляется горстка невероятно состоятельных людей, тогда как значительная часть населения стран терпят лишения и страдают от маргинализации.

Неудивительно, что во многих странах реакцией на эту ситуацию стал рост популярности популизма. Это коснулось не только США, но и Германии, Франции, Венгрии и Великобритании, а также других западных стран. Одной из основ этих популистских течений стало обещание восстановить прежний порядок, обеспечивающий «защиту» экономики страны, и отказаться от многих форм глобализма.

В настоящее время эти процессы проявляются различными формами фрагментации. Речь идёт не только об ограничении перемещения товаров через границы за счёт введения запретительных пошлин, но и об удержании цифровых активов и инфраструктуры внутри своих стран, чтобы место деятельности и регистрации цифровых компаний совпадало.

Стоит ли говорить, что ничего хорошего это Интернету не принесёт. Всё свидетельствует о том, что мы вернёмся к системе, в которой международное взаимодействие регулируется посредством множества правил, принятых на уровне договорных организаций. Принцип участия в управлении Интернетом всех заинтересованных сторон на международном уровне представляется не особо привлекательным, учитывая, насколько он был извращён небольшой кликой цифровых гигантов для извлечения ими максимальной пользы.

Эта проблема встаёт с особенной остротой в 2025 году. В рамках встречи ВВУИО+20 вновь поднят вопрос о целесообразности следования принципу участия в управлении Интернетом всех заинтересованных сторон. В наши дни на первый план вышел мем о «национальном интернет-суверенитете», а понятие многосторонности теперь кажется более привлекательным, чем принцип участия в управлении Интернетом всех заинтересованных сторон, в том, что касается удовлетворения запроса на повышение уровня самодостаточности национальных экономик, в особенности там, где на первый план в общественно-политической жизни вышел популизм. Эти дискуссии разворачиваются на фоне полного разрушения старого порядка усилиями США. Пока неясно, каким образом США намереваются отстаивать модель участия в управлении Интернетом всех заинтересованных сторон, и будут ли они вообще это делать. Предпринятые США в последнее время сумбурные действия по введению торговых пошлин свидетельствуют о том, что США утратили кредит доверия и больше не могут претендовать на роль непоколебимого сторонника принципа участия всех заинтересованных сторон в управлении Интернетом на международной арене.

В середине 2024 года ряд других национальных структур, включая регистратуры доменов .au (AUDA), .ca (CIRA), .nz (InternetNZ) и .uk (Nominet), создали коалицию в поддержку

этой модели управления Интернетом, назвав ее Коалицией технического сообщества в поддержку принципа участия всех заинтересованных сторон в управлении Интернетом. Получается, что эти страны пытаются заполнить эту нишу после ухода из неё США, чьё отсутствие среди этих стран действительно бросается в глаза.

Со своей стороны могу пожелать этой группе всяческих успехов. В то же время, нельзя не отметить, что, учитывая текущую международную ситуацию, условия для них складываются очень неблагоприятно. Им будет очень сложно убедить кого-либо поверить в идеалы, принятые на вооружение в рамках ВВУИО около 20 лет назад, и доказать, что модель участия всех заинтересованных сторон в управлении Интернетом может способствовать развитию цифровых экономик таким образом, чтобы все извлекали из этого выгоду. Это объясняется проблемами в области кибербезопасности и возникновением различных уязвимостей, настойчивостью крупнейших цифровых корпораций США в отстаивании своих интересов, а также исключительно непоследовательной позицией властей США на современном этапе. Гораздо проще прийти к выводу, что такая система сыграла отведённую ей роль в истории цифровых технологий, так что теперь такие компании, как Alphabet, Microsoft, Amazon и Meta, должны сказать нам спасибо за то, что мы дали им возможность быстро добиться мирового господства.

Что дальше?

Грядущие годы, к сожалению, ничего кроме исключительного пессимизма у меня не вызывают. Попытка сделать так, чтобы частные компании стремились отстаивать интересы общества в телекоммуникационной отрасли, участниками которой все мы являемся, снова провалились. Это напоминает мне то, как в начале XX века Теодор Вейл (Theodore Vail) пытался заключить сделку с Конгрессом США, чтобы сделать компанию AT&T монополистом в сфере телефонной связи, обещая, что компания взамен будет проявлять сдержанность, руководствоваться прогрессивными идеями и действовать в интересах страны и общества. В конечном счете AT&T следовала этим принципам не более десятилетия и не устояла перед соблазном злоупотреблять своей монополией.

Такое впечатление, что принцип участия в управлении Интернетом всех заинтересованных сторон уходит в прошлое под давлением стран, отстаивающих свою автономию. Позиция США на международной арене лишь ускорила этот процесс. Скорее всего, в области управления Интернетом произойдёт сдвиг к многосторонности, что повлечёт за собой увеличение роли ООН и ВТО в том, что касается деятельности стран средней руки, на фоне односторонних мер США и связанной с ними нестабильности.

Можно ли считать все эти изменения результатом президентских выборов 2024 года в США? Насколько бы изменилась ситуация, если бы кандидаты были другие, а результат отличался от реального?

Я считаю, что речь идёт о гораздо более глубоких процессах и силах, которые нельзя свести к отдельным деятелям и их действиям, какими бы хаотичными и непредсказуемыми они ни были. В нашем обществе назревают перемены, по своему масштабу и болезненности ничем не уступающие промышленной революции XIX века. Такие потрясения вносят разлад в функционирование общества и становятся источником нестабильности. Разворачивающаяся сейчас информационная революция пошла по тому же пути. Неудивительно, что отдельные страны стали действовать в таких ситуациях более решительно, пытались преодолеть наиболее явные социальные перегибы. Одним из побочных эффектов нарастания таких эгоцентричных устремлений стран и развития там популистских движений стало снижение доверия к различным региональным и всемирным международным институтам. Столкнувшись с неопределённостью и оказавшись в состоянии стресса, страны бросились «поднимать мосты», чтобы самоизолироваться от происходящих в мире перемен за счёт установления более жёсткого контроля над тем, что происходит внутри их границ. Социальные проблемы они списывают на действия иностранных структур, при этом утверждая, что повышение уровня самостоятельности страны позволит хотя бы отчасти возродить миф о национальном величии и процветании.

Совершенствование паровой тяги породило промышленную революцию. Это изменило общество, причём социальные последствия носили гораздо более широкомасштабные последствия по сравнению с изобретением достаточно простого механического устройства. Аналогичным образом можно предположить, что многие из проблем современности не связаны с Интернетом или способом управления им. Возможно, именно более широкие проблемы, связанные с нашим энтузиазмом в отношении вычислительной техники и коммуникаций, стали движущей силой масштабных социальных потрясений в современном мире.

*Заявление об отказе от ответственности

Изложенные выше взгляды могут не совпадать со взглядами и позицией Азиатско-Тихоокеанского сетевого информационного центра.

Об авторе

Джефф Хьюстон, магистр наук, главный научный сотрудник APNIC, региональной интернет-регистрации, обслуживающей Азиатско-Тихоокеанский регион.
www.potaroo.net

Интернет-управление на практике: невидимые механизмы, которые держат Сеть

Андрей Юров

Аннотация

За громкими дискуссиями о свободе слова, цифровом суверенитете и глобальной политике редко замечают ту часть интернет-управления, которая работает «под капотом» и обеспечивает стабильность всей Сети. Именно здесь распределяются IP-адреса и поддерживается работа корневых DNS-серверов — фундаментальных элементов, без которых Интернет просто не существовал бы. Сегодня в этих областях назревают важные перемены: новые предложения по модели управления региональными интернет-регистратурами и проект функциональной модели системы корневых серверов DNS. Эти инициативы меняют правила игры в практическом интернет-управлении и напрямую касаются устойчивости и будущего развития Сети, которой ежедневно пользуются миллиарды людей.



Ключевые слова:

цифровой суверенитет, управление Интернетом, Internet Governance.

Введение

За последние 20 лет дискуссии, касающиеся проблематики интернет-управления, постепенно сместились в область цифрового сообщества, прав человека и свободы слова. При этом не стоит забывать, что реальное управление Интернетом по-прежнему в значительной степени происходит на уровне инфраструктуры. На этом уровне три системы имеют фундаментальное значение:

- Система распределения номерных ресурсов;
- Глобальная система доменных имён и в особенности её корень;
- Система межсетевых соединений и обмена трафиком.

В этой статье мы остановимся на первых двух. Эти области и связанные с ними системы управления органично развивались с ранних лет Интернета и проявили поразительную адаптивность. Однако сегодня чувствуется власть времени. Интернет является неотъемлемой частью сообщества и од-

ним из факторов экономического и социального благосостояния, соответственно, и требования к управлению этими критическими областями высоки.

Отмечу, что система управления здесь существенно отличается от традиционных подходов к управлению критическими структурами, где национальные правительства несут основную ответственность и играют ключевую роль. Указанные же системы имеют глобальный характер и управляются частными организациями, на основе вовлечения всех заинтересованных сторон — так называемый мультистейкхолдеризм. На протяжении долгого времени предпринимались попытки переместить управление этими критическими системами в лоно ООН и поддержать международными договорами. В основном они оказались безуспешными, хотя и стимулировали важный диалог между заинтересованными сторонами, что привело к определённой демократизации управления цифровым миром в целом.

Краткая история системы распределения номерных ресурсов

Истоки современной системы распределения номерных ресурсов уходят далеко в прошлое. В 1990 году Совет по архитектуре Интернета (IAB) отметил, что «в связи с быстрым ростом числа сетей в Интернете и их одновременной интернационализацией настало время рассмотреть возможность дальнейшего делегирования полномочий по распределению и регистрации на международной основе» [1].

Двумя годами позже была создана первая региональная интернет-регистратура (РИР) – RIPE NCC, с зоной обслуживания, охватывающей Европу, страны бывшего СССР, Ближнего Востока и Северной Африки. В 1994 году последовало официальное признание IANA второй регистратуры – APNIC, отвечавшей за распределение адресного пространства и номеров автономных систем в Азиатско-Тихоокеанском регионе.

Региональные регистратуры RIPE NCC и APNIC эффективно обслуживали соответствующие сообщества операторов в соответствии с ими же разработанными политиками. Этот успех явился одним из факторов разделения функции распределения доменных имён и создания в США отдельной регистратуры для номерных ресурсов. В декабре 1997 была создана Американская регистратура интернет-номеров ARIN. Зона обслуживания включала Северную Америку, страны Латинской Америки, Карибского бассейна и южной части Африки.

В результате мир был разделён на три сферы обслуживания.

Когда в начале 2000-х годов стало очевидно, что нужна отдельная регистратура для обслуживания латиноамериканских сетей, Интернет уже давно вырос из научно-образовательной сети США и стал глобальной сетью, обладающей громадным экономическим и социальным потенциалом. Были формализованы процессы принятия важных решений, в них участвовало международное сообщество. Однако процесс создания новых РИРов отсутствовал. Этот пробел был восполнен документом ICP-2 «Критерии создания новых региональных интернет-регистратур» [2], определяющим основные требования к РИРу. Документ был разработан Советом поддерживающей организации по адресации ICANN (Address Supporting Organization, ASO) при поддержке RIPE NCC, APNIC, ARIN и ратифицирован Советом ICANN в июне 2001 года.

После годового пробного срока 7 ноября 2002 года была официально признана четвертая региональная интернет-регистратура – LACNIC. Часть зоны обслуживания ARIN (Центральная и Латинская Америка и часть стран Карибского бассейна) отошла к новой РИР. За LACNIC последовало создание AFRINIC (в апреле 2005 года), под чью ответственность попал весь Африканский континент, до этого обслуживаемый ARIN и RIPE NCC.

В октябре 2003 года APNIC, ARIN, LACNIC и RIPE NCC заключили соглашение об образовании Организации номерных ресурсов (Number Resource Organization, NRO, <http://www.nro.net>). В 2005 к ним присоединился AFRINIC.

Задачи NRO – обеспечение единого интерфейса взаимодействия системы РИР с внешним миром, а также координация различных совместных проектов регистратур. Руководством деятельностью NRO занимается исполнительный комитет, состоящий из пяти руководителей РИР (формально члены исполкома назначаются советом каждого РИРа).

NRO участвует в разработке политик через Номерной комитет (NRO Number Council). Комитет – это, по существу, независимая от NRO структура, тождественная Адресному совету (Address Council) поддерживающей организации по адресации ICANN (Address Supporting Organization, ASO). Каждое из региональных сообществ РИР выбирает трёх членов для включения в состав Номерного комитета (и, соответственно, в Адресный совет ASO).

Сегодняшняя проблематика

За 30 лет своего существования глобальная система распределения номерных ресурсов не претерпела значительных изменений. Да, увеличилось число РИРов, процессы стали более формализованы, была создана NRO, произошла реформа IANA, но архитектура и принципы работы остались прежними. Это удивительно, учитывая значительные изменения, которые претерпел сам Интернет, включая, не в последнюю очередь, практически полное отсутствие свободных адресов IPv4. Отчасти это объясняется тем, что распределение номерных ресурсов происходит в соответствии с политиками, которые претерпели существенные изменения и продолжают меняться в ногу со временем.

РИРы пересматривают основополагающие принципы системы распределения адресного пространства в отношении IPv4, такие как принцип консервации, необходимости (каждому по потребностям) и принцип, согласно которому IP-адреса не являются собственностью. Так, например, RIPE NCC полностью отказался от принципа необходимости и не требует подтверждения планов использования IPv4 при трансферах.

Но даже более существенным является тот факт, что совместно РИРы обслуживают пул из 3,69 миллиарда используемых адресов, что при цене за адрес около 20 долларов США (в пересчёте на блок /16) и лизинговой стоимости 0,50 доллара в месяц означает управление активами в несколько десятков миллиардов долларов. Неудивительно, что растёт напряжённость между разработанными сообществом политиками, нацеленными на благосостояние экосистемы, и конкретными бизнес-задачами. Это усугубляется тем фактом, что во многих РИРах за последнее десятилетие существенно изменилась композиция сообщества-членство за счёт стремительного роста членов РИР в погоне за оставшимся адресным пространством.

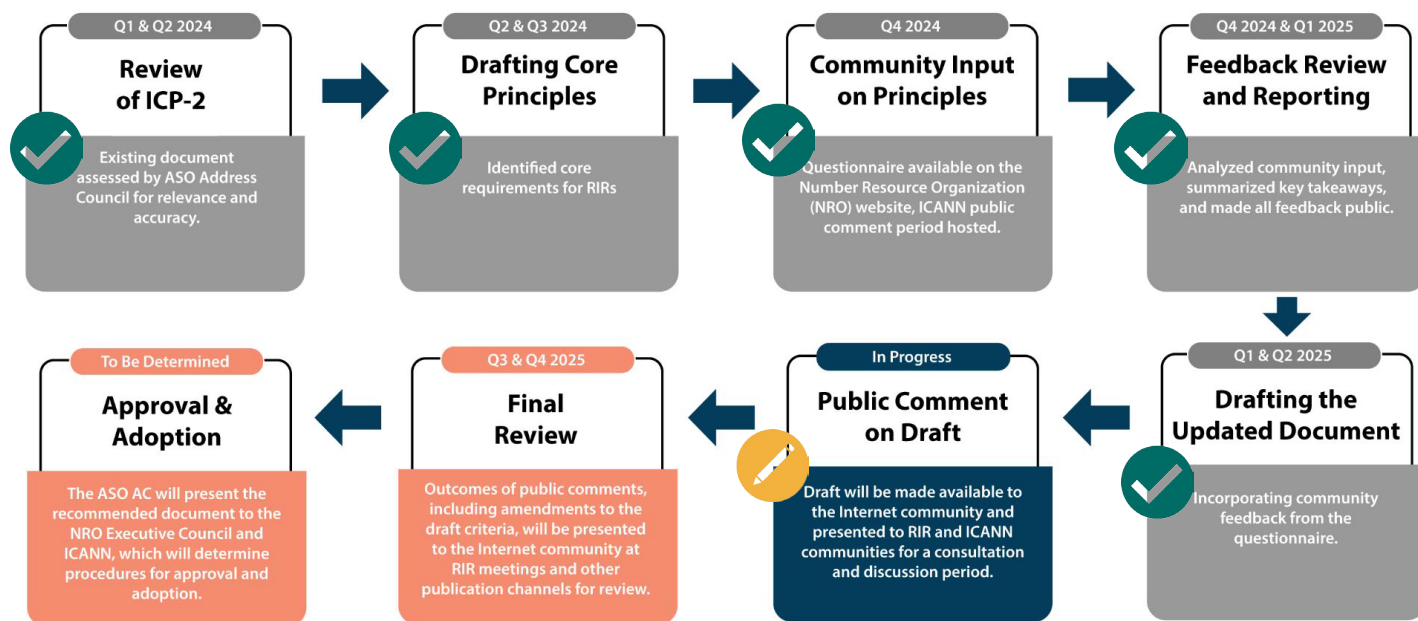


Рис 1. Процесс работы над ревизией ICP-2. Источник: RIPE NCC Open House: Updating ICP-2, 29 April 2025, https://www.ripe.net/documents/4014/RIPE_NCC_Open_House_-_Updating_ICP-2_29042025.pptx.pdf

Порой конфликт выходит за рамки РИРа и переходит в юридическую сферу, как, например, случилось с AFRINIC, когда он попытался отозвать адреса компаний, использующих их не в соответствии с политикой [3].

Ситуация с AFRINIC также поставила перед сообществом и NRO вопрос о том, что должно произойти, если РИР не в состоянии более выполнять свои функции или полностью утратил характеристики как РИР? Основополагающий документ, определяющий требования к организации для признания её в качестве РИРа, ICP-2, не содержит никаких указаний на условия, при которых РИР может утратить свой статус, и на процессы, которые с этим связаны.

Другими словами, в области управления глобальной системой обслуживания номерных ресурсов был очевиден прогал, который было необходимо закрыть как можно скорее. Для этого Исполнительный комитет NRO, состоящий из руководителей РИРов, обратился к Номерному комитету с просьбой организации обновления документа.

Предлагаемые изменения

Если вы знакомы с политикой ICP-2, то первое, что бросается в глаза, - это неформальный тон документа. Причина в том, что ICP-2 задумывался в качестве рекомендации ICANN при рассмотрении заявок от организаций, претендующих на статус РИРа. Напомню, что необходимость такого документа была обусловлена формированием IACNIC и впоследствии - AFRINIC. В то же время велись неформальные обсуждения возможности образования регистратур в других регионах, например, в странах бывшего СССР и Ближнего Востока. Необходимы были объективные критерии, в соответствии с которыми можно было бы принять или отвергнуть запрос.

В отношении процесса особых сомнений не было - ICANN рассматривает заявку и принимает решение. Собственно, по просьбе ICANN и был разработан данный документ. РИРы в ответ разработали рекомендации.

Однако документ оставил без ответа вопросы, важность которых сегодня очевидна:

- Каков процесс рассмотрения заявок и принятия решений? В оригинальном документе роль РИРов в этом процессе не определена, хотя решение ICANN может иметь существенные последствия для системы в целом и для конкретных РИРов. Например, признание нового РИРа неизбежно приведёт к пересмотру регионов обслуживания и переключению существующих контрактов. Сам процесс недостаточно чётко задокументирован. Есть ли возможность обжалования решения ICANN? Как подаётся заявка и каково её содержание?
- Распространяются ли эти критерии на фазу после признания РИР? Очевидно, что изначальные требования должны соблюдаться, но вполне возможно, что после создания РИР должен соответствовать дополнительным требованиям к системе управления, качеству работы и процессу разработки политик. Кто и как осуществляет мониторинг этого соответствия и каковы способы исправления ситуации?
- Что происходит, если РИР перестаёт удовлетворять определённым требованиям? Система, в которой организации существуют вечно, вряд ли реалистична. Различные обстоятельства могут привести к тому, что РИР не может выполнять свои функции в соответствии с требованиями. Каков процесс прекращения действия РИР, при каких обстоятельствах он может быть инициирован и кем?
- Наконец, каким образом обеспечивается непрерывность работы и целостность глобальной системы? Кто и каким образом обеспечивает резервирование критических функций и их активацию в непредвиденных обстоятельствах?

Другими словами, обновление документа ICP-2 подразумевало существенную ревизию и дополнение.

Подход Номерного комитета к этой непростой задаче был следующим: начать с ревизии основополагающих принципов. Принципов, которые охватывают не только стадию признания, но весь жизненный цикл РИР. Принципов, на которых должны базироваться процессы принятия решений. Провести консультационный процесс с глобальным интернет-сообществом и по результатам разработать проект обновлённого документа ICP-2. Процесс этот дорабатывался и детализировался по мере продвижения работы и в конечном счёте принял форму, представленную на рисунке 1.

Почему не был выбран процесс разработки глобальных политик, не совсем понятно. Хотя формально данный документ не является номерной политикой, соответствующий процесс позволил бы обеспечить вовлечение региональных сообществ проверенным практикой стандартным образом. Возможно, ввиду проблем с AFRINIC, не позволяющих обеспечить формальное участие африканского сообщества в этом процессе, этот путь был отвергнут.

На данном этапе проводится обсуждение второй ревизии документа. Она существенно отличается от оригинального документа ICP-2, начиная с названия – «Governance Document for the Recognition, Operation, and Derecognition of Regional Internet Registries» (Руководящий документ по признанию, функционированию и лишению статуса региональных интернет-регистратур) – и заканчивая существенно расширенными рамками: новый документ охватывает весь жизненный цикл РИР (от признания до, при необходимости, лишения статуса и прекращения деятельности) и вводит более подробные требования к управлению, ответственности, прозрачности и процедурам.

Документ непростой и предложенные в нём процессы также весьма запутанны. Это отчасти объясняется различными изменениями, основанными на предложениях и комментариях сообщества, которые наложили свой отпечаток на читаемость документа. Но в основном это обусловлено сложностью самой системы. Хотя система распределения номерных ресурсов является иерархической – ICANN/IANA отвечают за глобальный пул, ресурсы которого распределяются РИРам, которые, в свою очередь, распределяют их по запросам локальных регистратур или сетевых операторов, – система управления таковой не является.

Каждый из РИРов является независимой организацией, по существу, подотчётной только сообществу и членам, которых она обслуживает. Между РИРами существуют официальные отношения, но они не являются коммерческими контрактами в традиционном понимании. Отношения эти закреплены главным образом в Меморандуме о взаимопонимании между NRO (2003 год) [4], который определяет, как РИРы действуют коллективно, сохраняя при этом собственную автономию.

В отношениях с ICANN также отсутствует субординация, предполагая координационный характер взаимоотношений. Это закреплено в Меморандуме о взаимопонимании между ASO и ICANN (2019) [5]. Этот документ устанавливает рамки

взаимной координации и роли в рамках процесса разработки глобальных политик.

Другими словами, власть и легитимность системы находится в руках соответствующих региональных сообществ, а не ICANN или даже NRO.

Именно поэтому более детальный процесс принятия решений в новом документе переносит центр тяжести с ICANN на индивидуальные РИРы, а вся система базируется на координации, добросовестности, взаимном уважении, а не подписанных контрактах.

Хотя документ предлагает достаточно детальные требования к процессам признания новых РИРов и лишения статуса для существующих, аудиту и непрерывности функционирования, прежде чем документ может быть применён на практике, его необходимо будет дополнить так называемыми процедурами реализации (implementation procedures). Каковы объективные метрики для оценки соответствия требованиям документа, каковы требования и процесс выбора оператора экстренной помощи, как в реальности будет выглядеть процесс лишения статуса и передачи полномочий другой организации, в том числе и с правовой точки зрения? Но эти вопросы выходят за рамки работы Комитета.

Перспективы развития системы РИР

Важно заметить, что хотя целью ревизии ICP-2 является обеспечение организационного фундамента функционирования системы РИР в будущем, за исключением нескольких областей, документ в лучшем случае документирует сегодняшнее, если не вчерашнее состояние системы. Фронт работ был определён с самого начала – обновление документа в рамках существующей архитектуры.

Вне всяких сомнений, существующая система доказала свою жизнеспособность, обеспечивая распределение ресурсов на протяжении более трёх десятилетий. Однако меняющийся характер номерных ресурсов, композиция и интересы сообщества ставят важные вопросы о том, какова будет система в будущем.

Несмотря на предохранительные меры, предусмотренные в Руководящем документе, настоящая система имеет ряд фундаментальных проблем. Правительства и компании иногда с беспокойством относятся к неопределённости системы управления региональными интернет-регистрами (RIR), которая недостаточно формализована и не основана на международном праве. Это создаёт непредсказуемость и зависимость от нескольких частных некоммерческих компаний. Система основана на взаимных соглашениях, коллективной ответственности и корпоративном праве пяти различных юрисдикций, а не на мандате, основанном на международных договорах.

Несмотря на свою уникальность, существует определённая параллель между РИР и кадастром недвижимости. Если сравнить глобальную систему распределения номерных ресурсов с глобальными/региональными кадастровыми системами, можно извлечь несколько ценных уроков в области управления, которые система RIR могла бы использовать для укрепления своей легитимности, предсказуемости и устойчивости, не подрывая при этом свой принцип управления «снизу вверх». Обе системы управляют ограниченными, критически важными ресурсами от имени общества; обе требуют точных записей, долгосрочной преемственности и общественного доверия. Кадастровые системы традиционно устанавливаются на основе национального законодательства и в некоторых случаях координируются на региональном или глобальном уровне, что позволяет извлечь уроки, которые могут укрепить устойчивость и легитимность системы РИР.

Вот несколько областей, где может быть применен опыт кадастровой системы:

Формальное признание и легитимность

Кадастровые системы основываются на законах или (международных) договорах. Хотя система RIR основана на принципах ответственности перед сообществом и корпоративном праве, более широкое официальное признание — например, посредством меморандумов о взаимопонимании с правительствами и межправительственными организациями — может обеспечить дополнительную предсказуемость и стабильность.

Взаимодействие и гарантии обслуживания

Региональные кадастровые инициативы обеспечивают соблюдение общих стандартов обмена данными и взаимодействия. Аналогичным образом, РИРы могут укрепить глобальную согласованность услуг регистрации путём стандартизации интерфейсов взаимодействия и обмена данными, обеспечивая надёжность и доверие во всех регионах.

Планирование преемственности

Национальные кадастры гарантируют преемственность даже в случае институциональных изменений. Система РИР пользуется аналогичными гарантиями, включая чёткие процедуры наследования и прекращения признания, и может расширить их за счёт резервирования и механизмов депонирования.

Прозрачность и подотчетность обществу

Земельные реестры являются публичными и подлежат судебному или независимому надзору. Система RIR может усилить свою подотчётность за счёт повышения прозрачности, предоставления независимых механизмов апелляции и проведения периодических проверок системы управления.

Гарантии от захвата

Кадастровые системы защищены от приватизации или неправомерного влияния для сохранения прав собственности. Система RIR может усилить аналогичные гарантии, гарантируя, что ни одно правительство, бизнес или группа интересов не смогут поставить под угрозу её нейтральное управление.

Последние три области освещены в Руководящем документе. Безусловно, дьявол кроется в деталях, и эффективность подходов, описанных в документе, существенным образом зависит от процедур реализации, которые должны быть разработаны в будущем.

Краткая история развития системы корневых серверов

История становления системы управления Интернетом — это, по существу, история становления системы управления DNS. Коммерциализация Интернета в первую очередь и в наибольшей степени затронула именно эту область. А управление инфраструктурой Интернета неразрывно связано с контролем за корневой зоной DNS. От практически монопольного контроля за корневой зоной и регистрации в глобальных доменах компанией Network Solutions Incorporated (NSI, ныне Verisign) до корпорации ICANN и IANA/PTI, формально независимых от правительства США, и раундов по продаже глобальных доменов.

В настоящее время корневую зону обслуживают 13 DNS-серверов [6], также называемых корневыми (КС). Имена КС начинаются с буквы латинского алфавита (от А до М) и имеют общее окончание root-servers.net, например, a.root-servers.net. Эта первая буква также используется как сокращённое имя сервера, например, сервер k.root-servers.net называют «К-сервер». Операторами КС (ОКС) являются 12 организаций по всему миру, получившие право управления серверами в относительно отдалённом прошлом, когда подобные вопросы решались менее формально. Среди операторов — университеты, организации министерства обороны США, некоммерческие ассоциации. За исключением оператора L-сервера, который находится под управлением ICANN, операторы финансово и юридически независимы от корпорации ICANN, в рамках которой действует IANA. При принятии операционных решений операторы руководствуются технической целесообразностью и существующими стандартами (например, RFC 2870 [7]), в основном поддерживая статус-кво. Принято считать, что подобная независимость и разнородность операторов КС является основой технической и политической стабильности системы в целом, исключая узурпацию управления какой-либо из сторон.

Реформа IANA

До октября 2016 года функцию надзора за корневой зоной выполняло правительство США в лице NTIA, поскольку именно это агентство министерства торговли являлось держателем договора на предоставление услуг IANA.

Это означало, что NTIA утверждало любые изменения в корневой зоне и базе данных Whois. Без этого утверждения Verisign, которая, собственно, технически обслуживает и публикует корневую зону, изменений в неё не внесёт.

С передачей функций IANA мировому сообществу NTIA более не участвует в процессе внесения изменений в корневую зону. Контракт между правительством США и Verisign на обслуживание корневой зоны теперь заключён напрямую между Verisign и ICANN. В новой схеме управления корнем DNS Verisign выполняет роль так называемого Root Zone Maintainer и отвечает за публикацию зоны на скрытом мастер-сервере, с которого она распространяется на все 13 КС с использованием протокола TSIG, защищающего данные от модификации при передаче.

Состав корневой зоны постоянно меняется. В среднем в зону вносится несколько изменений в неделю. Например, изменяется информация о DNS-серверах, обслуживающих домен верхнего уровня. Или же требуется добавление нового домена верхнего уровня, хотя такие изменения происходят гораздо реже.

Сегодняшняя проблематика

Сегодня ОКС действуют полностью независимо, по собственной доброй воле и за счёт собственного финансирования, без какого-либо прямого контроля со стороны заинтересованных сторон сервиса, который предоставляется исключительно на основе исторического доверия и добросовестности. Консультативный комитет по системе корневых серверов RSSAC задокументировал большую часть истории и современной структуры работы и управления корневыми серверами, но управление системой КС остаётся в значительной степени неформальным и недокументированным.

С этим связаны очевидные проблемы:

- отсутствие подотчётности и прямого контроля со стороны заинтересованных сторон;
- отсутствие прозрачности требований и соответствия;
- отсутствие формальных обязательств и гарантий устойчивого функционирования как отдельных элементов (операторов), так и системы в целом. В частности, в отношении финансовой устойчивости;
- отсутствие формальных политик, в особенности политик принятия и исключения оператора

Предлагаемые изменения

Документ RSSACo55 [8] определяет 11 принципов функционирования системы КС. Надо отметить, что эти принципы не новы и на практике реализуются существующими ОКС. Наиболее важные в контексте нашего обсуждения принципы:

- IANA является источником данных корневой зоны. Это означает, что корневые серверы обязаны публиковать немодифицированную корневую зону, включая данные DNSSEC.



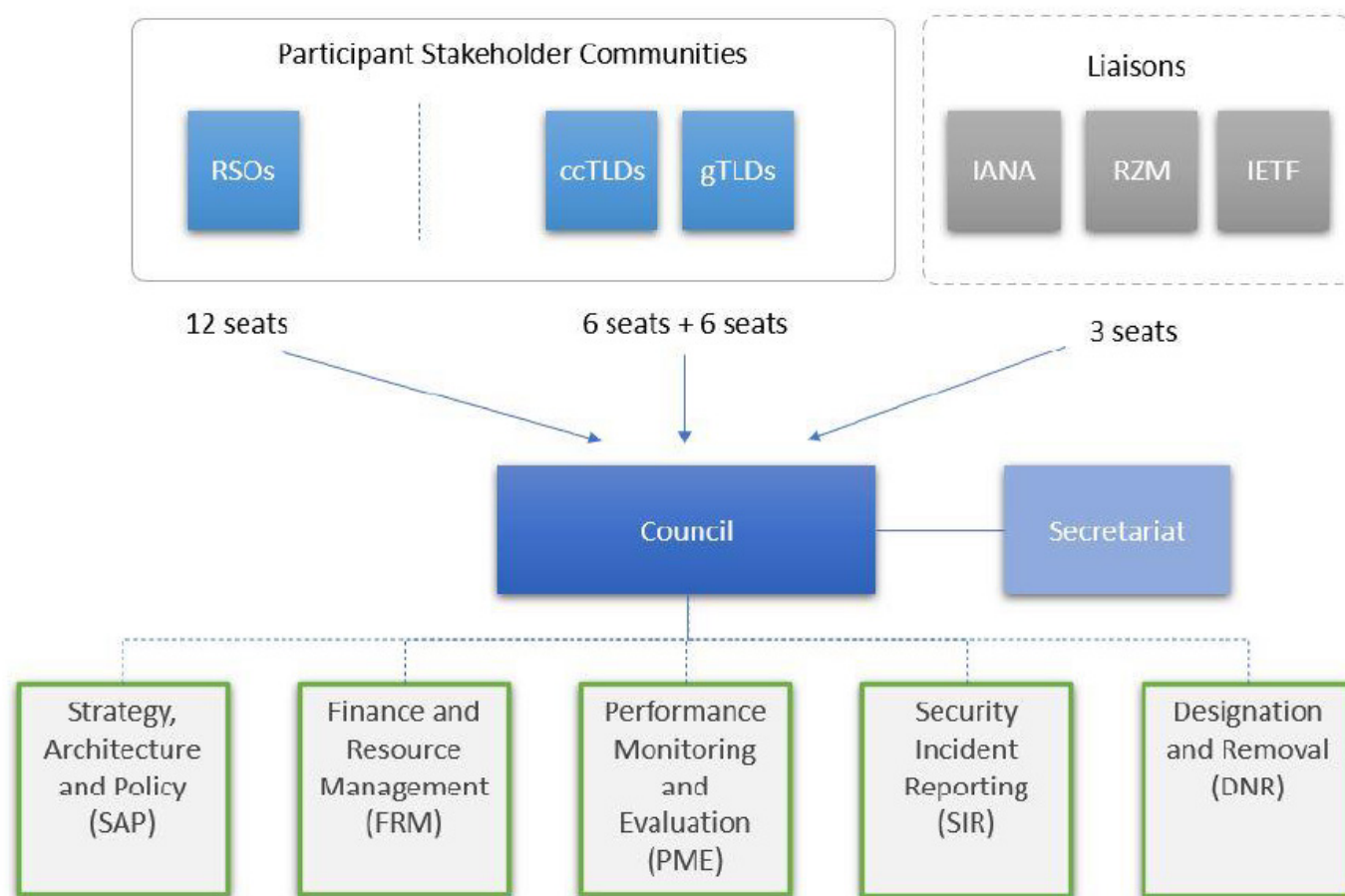


Рис. 2. Компоненты структуры управления системой КС. Источник: Functional Model for Root Server System Governance, <https://www.icann.org/en/public-comment/proceeding/functional-model-for-root-server-system-governance-11-08-2025>

- Разнородность индивидуальных корневых серверов и их операционные практики являются сильной стороной всей системы. Для системы КС стабильность важнее производительности. Если система состоит из однородных компонентов, подверженных общему дефекту, велик риск выхода из строя всех компонентов системы одновременно.
- Технические параметры работы протокола DNS определены IETF. Это означает, что корневые серверы поддерживают текущую версию протокола и не используют нестандартизованные расширения.
- ОКС должны быть нейтральными и беспристрастными. ОКС нейтральны к политике географических регионов и государств при предоставлении услуг корневого DNS. Это, например, означает, что недопустима блокировка запросов на основе местоположения клиента.

Эти принципы призваны обеспечить полную нейтральность ОКС в отношении данных, которые они публикуют. Это не простая прокламация. В прошлом были случаи, когда операторы предотвращали или задерживали загрузку ошибочных данных корневой зоны из IANA/Verisign. Хотя это было обусловлено техническими мерами безопасности, а не политическими соображениями, особенно в начале своего становления существовал определённый идеализм, представляющий ОКС защитной силой против возможного произвола правительства США или технических ошибок IANA.

Эти принципы являются граничными условиями предлагаемых изменений в ОКС. Предложенная функциональная модель [9] была разработана рабочей группой по управлению системой КС GWG на основе рекомендаций RSSAC [10].

В качестве основного управляющего органа системы управления проект предлагает создание Совета и поддерживающего его секретариата в рамках ICANN. Впоследствии Совет может стать независимой организацией или продолжать оставаться в лоне ICANN, правда, детали этих взаимоотношений и их трансформаций остаются за рамками проекта.

Предполагается, что Совет должен выполнять следующие функции, которые могут быть реализованы в виде процессов, постоянных комитетов, рабочих групп или назначенных лиц, как это определено Советом:

- Стратегия, архитектура и политика (SAP)
- Управление финансами и ресурсами (FRM)
- Мониторинг и оценка эффективности (PME)
- Отчетность об инцидентах безопасности (SIR)
- Назначение и удаление (DNR)

Хотя модель не предлагает конкретные ответы на такие вопросы, как кто и как может стать оператором КС или как можно создать новый КС, организационная структура призвана заложить основу процессам и функциям, которые в будущем смогут разработать и внедрить соответствующие правила.

Так, функция PMMF призвана обеспечить объективный мониторинг работы серверов. В случаях, когда результаты измерений показывают, что ОКС не соответствует установленным пороговым значениям, PMMF подготовит отчёт о неудовлетворительной работе ОКС. При выявлении документально подтверждённой тенденции неудовлетворительной работы SAPF может обратиться к DRF для принятия мер. DRF – это реактивный комитет, который реагирует на призыв SAPF к действию при необходимости назначения или отстранения оператора.

Если будет установлено, что ОКС не выполняет свои функции, SAPF должен связаться с соответствующим оператором. В ответ оператор должен предоставить подробный ответ, включающий план устранения проблем с указанием сроков их устранения. Неспособность устранить проблемы будет отражена в отчётах PMMF, и SAPF может при необходимости принять меры, поручив DRF исследовать вопрос. DRF представит Совету ICANN рекомендацию об отстранении настоящего и назначении нового ОКС.

- Также модель пытается применить разумные экономические принципы к развитию и финансированию системы КС. Эту проблему призвана решить функция управления финансами и ресурсами (FRM). Предполагается, что субъекты, для которых работа системы КС имеет критическое значение, должны взять на себя ответственность за финансирование этих услуг.

В этом проекте, для которого недавно закончился консультационный период, обсуждается также поэтапный подход к внедрению. Приведут ли описанные структуры и функции к решению указанных ранее проблем или система погрязнет в бюрократических процессах и комитетах – время покажет.

И в то же время, как отметил Джефф Хьюстон в своей статье «Управление корнем DNS» [11], сегодня, с повсеместным использованием CDN, возможно, стоит взглянуть на корневую зону не на как что-то священное, обслуживаемое таинственным клубом ОКС, а как на заурядный объект контента. Как заключает в своей статье Джефф, возможно, «... продолжение существующих соглашений с операторами корневых сервисов не является для нас единственным доступным вариантом. Более того, неясно, представляют ли дальнейшие инвестиции в организационную структуру, связанную с этими устаревшими соглашениями, наилучшее возможное использование нашего времени и ресурсов, особенно если целью является повышение устойчивости и производительности корневой системы DNS».

Заключение

Предлагаемые изменения предполагают формализацию процессов управления обеих систем. Это призвано сделать процесс принятия решений более предсказуемым, прозрачным и открытым для участия заинтересованных сторон. И следовательно – более надёжным и заслуживающим доверия, не в последнюю очередь среди национальных правительств.

С другой стороны, можно заметить, что представленные проекты не предполагают существенной реформы в этих

областях. Корневая зона по-прежнему публикуется через систему корневых серверов, обслуживаемых ограниченным числом операторов. Распределение номерных ресурсов производится в соответствии с политиками, разработанными сообществом, между членами ассоциации региональной интернет-регистратуры, по существу являющейся естественной монополией.

Возможно, в будущем будут предложены более радикальные изменения. Например, публикация корневой зоны в CDN или автоматизация распределительной функции РИР с помощью блокчейн со смарт-контрактами. Время покажет. Пока же системы, скорее всего, будут развиваться эволюционным путём. ■

Список литературы:

- [1] RFC 1174 “IAB Recommended Policy on Distributing Internet Identifier Assignment and IAB Recommended Policy Change to Internet «Connected» Status” — <https://www.rfc-editor.org/rfc/rfc1174>
- [2] ICP-2: Criteria for Establishment of New Regional Internet Registries — <https://www.icann.org/resources/pages/new-rirs-criteria-2012-02-25-en>
- [3] AFRINIC Litigation related Frequently Asked Questions (FAQs) — <https://afrinic.net/litigation-faq>
- [4] NRO Memorandum of Understanding — <https://www.nro.net/nro-memorandum-of-understanding/>
- [5] Address Supporting Organization (ASO) Memorandum of Understanding — <https://aso.icann.org/wp-content/uploads/2019/11/ASO-MoU-Executed-Nov-7-2019.pdf>
- [6] С началом внедрения технологии аникаст в 2003 году количество фактических узлов корневых серверов значительно выросло. На сегодня корневую зону обслуживают 1988 узлов. По существу, «буква» связана с организацией-оператором и, что более важно, IP-адресом сервера.
- [7] Root Name Server Operational Requirements. RFC2870 — <https://www.rfc-editor.org/rfc/rfc2870.html>
- [8] RSSAC055: Principles Guiding the Operation of the Public Root Server System — <https://itp.cdn.icann.org/en/files/root-server-system-advisory-committee-rssac-publications/rssac-055-07jul21-en.pdf>
- [9] Functional Model for Root Server System Governance — <https://www.icann.org/en/public-comment/proceeding/functional-model-for-root-server-system-governance-11-08-2025>
- [10] RSSAC037 A Proposed Governance Model for the DNS Root Server System — <https://itp.cdn.icann.org/en/files/root-server-system-advisory-committee-rssac-publications/rssac-037-15jun18-en.pdf>
- [11] Geoff Huston. The Governance of the Root of the DNS — <https://www.potaroo.net/ispcol/2025-08/rssgwg.html>

Об авторе

Андрей Юров, ФРСТ «ИнДата»

Знаки уходящего телекома на чугуне

Алексей Кипчатов



Аннотация

Чугунные люки телеком-инфраструктуры на тротуарах под нашими ногами, с одной стороны, скрывают от глаз сложные кабельные переплетения, передающие всё то сонмище информации, которую способны генерировать и потреблять современные люди и серверы. А с другой стороны, отлитые в чугуне знаки открывают глаза на историю становления телекома. Старые люки времён компаний-пионеров телефонии встречаются всё реже: они стираются ногами, ломаются под колёсами, уходят в музеи или частные коллекции, а чаще сдаются в металлолом и заменяются на новые. В заметке приведены фотографии люков телефонных компаний начала прошлого века с попыткой сохранить для истории и наметить наследственную структуру эволюции символов раннего телекома во времени и по географии.

Ключевые слова:

история телефонии, символы связи, эмблемы компаний, кабельная канализация, крышки люков.

Техническая база канализирования линий связи

Сначала был телеграф. Он обеспечивал связь между телеграфными аппаратами с помощью последовательной передачи, по сути дела, бинарной информации путём смены полюсов тока на линиях. Медленная передача телеграфного сигнала помещалась в узкую частотную полосу междугородних и международных телеграфных линий. Большое количество сообщений выстраивались в очередь на телеграфных станциях, чтобы быть переданными в нужном направлении. Электрические сигналы ходили между станциями, и до конечных абонентов они доставлялись в виде бумажных депеш. Таким образом, одна телеграфная линия за счёт мультиплексирования отправок по времени передавала достаточно много сообщений на большие расстояния. А за счёт того, что телеграфисты принимали

сообщения, записывали их и потом передавали на следующий узел, осуществлялась регенерация сигнала, и телеграмма могла быть доставлена за двое суток в любую точку мира, где был телеграфный узел. Количество телеграфных линий на узлах связи до поры до времени было счётным и ненамного превышало количество межузловых связей. И шли они на подвесе на столбах.

Потом появился телефон. По сравнению с телеграфным сигналом телефонный был широкополосным. Расстояние возможной связи резко сократилось до десятков километров. Возросли требования к качеству самих линий. Но самое важное в продвижении телефонии состояло в том, что телефонные аппараты находились у абонентов и с помощью индивидуальных проводов протягивались до телефонной станции. Для установления связи оператор собирал (коммутировал) канал связи абонент_А — станция_1 — ... — станция_п — абонент_В. А после разговора



Рис. 1. «Великая метель» в Нью-Йорке, 1888 г. Многие воздушные провода оборвались, представляя опасность для жителей города.

этот канал раскоммутировался, и линии освобождались для других абонентов/звонков. Так как количество абонентов и количество одновременно ведущихся разговоров росло неуклонно, то и количество проводов, подходящих к телефонным станциям, начало расти катастрофически.

Телеграфные и телефонные линии на заре их становления были однопроводными. Цепь замыкалась через заземление аппаратов в местах их установки. Телеграфные/телефонные линии шли по воздуху, подвешенные на столбах. Или в кабелях по дну водоёмов. Уплотнять провода связи, складывая их в многопроводные кабели, не получалось из-за взаимоиндукции. И хотя основополагающий труд Джеймса Максвелла «Трактат об электричестве и магнетизме», связывающий в единую теорию электричество и магнетизм, был написан в 1873 году, ещё до изобретения телефона, но он был не понят и был плохо принят в течение почти 15 лет даже учёными. Развитие обеспечивали энтузиасты, изобретатели и предприниматели, и шло оно скорее перебором вариантов технической реализации и их экспериментальной проверки на «живых» сетях и абонентах, чем за счёт расчётов на основе теоретических знаний законов электромагнетизма.

Опытным путём было обнаружено, что двухпроводная линия существенно лучше противостоит помехам как от атмосферного электричества и силовых электрических устройств, так и от взаимоиндукции линий связи, порождающей перекрёстные помехи. В 1881 году изобретатель телефона Александр Белл (Alexander Graham Bell) патентует телефонную цепь, состоящую

из двух изолированных проводов: «Провода, образующие металлическую цепь, покрываются (один или оба) изоляционным материалом и после соединения встраиваются в изоляционный материал или окружаются им» (Pat. 244,426 July 19, 1881). Идея была проста — на рядом расположенные прямой и обратный провод индуцируются одинаковые наводки, которые взаимоуничтожаются за счёт разнонаправленности токов в двухпроводной линии. Двухпроводная линия обеспечивала возможность перемещения телефонных линий со столбов под землю. Но по сравнению с воздушными линиями это было дорогое и сложное решение. Поэтому городская телефония на раннем этапе проникновения телефонии строилась, как правило, по однопроводным схемам, междугородная — по двухпроводной схеме. Разные подходы затрудняли техническое взаимодействие телефонных сетей или делали его невозможным, если они развивались разными операторами по-разному. И до начала XX века местные телефоны и телефоны дальней связи физически были разными аппаратами.

Конкуренция и монополия в развитии электросвязи

В 1876 году Александр Белл запатентовал телефон. Годом позже, в 1877-м, в Бостоне была основана Bell Telephone Company, которая уже в 1878-м проложила первую телефонную линию в Нью-Хейвене, штат Коннектикут, и начала активно продвигать телефон как коммерческую услугу.

История Bell Telephone Company в значительной степени связана с приобретением патентов и акций, а также слияниями и поглощениями, направленными на максимизацию прибыли от патентной защиты. За пределами США компания действовала через International Bell Telephone Company (IBTC), основанную в 1882 году в Антверпене, Бельгия. IBTC занималась производством оборудования для телефонии в Европе, поставляла его государственным и частным телефонным компаниям или участвовала в развитии европейских сетей с помощью капитала и технологий.



Рис. 2. Телефонная станция в Стокгольме, 1890 г.

При строительстве телеграфных сетей и их интеграции европейские страны не всегда охотно принимали американский капитал и патентную систему США, предпочитая развивать собственные телефонные сети. Когда американские компании пытались повторить свои успехи в Европе, они столкнулись с неожиданными препятствиями. В системах передачи и распространения информации на первое место ставились государственные интересы, а интересы коммерческого мира и частных лиц отходили на второй и третий план [1]. Великобритания, Германия, Франция, Австрия, Венгрия, Болгария и Швейцария не поддерживали иностранное участие в своих телефонных компаниях и развивали их как государственные предприятия. В России, Дании, Швеции, Норвегии, Нидерландах и Италии частично допускалось участие иностранного капитала под контролем правительств.

Шведский бум развития телефонии

Швеция в конце XIX века стала лидером в развитии телефонной связи. На местном рынке появились три ключевых игрока: Stockholm Bell Telefonaktiebolag, дочерняя компания International Bell Telephone Company; государственная телеграфная корпорация Kongl. Telegrafverket, она же Televerket под брендом Rikstelefon; и частная компания Stockholms Allmänna Telefonaktiebolag (SAT).

Создатель Allmänna Хенрик Седергрен (Henrik Thore Cedergrén) сначала занимался поставками и поддержкой белловского оборудования в Швецию. Ремонтировал он его в мастерских Ларса Эрикссона (Lars Magnus Ericsson), который к тому моменту вернулся в Стокгольм после двух лет работы в Германии в конструкторском бюро Сименса. Высокие цены, заданные Bell Telefonaktiebolag, спровоцировали Седергрена организовать свою телефонную компанию с бизнес-идеей «телефон в каждом доме Стокгольма, низкие тарифы, накопление прибыли компании и низкие дивиденды по акциям». В 1883 году, через три года после прихода Белла в Стокгольм, SAT начал включать первых телефонных абонентов, и он работал в тесном партнёрстве с быстрорастущим шведским производителем телефонного оборудования Aktiebolaget LM Ericsson & Co со своими патентами. Белловское предприятие, везущее свое дорогое оборудование из-за рубежа и сохранявшее высокие цены, начало проигрывать конкуренцию и в 1888 году было выкуплено государственным Televerket. В конкурентной борьбе за шведский телефонный рынок остались два игрока — Rikstelefon и Stockholms Allmänna Telefonaktiebolag.

Характерно, что шведское правительство не накладывало условия на отчисления с частного телефонного бизнеса государству. Это, а может быть, везение, что телефонный бизнес и «импортозамещение» белловских трубок в Швеции развивали талантливые инженеры, предприниматели и государственные чиновники, а может то, что Швеция оставила за государственными телеграфистами монополию на междугороднюю и международную связь и до поры до времени не мешала Седергрену и Эрикссону развивать местную телефонию, обеспечили Швеции в конце XIX века самый высокий среди европейских

государств темп телефонизации и самые низкие цены на телефонную связь.

Потом, в первые два десятилетия XX века, конкуренция затормозит развитие шведской телефонии, и начнётся телефонная война, да такая, что станет невозможно совершать звонки между сетями. Эта жёсткая конкуренция наблюдалась в период с 1903 по 1918 год и завершилась тем, что частная SAT была поглощена государственным Televerket, и Швеция перешла на модель функциональной телефонной монополии. В этот период оказалось, что германская и британская модели государственного монопольного развития телефонии или американская модель, где реализовалась коммерческая телефонная монополия, позволили обогнать и уйти в далёкий отрыв по проникновению телефонов и развитию телефонной индустрии.

Но это будет позже, а пока, в конце XIX века, был шведский телефонный триумф, и его инженерные и организационные разработки стали образцом развития и начали распространяться за границы Швеции по Европе и за её пределами. Вместе со шведскими телефонами проникала графическая символика шведских компаний, оставляя свои знаки на зданиях, оборудовании, люках кабельной канализации.

Знаки пионерской телефонии

В конце XIX века понятия бренд и брендовая идентичность как некий неизменный графический корпоративный стиль ещё не родились. Нормальным было изображать факсимиле или клейма так, как рука художника возьмёт при очередном его исполнении. Поэтому на артефактах вековой и более давности так разнятся начертания и изображения текстовых и графических символов, так много наблюдается вариаций и импровизаций в рекламных плакатах, буклетах или на упаковках массовых товаров. Принципы и ценности индустриального дизайна сформируются лишь к середине XX века.

Соответственно, и у телеграфных/телефонных компаний того времени графические образы их идентичности только появлялись. Историки бренда Telecom Italia пишут: «В то время у компании не было настоящего логотипа, задуманного как точный и неизменный знак; официальное название часто сопровождалось символическими элементами, такими как символ электрического тока, в соответствии со вкусом того времени» [2].

1. Символы электрического тока — ломаные стрелы

Конец XIX века и начало XX — это бум промышленного развития, механизации и электрификации производства, проникновение электричества во все сферы жизни, что коренным образом меняло экономику, общество, культуру и темп человеческой деятельности. Этот период стал эпохой Второй промышленной революции, которая стёрла привычные границы пространства и времени. И одним из повторяемых общеупотребимых знаков того времени стал пучок искр или молний, которым изображали электрические явления или помечали электрические

объекты. Ломаные стрелы, разлетающиеся от звезды с короной, были логотипом национального телеграфного оператора Швеции Televerket, и они же стали символом его телефонного подразделения. У норвежского оператора связи была четырёхконечная звезда с шестью разлетающимися вправо и влево стрелами. У белловского производителя телефонов Western Electric символом была скульптура Духа Телекоммуникаций с пучком молний в руке, которая исходно называлась «Гений Электричества» [3].



Рис. 3. Эмблема Western Electric.

Ломаные пересекающиеся стрелы стали эмблемой Российского Главного управления почт и телеграфов (ГУПТ) с 1884 по 1917 год, и они же вернулись на эмблему современного Минцифры. Ломаные пересекающиеся стрелы были эмблемой телеграфных войск, позже искровых рот и всех войск связи Российской империи и СССР. Инженерные войска, которые обеспечивали строительство и функционирование армейских сооружений связи, своей также эмблемой имели скрещённые лопаты с молниями.



Рис. 4. Ломаные стрелы на эмблемах российских ведомств и войск.

Вторым по значимости знаком принадлежности к развивающейся телефонной отрасли были изображения телефонных трубок. В конце XIX века эти трубки были в стиле белловских butterstamp.

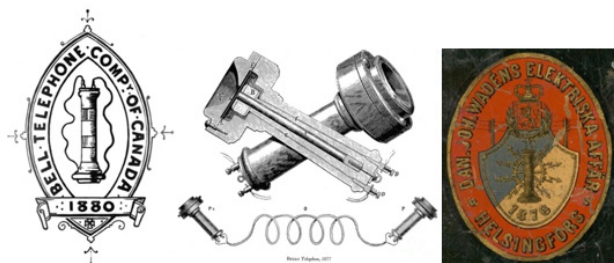


Рис. 5. Телефонные трубки на эмблемах компаний связи в конце XIX — начале XX века.

2. Символика шведских фирм

Два шведских предприятия (Allmänna Telefonaktiebolag и Rikstelefon), породившие шведский телефонный бум и ставшие примером развития телефонных сетей для ряда европейских государств, распространили по миру и свою символику.

У Allmänna Telefonaktiebolag в центре изображена телефонная трубка, и стрелы, исходящие из неё, означают не электрические искры, а звук. Этот знак вписывается в звезду с 12-ю лучами, отрисованными расходящимися от центра штрихами.

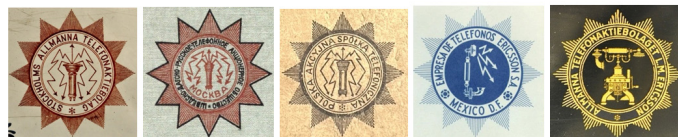


Рис. 6. Графические образы Allmänna.

Основной знак Rikstelefon — пятиконечная звезда с короной над ней и пучки искр, расходящиеся от неё влево и вправо, по четыре в каждом. Иногда звезда заменялась скрещёнными телефонными трубками Белла.



Рис. 7. Эмблемы Rikstelefon.

Появление телефона в Российской империи

27 февраля 1881 года было принято положение «Об устройстве городских телефонных сообщений», которое вводило разрешительный характер для строительства телефонных сообщений по проектам, которые утверждал Телеграфный департамент МВД Российской империи [4]. Также накладывались технические, надзорные, финансовые, тарифные и другие условия, а также 10% отчисления от сборов в доход казны. И в 1882 году начали работать российские телефонные сети в Санкт-Петербурге, Москве, Варшаве, Одессе и Риге, а право оказывать монопольные телефонные услуги в крупных городах Российской империи получила International Bell Telephone Company, выкупившая его у купца I гильдии В.О. фон Баранова, первым подсуетившегося в заключении контракта с Министерством внутренних дел. Включив сотню-другую абонентов, дальнейшую телефонизацию ИВТС проводила не спеша и больше торговалась за снижение отчислений в казну и инвестиции Российской империи в своё дальнейшее развитие.

К 1886 году общее число абонентов у Белла росло не так быстро, и их общее число по всем городам приближалось к трём тысячам. В следующих пяти городах — Нижнем Новгороде, Ро-

стове-на-Дону, Ревеле, Либаве и Баку, — запланированных для ввода телефонной связи Главным управлением почт и телеграфов, контракты на устройство телефонных сообщений выиграли местные предприниматели.

Чуть ранее, в 1884 году, в качестве эксперимента МВД начало строить телефонную сеть в Киеве за счёт казны Российской империи. Если этот подход окажется выгодным для казны, то опыт предполагалось тиражировать на всю империю. До завершения эксперимента продолжение заключения контрактов с частными предпринимателями приостановили. В 1891 году, через пять лет с начала реализации киевского эксперимента, он окупился и начал приносить прибыль. На тот момент в Киеве было 400 абонентов. Расходы казны не пропали даром, киевская телефонная сеть начала развиваться, и какое-то время спустя кабельные линии начали пропускать через кабельную канализацию.

«Правительственный телефон»

На нескольких сохранившихся крышках люков виден оттиск того времени. Есть в Киеве крышки люков с надписью «Прав. Телефонъ» и изображением скрещённых белловских трубок со разлетающимися снопами искр.



Рис. 8. Прав. Телефон, Киев.

Точно такие же белловские трубки с такой же ориентацией амбушюрами вниз, с искрами, короной и с надписью Rikstelefon изображены на точно таких же квадратных люках в Стокгольме. «Rikstelefon» дословно переведено на русский на киевских люках.



Рис. 9. Rikstelefon, Стокгольм.

Интересное: Riks — не самостоятельное шведское слово, но с него начинаются слова, обозначающие «национальный», «пра-

вительственный». Аналогично — датский национальный оператор исходно назывался Rigstelefonen (Правительственные телефоны), позже переименованный в Statstelefonen (Государственные телефоны). Слово Allmänna, наоборот, означает «общественный», «общий».

Почему, как и когда точно символика Rikstelefon попала в Киев — вопрос.

Люки телефонной канализации со словами «Правительственный» обнаруживаются в Самаре. В Самаре графика на люках оригинальная, она не является калькой с люков шведского государственного оператора Kongl. Telegrafverket.

Самарская правительственная телефонная сеть — 1915, Самара. Второе изображение — реконструкция для более наглядного выделения скрещённых трубок и видеоизменённых стрел с герба ГУПТ. Таких люков в Самаре до недавнего времени было несколько [5].



Рис. 10. Люки телефонной канализации в Самаре.

В Саратове есть затёртые люки с надписями «Правительственный телефонъ — Саратовъ», ориентировочно 1914 год [6].



Рис. 11. Люк телефонной канализации в Саратове.

Что было изображено на саратовской крышке правительственного телефона — стёрлось под ногами, и найти информацию пока так и не удалось.

Правительственные телефоны с символикой, восходящей к Rikstelefon, то есть с белловскими трубками амбушюрами вниз и характерными пучками искр, можно обнаружить в северной Италии. Первый люк — Telefoni dello stato — Государственный телефон. Фото — А. Газизов, 2025. Второй люк с такими же трубками — Societa Telefonica alta Italia — Телефонная компания северной Италии. Откуда и почему на этих люках знак Rikstelefon? В итальянском анализе эволюции брендов Telecom Italia [2] этих трубок с пучком молний не представлено. Но люки эту символику хранят до наших дней.



Рис. 12. Итальянские люки телефонной канализации.

Загадки проникновения символов шведского «Рикстелефон» видны и на следующей серии люков, которые относятся к середине XX века. Более распространённый символ Rikstelefon — это не скрещённые трубки Белла, а звезда с большой короной и разлетающиеся пучки молний. Эти знаки до сих пор есть в Стокгольме на люках, телефонных будках и почтово-телеграфных офисах.



Рис. 13. Люк телефонной канализации в Стокгольме, середина XX века.

Точно такие же стрелы, но без короны есть на люках в Таллине с буквами РМЗ БВМС, которые означают не функциональную принадлежность люка, а его производителя — Ремонтно-механический завод Балтвоенморстроя. Это ориентировочно 1948 год или позже.



Рис. 14. Люк телефонной канализации в Таллине, конец 1940-х годов.

Следующий люк найден мной в Одессе с буквами ОС в ромбе и теми же самыми стрелами. ОС = «ОдессаСтрой»? И на этом люке хорошо видно, что стрелы внутри 16-лучевой звезды. Похожая звезда, но 12-лучевая, была на шведских люках другой телефонной компании — Allmänna Telefonaktiebolag.

И ещё один люк с точно такими же звездой и стрелами есть в Хабаровске, но он не с четырьмя стрелами, а с двумя, как

у советских инженерных войск. И с буквами в ромбе МС — «Министерство Связи»?



Рис. 15. Люк телефонной канализации в Одессе.



Рис. 16. Люк телефонной канализации в Хабаровске.

Мы далеко ушли вперёд по времени и разлетелись по географии от Милана до Хабаровска, следуя за знаками «Рикстелефона». И это далеко не все из известных крышек люков с такой символикой, а лишь самые выразительные. Вернёмся в Российскую империю начала XX века.

Шведско-датско-русское телефонное акционерное общество

Исходя из успеха в Киеве, все дальнейшие шаги по развитию телефонных сетей в городах Российской империи производились ГУПТ за счёт государственного бюджета. Исключением были те первые десять городов, которые начали развиваться на негосударственные деньги, и одиннадцатый регион — Финляндия, где ранее была утверждена Александром III отдельная модель развития телефонии. Её успешно осуществлял механик Даниэль Йоханнес Ваден, в итоге эта модель стала «Сонерой» и уже в начале XXI века растворилась в шведской «Телии», новом имени государственного Televerket.

В России в 1901 году заканчивался срок действия белловской концессии. В это время стало понятно, что развитие телефонных сетей оказалось жёстко связано с размером государственных инвестиций и постепенно начинало тормозиться, а абонентская цена сохранялась предельно высокой. Поэтому частные инвестиции в телефонные сети решено было оставить, а условием заключения нового контракта ГУПТ объявил снижение абонентской платы.

Победителем нового конкурса стало Шведско-датско-русское телефонное акционерное общество, ключевым владельцем которого был владелец шведской части Хенрик Седергрэн, носитель идеи снижения абонентской платы. Он подписывался под годовой абонплатой в 86 рублей вместо 250 рублей от Белла. К тому времени компания Ларса Эрикссона, партнёра Седергрэна и ведущего мирового производителя телефонного оборудования, на протяжении ряда лет поставляла оборудование и вела монтаж телефонных станций по городам Российской империи. В Петербурге в 1900 был запущен большой телефонный завод Русского акционерного общества «Л.М. Эриксон и К°». Это обеспечивало новому победителю существенную экономическую прочность на закупках оборудования.

Шведско-датско-русское телефонное акционерное общество подошло к проекту с грандиозными планами. В Москве начал строиться телефонный узел на 60 тысяч абонентов. Естественно, что телефонные линии к такому большому узлу сразу закладывали в подземной канализации. А на люках этой канализации изображалась эриксоновская телефонная трубка с ломаными стрелами, изображающими звук трубки внутри 12-лучевой звезды. И этот образ лёг в основу многих люков связи, выпущенных в XX веке в СССР.



Рис. 17. основополагающие люки телефонной канализации — Москва, 1901-1917.

Все дореволюционные телефонные люки Москвы в настоящее время утрачены, живьем их можно увидеть лишь перед Музеем истории телефона (г. Москва, Садовая-Кудринская улица, дом 19-2), где они находились, можно узнать в публикациях энтузиастов [7].



Рис. 18. Люки телефонной канализации в Екатеринбурге (фотографии 2012 года, современная судьба люков неизвестна).

Сравните: ниже — оригинальные люки Allmänna Telefonaktiebolag.



Рис. 19. Оригинальные люки Allmänna Telefonaktiebolag.

Первый люк найден в старом городе в Стокгольме, второй — в Риге, где он явно выставлен напоказ и был размещён на тротуаре прямо на входе в собор Святого Петра, поэтому быстро стирается ногами туристов. Как и почему он попал в Ригу в неизменном виде — вопрос.

Ниже приведены фотографии линейки люков со звучащей трубкой Allmänna Telefonaktiebolag и Шведско-датско-русского телефонного акционерного общества, отлитых после 1917 года.

Рис. 20. Люк телефонной канализации — Варшава, PAST (Polska Akcyjna Spółka Telefoniczna) [8], фото люка заимствовано из википедии [С].

Рис. 21. Люк телефонной канализации — НКПТ (Народный комиссариат почт и телеграфа, Наркомпочтель — 1923-1932), Москва.

Рис. 22. Люк телефонной канализации — 1928, Екатеринбург.

Рис. 23. Люк телефонной канализации — кабель, Санкт-Петербург.

Рис. 24. Люк телефонной канализации — НКПТ, Харьков.

Рис. 25. Люк телефонной канализации — НКС (Народный комиссариат связи, 1932-1946), Одесса.

Рис. 26. Люк телефонной канализации — МС (Министерство Связи, 1946-1991), Таллин.

Рис. 27. Люк телефонной канализации в Киеве.

Рис. 28. Люки без звучащей телефонной трубки Эрикссона, но в узнаваемой 12-конечной звезде TELVE — Telephone Company of the Veneto, подразделение Telecom Italia, фото заимствовано из Википедии [С].

Рис. 29. STIPEL — Inter-regional Telephone Company of Piedmont and Lombardy, подразделение Telecom Italia, фото заимствовано из Википедии [С].

Заключение

Есть ещё много разновидностей люков с элементами знаков пионерской телефонии — ломаными стрелами, телефонными трубками, 12-конечными звёздами, часто изображаемыми с существенными отклонениями от исходных образов, вплоть до неузнаваемости. Их можно находить, осмысливать, систематизировать и делать какие-то выводы. Вероятно, остались ещё



Рис. 20.



Рис. 21.



Рис. 22.



Рис. 23.



Рис. 24.



Рис. 25.



Рис. 26.



Рис. 27.



Рис. 28.



Рис. 29.

люки начала века с символикой «Правительственный телефон» в других городах и странах. А может, они уже утрачены, и никогда мы не узнаем, что они существовали. Поэтому те немногие энтузиасты, которые фотографируют, систематизируют и публикуют изображения старых крышек люков на сайтах и блогах, сохраняют знаки и образы нашего совсем недалёкого прошлого и укрепляют то основание, на котором мы все с вами стоим [5-11].

Сила образов, отлитых в чугуне, состоит в том, что они общедоступны. Поэтому часто изображения люков становятся иллюстрациями к историческим статьям и историческим символам. Телеком-отрасли в этом повезло больше других. У нас есть красивые люки, образы на которых хранятся долго и дают зацепки для осознания истоков.

Эта статья — попытка сохранить знаки зарождения отрасли для будущего, ведь бумага надёжнее чугуна на тротуарах и долговечнее всего цифрового мира, который может быть выключен «щелчком тумблера» или переписан и растражирован в ином смысле с помощью ИИ — по глупости, заблуждению или злонамеренно, чтобы предать забвению наше прошлое. ■

Список литературы:

- [1] Kingsbury, John E. The Telephone And Telephone Exchanges: Their Invention And Development, Longmans, Green, and Co., New York/ London, 1915. <https://archive.org/details/telephonetelephookingrich/>
- [2] Логотипы Telecom Italia и их изменение с течением времени. <https://www.museodelmarchioitaliano.it/en/tim-2/>
- [3] Spirit of Communication. https://en.wikipedia.org/wiki/Spirit_of_Communication
- [4] Высоков М.С. История электросвязи российской империи. — Москва, Изд. Ретн, 2010.
- [5] История электросвязи в Самаре. Музей Ростелекома. <https://sv-bob.livejournal.com/409237.html>

- [6] Что можно увидеть, разглядывая под ногами крышки телефонных люков. <http://www.control-point.ru/rossiya/lyuk-telefonnyj-gts/>
- [7] Канализационный люк «Шведско-датско-русское телефонное акционерное общество». <https://leonovvaleri.livejournal.com/69221.html>
- [8] Historia logo Ericsson na warszawskich studzienkach telefonicznych. <https://www.signs.pl/historia-logo-ericsson-na-warszawskich-studzienkach-telefonicznych,401159,artykul.html>
- [9] Крышки люков — История люков телефонной сети в Москве и Московской области. <https://logoworks.narod.ru/city/wells-tel.html>
- [10] География под ногами. Ч.7. Все дороги ведут в Саратов. <https://sarlynx.livejournal.com/54115.html>
- [11] Крышки колодцев связи «Телефон» со стрелами. <https://v-kleshev.livejournal.com/55876.html>
- [C] фото из «Википедии»:

провода над Нью-Йорком, 1988 год. https://commons.wikimedia.org/wiki/File:Blizzard_1888_01.jpg

провода телефонной башни Telefontornet над коммутатором, Стокгольм. <https://www.flickr.com/photos/tekniskamuseet/6838150900/in/album-72157629589461917>

крышка люка PAST. https://pl.m.wikipedia.org/wiki/Plik:Studzienka_PAST_Warszawa.jpg

крышка люка TELVE. https://en.wikipedia.org/wiki/File:Telve_Chiusino_Udine_20120414.JPG

крышка люка STIPEL. https://commons.wikimedia.org/wiki/File:Stipel_chiusino_Milanino_20110511.jpg

Об авторе

Кипчатов Алексей Александрович, к.ф.-м.н.,
руководитель направления, компания «ТрансТелеКом», Москва.

Новости науки и техники

Компания Salesforce заявила, что не будет вести переговоры с киберпреступниками

Компания Salesforce публично объявила о том, что не намерена ни вступать в переговоры, ни тем более выплачивать выкуп киберпреступникам, стоящим за взломом её систем, который породил волну едва ли не самых громких кибератак нынешнего года. Salesforce является мировым лидером рынка систем управления взаимоотношениями с клиентами (CRM-системы), её разработками пользуются десятки крупнейших компаний и известнейших брендов мира.

Атаки были организованы хакерской группировкой Scattered Lapsus\$ Hunters и развивались двумя волнами. Первая началась ещё в конце 2024 года, когда злоумышленники, используя методы социальной инженерии и выдавая себя за сотрудников службы IT-поддержки, убеждали сотрудников подключить вредоносное приложение OAuth к системам Salesforce своей компании. После подключения хакеры использовали соединение для загрузки и похищения баз данных. Вторая волна атак стартовала в начале августа 2025 года, когда злоумышленники использовали украденные токены OAuth SalesLoft Drift для доступа к CRM-средам клиентов и извлечения данных.

В результате жертвами стали 39 компаний и брендов, включая FedEx, Disney/Hulu, Home Depot, Marriott, Google, Cisco, Toyota, Gap, Kering, McDonald's, Walgreens, Instacart, Cartier, Adidas, Saks Fifth Avenue, Air France, KLM, Transunion, HBO MAX, UPS, Chanel и IKEA. Киберпреступники объявили о похищении в общей сложности почти одного миллиарда записей данных. Они потребовали выкуп от каждой из пострадавших компаний, а также предложили Salesforce одним платежом «рассчитаться» за всех своих клиентов, угрожая в противном случае выложить похищенные данные в открытый доступ 10 октября.

Ответом на эти угрозы и стало заявление Salesforce об отказе от какого-либо сотрудничества с вымогателями. При этом компания разослала своим клиентам уведомления о том, что угрозы публикации похищенных данных со стороны Scattered Lapsus\$ Hunters являются, судя по всему, вполне реальными. Хакеры, со своей стороны, уже создали сайт для публикации утечек, разместив его на домене breakforums.hn — очевидно, «в честь» печально известного хакерского форума BreachForums, славившегося продажей и публикацией утечек похищенных данных.

Однако буквально накануне срока публикации ФБР США совместно с правоохранительными органами Франции провели масштабную операцию по блокировке инфраструктуры

и конфискации всех доменов BreachForums. В результате посетителей сайта breakforums.hn встречает лишь уведомление о том, что домен конфискован ФБР. Представители хакерской группировки уже признали в сообщении в Telegram провал своих первоначальных планов. Они назвали блокировку доменов «неизбежной» и несколько высокопарно заявили о завершении эпохи интернет-форумов. Впрочем, они добавили, что не отказываются от своих намерений, и похищенные у Salesforce данные всё равно будут опубликованы.

Источник: Bleeping Computer

<https://www.bleepingcomputer.com/news/security/salesforce-refuses-to-pay-ransom-over-widespread-data-theft-attacks/>
<https://www.bleepingcomputer.com/news/security/fbi-takes-down-breachforums-portal-used-for-salesforce-extortion/>

Германия против тотального контроля

Власти Германии не поддержат законопроект Европейского Союза, обязывающий поставщиков услуг в сфере телекоммуникаций, таких как WhatsApp, Signal и других, отслеживать сообщения пользователей на предмет потенциального наличия материалов, содержащих сцены сексуального насилия над детьми (child sexual abuse — CSA). Этот проект, известный под названием Chat Control, предусматривает обязанность коммуникационных платформ использовать контент-фильтры на основе искусственного интеллекта для блокировки материалов CSA и привлечения к ответственности тех, кто хранит и распространяет их. При этом сервисы, использующие сквозное шифрование, не освобождаются от этой обязанности.

«Мы, фракция ХДС/ХСС, выступаем против необоснованного мониторинга чатов. Это было бы равносильно вскрытию всех писем в качестве меры предосторожности, чтобы проверить, нет ли в них чего-либо противозаконного. Это неприемлемо, и мы этого не допустим», — заявил в своём выступлении депутат Бундестага от Христианско-демократического союза (ХДС), входящего в правящую коалицию страны, Йенс Шпан (Jens Spahn).

Вокруг законопроекта Chat Control уже много месяцев не утихают ожесточённые дискуссии, и позиция Германии в этом вопросе исключительно важна. Для принятия законопроекта лидерам ЕС необходима поддержка правительств, представляющих большинство населения стран-членов блока. Ранее в поддержку проекта уже высказались Франция, Испания, Португалия и ряд других стран. Среди стран, пока не определившихся со своей позицией, крупнейшими являются Италия, Бельгия и Швеция. А наиболее крупными противниками Chat Control до недавнего времени выступали Польша и Нидерланды. И присоединение к этому лагерю Германии, где проживают 83,5 миллиона человек (примерно 19% от общей численности населения стран Европейского Союза) — аргумент более чем весомый.

В отличие от политиков, представители правозащитных организаций и технологических компаний практически единодушны в крайне негативной оценке законопроекта. Так, организация European Digital Rights (EDRi) убеждена, что предлагаемые для обязательного внедрения коммуника-

ционными платформами технологии неэффективны и ненадёжны. А ущерб от их возможного внедрения многократно перевешивает гипотетическую пользу. «Негативное влияние Chat Control на демократию будет беспрецедентным. Легализуя эти опасные практики, ЕС подаст сигнал остальному миру, что конфиденциальности цифровых коммуникаций быть не может», — заявляют её представители.

Не менее резко высказалась и президент Signal Мередит Уиттакер (Meredith Whittaker) в своём открытом письме, адресованном политическим деятелям Германии. «Под видом защиты детей последние предложения по контролю чатов потребуют массового сканирования всех сообщений, фотографий и видео на устройстве пользователя для определения того, является ли контент допустимым или нет. Это ужасающая идея по многим причинам. Во-первых, технический консенсус очевиден. Сканирование каждого сообщения — независимо от того, делается ли это до или после шифрования — сводит на нет саму идею сквозного шифрования. [...] Эта угроза настолько серьёзна, что даже разведывательные службы сходятся во мнении, что она обернётся катастрофой для национальной безопасности. Эти предложения игнорируют стратегическое значение частной переписки и давний технический консенсус относительно того, что невозможно создать бэкдор, доступный только «хорошим парням». По сути, они предлагают массовую слежку без ограничений, которая позволит раскрыть интимные и конфиденциальные сообщения всех, будь то правительственные чиновники, военные, журналисты-расследователи или активисты. Несмотря на все разговоры Европы о суверенитете, это абсурдное решение в области кибербезопасности по многим направлениям».

Уже 40 европейских компаний, выступающих в защиту конфиденциальности, направили схожее по своим тезисам коллективное письмо немецким властям. Они подчёркивают, что в случае принятия законопроекта будут вынуждены выйти из-под юрисдикции ЕС и покинуть европейские рынки.

Источник: TheRegister
https://www.theregister.com/2025/10/08/germany_chat_control_opposition/

Северокорейские хакеры с начала года похитили криптовалюту более чем на 2 миллиарда долларов

Компания Elliptic, специализирующаяся в области блокчейн-аналитики, сообщила о том, что по оценкам её экспертов, с начала года хакеры из Северной Кореи смогли похитить криптовалютные активы на сумму более 2 миллиардов долларов. Таким образом, установлен новый печальный рекорд: это достижение намного превосходит прежний зафиксированный максимум — 1,35 миллиарда долларов в 2022 году, и почти вдвое превышает результат прошлого года. А ведь 2025 год еще совсем не окончен.

Ситуация вдвойне тревожна, поскольку, по сведениям представителей ООН и правительственных экспертов ряда стран, хакерские группировки из КНДР действуют при полной



поддержке и по прямому указанию правительства страны, а похищенные средства направляются главным образом на развитие военных программ, в том числе на разработку и производство ядерного оружия. Исследователи Elliptic утверждают даже, что финансирование северокорейской власти находится всё в большей зависимости от похищенной хакерами криптовалюты.

Наибольший вклад в результат текущего года внесла февральская кибератака на криптовалютную биржу ByBit. Тогда северокорейским хакерам удалось похитить криптовалюту на сумму порядка 1,46 миллиарда долларов. Среди других инцидентов с участием киберпреступников из КНДР — атаки на сервисы LND.fi и Seedify и криптовалютные биржи WOO X и BitoPro. Всего же с начала года эксперты Elliptic смогли установить причастность северокорейских хакеров к 30 атакам, повлёкшим похищение криптовалютных активов. Причём сами эксперты называют свои оценки весьма консервативными, поскольку многие инциденты либо не получают огласки вовсе, либо сумма ущерба существенно занижается.

Говоря о тенденциях самих атак, специалисты Elliptic отмечают, что киберпреступники всё чаще атакуют не компании, а конкретных сотрудников компаний либо криптовалютных инвесторов, располагающих значительными средствами. Соответственно, атаки с использованием изощрённых методов социальной инженерии приходят на смену эксплуатации уязвимостей ПО сервисов децентрализованных финансов. Более сложными и изощрёнными становятся и способы отмывания похищенных средств. Тем не менее, в Elliptic уверены, что прозрачность блокчейн-систем всё же позволяет расследователям обнаруживать перемещение крупных сумм похищенной криптовалюты и существенно затрудняет жизнь киберпреступникам.

Источник: Bleeping Computer
<https://www.bleepingcomputer.com/news/cryptocurrency/north-korean-hackers-stole-over-2-billion-in-crypto-this-year/>

Новости доменной индустрии

Фишинг с большой дороги: мошенники массово создают поддельные сайты оплаты проезда

Специалисты компании F6 обнаружили разветвлённую инфраструктуру вредоносных доменов, выдающих себя за официальные сервисы оплаты транспортных услуг.

Так, одна из сетей, созданных злоумышленниками, включала 39 доменов, в том числе для оплаты проезда по Московскому скоростному диаметру, платным дорогам Санкт-Петербурга, Вознесенскому тракту в Казани и скоростным автодорогам России. Большинство из мошеннических сайтов появились в мае 2025 года.

Обнаруженные сайты визуально похожи на официальные ресурсы и свободно индексируются в поисковых системах. Один из вредоносных доменов, предлагающий оплатить проезд по Московскому скоростному диаметру, оказался даже на верхних строках поисковой выдачи.

Схема работает следующим образом: после ввода данных о личном автотранспорте — госномера автомобиля или номера транспортной карты — пользователю отображается «задолженность», которую требуется оплатить. Затем ресурс запрашивает платёжные данные — номер банковской карты, срок действия, CVV. Причём при вводе данных карты ресурс отправляет запрос на подтверждение с помощью SMS, повышая правдоподобие схемы. Опасность в том, что после ввода реквизитов банковской карты и суммы платежа деньги списываются, данные банковской карты также остаются в руках у мошенников и могут использоваться повторно.

Согласно данным УБК (Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий) МВД России, максимальный ущерб от подобного вида фишинга превысил 22 тысячи рублей.

Три года назад эксперты F6 уже находили аналогичную сеть из 36 фишинговых ресурсов, больше всего из них действовали под видом сайтов пополнения счёта петербургской транспортной карты «Подорожник». Причём, если жертвы неохотно оплачивали «проезд» по автодорогам, злоумышленники меняли на сайте «начинку» на оплату штрафов ГИБДД.

Источник: <https://www.f6.ru/media-center/press-releases/phishing-from-the-high-road/>



В центре внимания — кибербезопасность!

14-16 сентября 2025 года в Калининграде состоялась 18-я Международная конференция администраторов и регистраторов национальных доменов верхнего уровня стран СНГ, Центральной и Восточной Европы (TLDCON 2025), организованная Координационным центром доменов .RU/.РФ. Второй день деловой программы конференции был посвящён вопросам кибербезопасности. Участники рассказывали о применяемых практиках борьбы с киберугрозами и рассматривали возможность и необходимость разработки новых политик, призванных обеспечить нормативную базу снижения злоупотреблениями DNS.

Недавно институт Net Beason выпустил пакет рекомендаций, направленных на снижение количества злоупотреблений DNS. В частности, регистраторам рекомендуется проверять домены, связанные с регистрантом, если хотя бы один из зарегистрированных им доменов замечен в злоупотреблениях. Ольга Баскакова (Координационный центр доменов .RU/.РФ) отметила, что подобный механизм реализован и успешно работает с 2012 года в рамках проекта Координационного центра «Нетоскоп». В отличие от представленной рекомендации, проверки связности доменов занимаются доверенные эксперты, работающие в области кибербезопасности, включая НКЦКИ.

«С нашей точки зрения, это более оправданная схема, т.к. не все регистраторы могут осуществлять должную экспертизу по выявлению связи. Каждый должен заниматься своим делом: регистратор — регистрировать домены, эксперты — выявлять противоправную активность и бороться с ней», — подчеркнула Ольга.

Далее участники TLDCON 2025 обсудили современный ландшафт киберугроз, отметив существенный рост угроз, связанных с распространением вредоносного ПО и появлением новых группировок злоумышленников. При этом активное

распространение получает скам: домены со скамом блокируются значительно дольше, чем домены с фишингом — этим и пользуются злоумышленники. Станислав Гончаров (F6) сообщил, что в среднем на один бренд в 2025 году приходилось 2299 фишинговых ресурсов и 1238 доменов со скамом.

Итоги секции подвел Антон Воронкин (НКЦКИ). Он отметил, что каждому важно быть осведомлённым о текущей ситуации, и только обобщение информации, полученной от многих экспертов по кибербезопасности, может помочь принять адекватные меры. Хорошим помощником в этом он назвал проект КЦ «Доменный патруль». В заключение Антон призвал регистраторов, компетентные организации и владельцев информационных ресурсов к объединению усилий.

Источник: <https://cctld.ru/media/news/kc/38704/>

Названы общие домены верхнего уровня, чаще всего используемые организаторами фишинговых атак

Компания Interisle, исследующая вопросы кибербезопасности, опубликовала очередной выпуск своего ежегодного отчёта Phishing Landscape report. Он основывается на данных о фишинговых атаках от организаций Anti-Phishing Working Group (APWG), OpenPhish, PhishTank и Spamhaus и обобщает сведения примерно четырёх миллионов сообщений о фишинге за период с мая 2024 по апрель 2025 года.

Число доменных имён, ассоциированных с фишингом, выросло за это время на 38% по сравнению с тем же периодом годом ранее. Доля фишинговых имён в общих доменах .com/.net и национальных доменных зонах сократилась — с 37% до 32% и с 15% до 11% соответственно. А вот новые общие домены верхнего уровня демонстрируют крайне негативную динамику. Так, в 2021 году на их долю приходилось 9% всех зарегистрированных в мире доменных имён и 21% имён, ассоциированных с фишингом. С тех пор доля рынка новых доменов выросла всего лишь до 11%, а вот их доля в фишинге — до 51%.

И хотя в абсолютных цифрах лидером остаётся, разумеется, домен .com (455 297 жалоб на фишинг), объясняется это исключительно тем, что домен является абсолютным лидером рынка, многократно опережая всех конкурентов по количеству регистраций. Если же смотреть на соотношение общего числа зарегистрированных имён и числа имён, ассоциированных с фишингом, то картина получается совсем иная — и крайне печальная. В домене .xip, например, на момент подготовки отчёта были зарегистрированы 42 724 имени и 42 681 из них было упомянуто в жалобах на фишинг. Таким образом, уровень фишинга в доменной зоне является практически стопроцентным. Почти аналогичные показатели и в доменных зонах .bond, .cfd, .today и .lol.

Если говорить о компаниях-регистраторах, то максимальный процент фишинговых регистраций у NiceNic, Aceville,

Dominet, Webnic и OwnRegistrar. Ну а главной «приманкой» для организаторов фишинговых атак из года в год остаётся цена регистрации имени. Чем она ниже, тем выше вероятность, что домен будет зарегистрирован с неблагоприятными целями.

Источник: https://domainnamewire.com/wp-content/Interisle_Phishing-Landscape-2025.pdf

Новые домены показали выдающийся рост, но это вряд ли повод для радости

Начало лета 2025 года принесло значительный рост числа регистраций в некоторых новых общих доменах верхнего уровня. Лидерами по этому показателю стали домены .watch, .yachts, .autos, .irish, .boats и .qpon. Показатели роста в них колеблются в пределах от 50% до 73% по сравнению с данными файлов зон на конец мая. Казалось бы, стоит порадоваться достигнутому успеху, но в действительности поводов для радости не слишком много.

Бурный рост числа регистраций почти всегда связан с промо-акциями и снижением цен в доменной зоне. А этим практически всегда пользуются злоумышленники для автоматической массовой регистрации доменных имён. Хорошим примером может служить домен .autos, управляемый регистратурой .xyz. На протяжении июня стоимость годовой регистрации имени в нём не превышала двух долларов. За месяц число регистраций выросло более чем на 51 тысячу. Но достаточно беглого взгляда, чтобы убедиться: большинство этих регистраций составляют такие доменные имена, как yqtsfg.autos, rgwydp.autos или lxnnu7.autos, которые решительно невозможно ни запомнить, ни произнести. Аналогичная ситуация и в домене .yachts: как сообщает ресурс Domain Incite, из 33 620 зарегистрированных в нём в июне новых имён 27 335 имеют в своём составе произвольные наборы цифр.

Вполне очевидно, что ни одному человеку просто не придёт в голову регистрировать такие доменные имена. Но их и регистрируют не люди, а настроенные злоумышленниками алгоритмы. В дальнейшем такие «одноразовые» домены используются для фишинга, распространения спама, вредоносного ПО и других противоправных действий. Можно согласиться с тем, что иногда автоматическая массовая регистрация доменов осуществляется и с благими целями, например, исследовательскими. Но в подавляющем большинстве случаев цели всё же другие.

Не так давно представители Правительственного консультативного комитета настоятельно рекомендовали ICANN выработать меры, способные поставить заслон на пути массовых автоматических регистраций. И июньские итоги в очередной раз подтверждают, что такая необходимость действительно существует.

Источник: <https://cctld.ru/media/news/industry/38343/>

Интернет изнутри ➡

БЕСПЛАТНЫЙ ЭКЗЕМПЛЯР