Банк России

ОБЗОР ОСНОВНЫХ ТИПОВ КОМПЬЮТЕРНЫХ АТАК В ФИНАНСОВОЙ СФЕРЕ В 2024 ГОДУ

Москва
2025

ОГЛАВЛЕНИЕ

Обзор подготовлен Департаментом информационной безопасности.

Фото на обложке: Shutterstock/FOTODOM
107016, Москва, ул. Неглинная, 12, к. В
Официальный сайт Банка России: www.cbr.ru

ВВЕДЕНИЕ

Анализируя динамику компьютерных атак (КА)[1] 2023 г., можно с уверенностью сказать: в 2024 г. злоумышленники развивали и совершенствовали существующие тактики и техники атак. Среди ключевых направлений успешных КА – эксплуатация уязвимостей, атаки типа «отказ в обслуживании» (далее – DDoS), атаки через скомпрометированные информационные инфраструктуры (ИИ) подрядных организаций, компрометацию учетных записей (УЗ) из-за невнимательности и/или отсутствия контроля применения парольных политик на ИИ финансовых организаций.

У организаций финансовой сферы с ростом количества компьютерных инцидентов (КИ)[2], вызванных компрометацией подрядных организаций (атаки на цепочку поставки), появилась необходимость превентивного реагирования и на такие угрозы. Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России (ФинЦЕРТ) ведет активную работу по организации взаимодействия с разработчиками и интеграторами различных ИТ-решений и услуг, продукты которых активно используются финансовым сектором. На текущий момент информационное взаимодействие осуществляется более чем с 60 подобными компаниями, что позволяет комплексно повышать уровень информационной безопасности и осведомленности о компьютерных угрозах как поставщиков услуг, так и организаций финансовой сферы.

Регулярная оценка ландшафта угроз позволяет ФинЦЕРТ своевременно готовить информацию об уязвимостях и направлять ее участникам информационного обмена (УИО) для реагирования и принятия компенсирующих мер, ориентированных на сдерживание целевых КА.

За 2024 г. ФинЦЕРТ направил свыше 360 машиночитаемых бюллетеней с актуальными индикаторами КА, а также 38 оперативных бюллетеней с аналитической информацией о существующих компьютерных угрозах и рекомендациями по противодействию им.

Кроме того, актуальные векторы атак и процесс взаимодействия с ФинЦЕРТ были отработаны в рамках ежегодно проводимых киберучений, в которых участвовали более 290 организаций финансовой сферы.

Во время киберучений совместно с Федеральным государственным унитарным предприятием «Главный радиочастотный центр» были реализованы следующие мероприятия:
- проведено внешнее сканирование информационных ресурсов участников киберучений;
- отработан процесс оперативной передачи информации о выявленных угрозах;
- выполнена проверка готовности кредитных организаций к оперативному приостановлению обмена электронными сообщениями в платежной системе Банка России при выявлении инцидентов защиты информации (ЗИ), при осуществлении переводов денежных средств на объектах ИИ участника информационного обмена, которые привели или могут привести к осуществлению перевода денежных средств без согласия УИО.

---

[1] Компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

[2] Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедшей в результате компьютерной атаки.

В рамках развития международного взаимодействия в сфере информационной безопасности (ИБ) и киберустойчивости ФинЦЕРТ организовал и провел первые трансграничные киберучения с представителями центральных банков стран БРИКС. Киберучения проходили в 2 этапа. Первый, дистанционный, прошел в начале августа 2024 года. Во время его проведения отрабатывалось взаимодействие участников в части обмена информацией о выявленной угрозе ИБ с использованием бюллетеней, подготовленных в соответствии с утвержденным форматом Канала BRISC.

Второй этап провели в середине сентября на площадке Университета Иннополис (Республика Татарстан) в очном формате. В течение этого этапа участники отрабатывали навыки реагирования на компьютерные атаки, использования различных средств их обнаружения, поиска следов злоумышленников (индикаторов компрометации) и ликвидации последствий атак.

В 2025 г. ФинЦЕРТ продолжит развивать практику проведения киберучений среди национальных (центральных) банков стран – участников межгосударственных союзов[3], в которые входит Россия.

С помощью тактик, примененных в 2024 г., злоумышленники продолжат использовать комбинацию инструментов и методов для скрытого проникновения, создания условий долговременного присутствия и разрушения информационных инфраструктур компаний. С целью сбора и кражи чувствительной информации мошенники будут стараться оставаться в системах как можно дольше, чтобы лучше изучить инфраструктуру. Как следствие, ожидается увеличение времени между компрометацией системы и фактами ее выявления со стороны служб ИБ.

В 2025 г. сохранится проблема атрибуции и обнаружения следов злоумышленников в связи с использованием ими скомпрометированных серверов, VPN и мобильных прокси для маскирования атак.

Очевидно, что последствиями успешных атак на коммерческие организации, обрабатывающие чувствительную информацию, являются утечки такой информации, которую в дальнейшем используют для проведения целевых атак на граждан. Злоумышленники находят все более изощренные методы воздействия на выбранные цели, что неуклонно ведет к росту количества и объема хищений денежных средств. Противодействие подобным преступлениям – одно из целевых направлений работы ФинЦЕРТ.

Дополнительно в рамках борьбы с фишингом[4], распространением информации о незаконной финансовой деятельности и деятельностью финансовых пирамид и безлицензионной деятельностью в сети Интернет ФинЦЕРТ за 2024 г. выявил и направил на блокировку порядка 46 000 доменов. Этот показатель превышает на 33% уровень 2023 года.

[3] ЕАЭС, АСЕАН, ШОС.

[4] Фишинг – вид интернет-мошенничества с целью получить доступ к конфиденциальным данным путем маскировки электронного письма или сайта под доверенный аналог.

КОМПЬЮТЕРНЫЕ АТАКИ НА ФИНАНСОВЫЙ СЕКТОР В 2024 ГОДУ

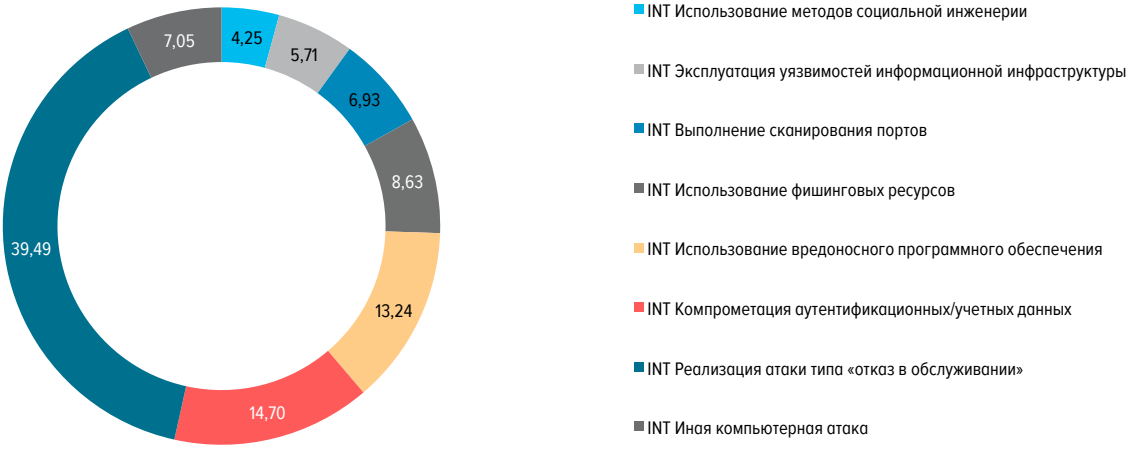
В 2024 г. через Автоматизированную систему обработки инцидентов ФинЦЕРТ (АСОИ ФинЦЕРТ) от участников информационного обмена было получено более 750 сообщений о фактах компьютерных атак и компьютерных инцидентов. Основными КА, сведения о которых получил ФинЦЕРТ от финансовых организаций, стали DDoS-атаки, атаки с использованием вредоносного программного обеспечения (ВПО), компрометация учетных данных (рис. 1).

РАСПРЕДЕЛЕНИЕ КОМПЬЮТЕРНЫХ АТАК *Рис. 1*

Источник: данные Банка России.

Анализ полученных запросов показал, что за 2024 г. атаки распределялись следующим образом:

РАСПРЕДЕЛЕНИЕ ВСТРЕЧАЕМОСТИ КОМПЬЮТЕРНЫХ АТАК ПО ТИПАМ *Рис. 2*
(%)



Источник: данные Банка России.

В 2024 г. среди вредоносного программного обеспечения преобладали такие типы, как Trojan.Agensla.gen и Trojan-PSW.MSIL.Stealer.gen, относящиеся к ВПО, направленному на возможность кражи учетных данных пользователей, а также удаленного подключения и управления зараженным устройством.

В ходе анализа целевых КА, связанных с распространением ВПО через электронные почтовые сообщения, ФинЦЕРТ учитывает следующие показатели:

– местонахождение почтового сервера, с которого направлено фишинговое письмо либо письмо с ВПО;
– местонахождение командного сервера, на который направлен запрос при запуске ВПО.

Географическое распределение источников атак, зафиксированных в 2024 г., выглядит следующим образом:

ГЕОГРАФИЧЕСКОЕ РАСПРЕДЕЛЕНИЕ ИСТОЧНИКОВ КОМПЬЮТЕРНЫХ АТАК *Рис. 3*

В 2024 г. увеличилась активность ВПО типа Trojan-Ransom, позволяющего зашифровывать данные на зараженном устройстве. Чаще всего в результате этих атак злоумышленники требовали выкуп для расшифровки данных пострадавшей организации. Вероятнее всего, увеличение подобного рода атак по сравнению с 2023 г. связано с публикацией в открытых источниках исходных кодов вирусов-шифровальщиков крупных группировок – например, Babuk[1] или Conti[2].

Стоит отметить, что атаки шифровальщиков на объектах компьютерных инцидентов могут происходить не сразу после компрометации системы. После заражения и распространения внутри объекта КИ может осуществляться постоянная кража информации, и только после исчерпания информационного интереса к объекту КИ начинается атака шифровальщиком. Это

[1] Babuk – программа-вымогатель, используемая одноименной хакерской группировкой для атак на корпоративные сети с начала 2021 года. Исходный код программы был выложен на русскоязычном хакерском форуме в сентябре 2021 года.

[2] Conti – программа-вымогатель, используемая одноименной хакерской группировкой ориентировочно с февраля 2020 года. С 2020 по 2022 гг. группировка атаковала около 860 организаций по всему миру. С конца мая 2022 г. группировка сообщила о прекращении своей деятельности.

означает, что временной промежуток между первичной компрометацией системы и последующей атакой шифровальщиками может достигать нескольких месяцев. Таким образом, в 2025 г. также ожидается большое количество инцидентов ИБ, связанных с атаками шифровальщиков.

Можно выделить три первоначальных вектора проникновения в ИИ организаций финансовой сферы:
- перебор связки логин-пароль;
- компрометация учетных записей подрядной организации;
- использование уязвимостей в ПО, установленном в атакуемой организации.

Исходя из полученных данных о первоначальном доступе в скомпрометированные системы организаций, можно сделать следующие выводы:
- парольная политика в отношении технических учетных записей базируется на использовании словарных паролей, что не соответствует минимальным требованиям, установленным разделом 7.2.2.3 ГОСТ Р 57580.1-2027 национального стандарта Российской Федерации «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (утвержден и введен в действие приказом Росстандарта от 08.08.2017 № 822-ст);
- финансовым организациям требуется пересмотреть матрицу доступа в отношении учетных записей подрядных организаций, обеспечивающих функционирование информационных систем. Кроме того, рекомендуется ограничивать права доступа для УЗ подрядных организаций, расширяя их на время проведения технических работ по обслуживанию систем. Этот шаг поможет минимизировать риски вредоносной активности в случае компрометации подрядчика;
- рекомендуется поддерживать информационные системы в актуальном состоянии: вовремя устанавливать обновления от разработчиков, особенно в отношении обновлений по ИБ. При невозможности установки обновлений в силу каких-либо обстоятельств рекомендуется рассмотреть возможность замены ПО на аналоги и/или разработать компенсирующие меры по повышению защищенности информационных инфраструктур.

Атаки через подрядные организации

Наиболее популярным в 2024 г. способом получения первоначального доступа в системы компаний финансовой сферы стала компрометация подрядных организаций.

С ростом количества компьютерных инцидентов у организаций финансовой сферы, вызванных компрометацией подрядных организаций (атаки на цепочку поставки), появилась необходимость превентивного реагирования и на такие угрозы. Начиная с 2022 г. ФинЦЕРТ ведет работу по взаимодействию с поставщиками различных ИТ-решений и услуг, продукты которых активно используются организациями финансовой сферы. Участие таких компаний в информационном обмене, с одной стороны, позволяет обеспечить сведениями об актуальных атаках и угрозах, направленных на поставщиков услуг, с целью своевременной защиты их инфраструктуры, а с другой – оперативно взаимодействовать при выявлении признаков компрометации их инфраструктуры и способствовать оповещению финансовых организаций о выявленных событиях информационной безопасности для принятия соответствующих мер реагирования.

За 2024 г. ФинЦЕРТ выявил 17 инцидентов у организаций, предоставляющих ИТ-услуги для более чем 70 компаний финансовой сферы, включая системно значимые кредитные организации.

ФинЦЕРТ направил более 80 уведомлений финансовым организациям с информацией о компрометации инфраструктуры подрядчиков с целью принятия мер реагирования. Несмотря на информирование, в ряде случаев ФинЦЕРТ зафиксировал целевые атаки с инфраструктур подрядных организаций на инфраструктуру финансовых компаний.

Рассмотрим ряд КА на подрядные организации, предоставляющие услуги финансовому сектору.

Атака на разработчика автоматизированных банковских систем

Подрядная компания оказывает услуги по внедрению собственных разработанных продуктов для организации и ведения банковской деятельности, а также деятельности управляющих компаний, бирж, брокеров и так далее.

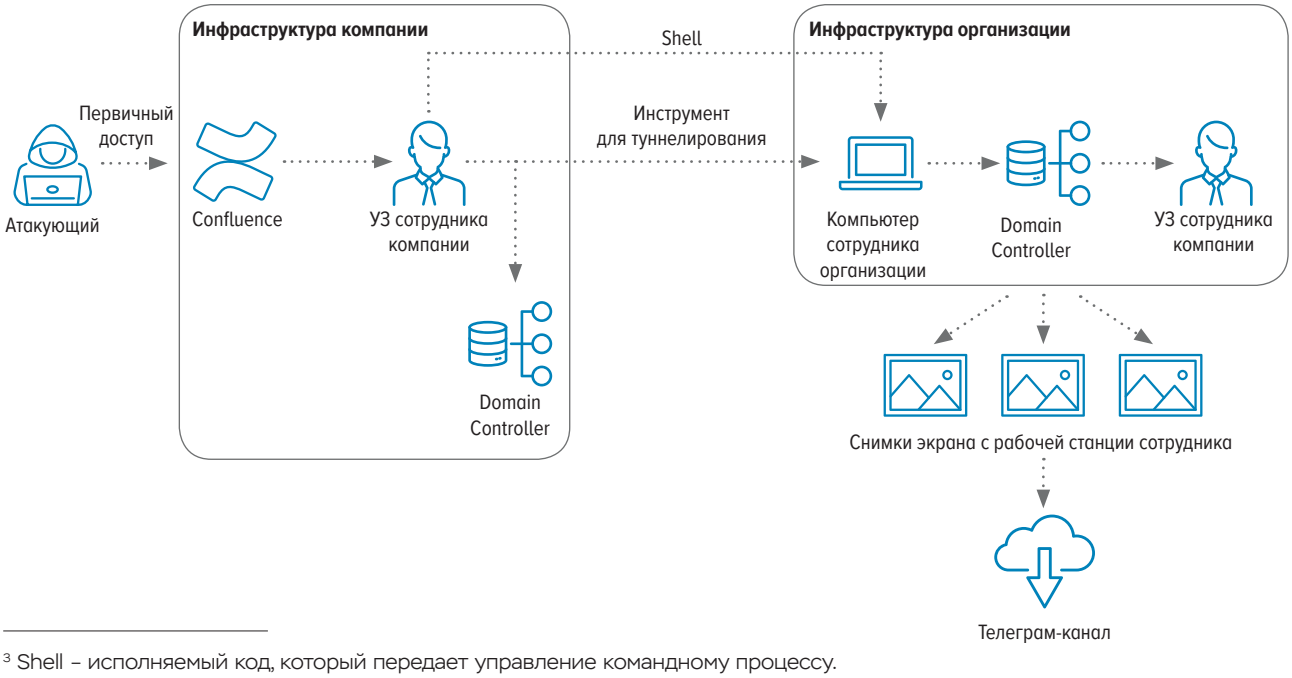
При внедрении и сопровождении продуктов большинство финансовых организаций предоставляли удаленный доступ работникам компании в информационной инфраструктуре.

В результате анализа инцидента установлено, что первичный доступ в сеть компании был получен путем эксплуатации одной из уязвимостей в системе Confluence. После получения первичного доступа к этой системе была скомпрометирована учетная запись работника компании, затем последовала компрометация домена контроллера RDS. После этого произошла компрометация системы управления виртуализацией EXSI.

Закрепившись в сети компании, злоумышленник начал атаку на организацию-заказчик из финансовой сферы. Используя скомпрометированную учетную запись сотрудника компании, атакующие установили ПО для туннелирования на компьютер сотрудника организации финансовой сферы. Затем через этот туннель на компьютер работника был установлен специальный Shell[3], позволяющий получить удаленный доступ к компьютеру извне и дистанционно выполнять произвольные команды. Таким образом, атакующие получили прямой доступ в ИТ-инфраструктуру организации.

На следующем этапе атакующие провели эскалацию внутри домена, что позволило получить доступ к компьютеру одного из сотрудников организации. Используя полученный доступ, атакующие сделали ряд снимков экрана в качестве доказательства успеха своей атаки. Снимки были опубликованы в телеграм-канале атакующих. Однако в ходе анализа инцидента факт утечки данных, несмотря на имеющийся доступ к компьютеру сотрудника организации, зафиксирован не был. Схема инцидента приведена на рис. 4.

РАЗБОР АТАКИ ЗЛОУМЫШЛЕННИКОВ *Рис. 4*



[3] Shell – исполняемый код, который передает управление командному процессу.

Атака на разработчика финтехпродуктов

Другая компания разработчика финтехпродуктов занимается созданием ИТ-решений и технологий для онлайн-кредитования и рыночного финансирования.

В результате компрометации компании произошла утечка баз данных, связанных с организациями финансовой сферы. Данные обрабатывались на стороне компании.

В ходе расследования инцидента было установлено, что злоумышленник подключался по паролю к скомпрометированной УЗ сотрудника компании с использованием VPN-сервисов для сокрытия источника атаки.

Вектор компрометации первичной УЗ сотрудника не установлен. Однако определено, что была скомпрометирована как минимум еще одна УЗ сотрудника компании, к которой атакующие подключались при помощи того же VPN-сервиса. Всего для подключения к скомпрометированным УЗ сотрудников компании использовалось 5 VPN-адресов, арендованных у хостинг-провайдеров на территории России и Германии.

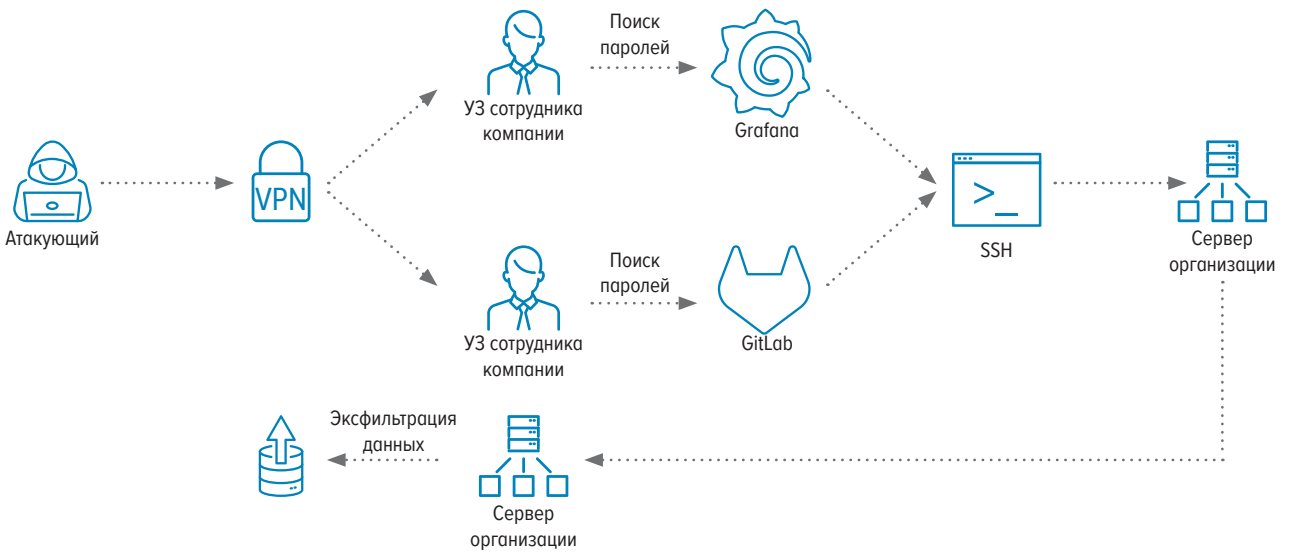
При подключении к скомпрометированным УЗ злоумышленники просматривали данные о проектах компании через систему Grafana в поисках информации о других УЗ и параметрах (ключах) подключения, хранящихся в открытом виде. Кроме того, злоумышленники искали логины и пароли в GitLab-репозиториях.

Затем злоумышленники попытались проникнуть внутрь инфраструктуры компании при помощи SSH-соединений, а также эксплуатировать уязвимость CVE-2022-2992 в GitLab, позволяющую удаленно выполнить произвольный код на атакуемом устройстве.

В ходе инцидента злоумышленнику удалось собрать данные, необходимые для успешного проникновения в инфраструктуру одной из организаций финансовой сферы. На другие компьютеры компании злоумышленники попали со скомпрометированного сервера через SSH-сервер с использованием выявленных учетных записей.

Стоит отметить, что после успешной компрометации сервера финансовой компании с него производилась обратная атака на один из серверов разработчика финтехпродуктов. Затем зафиксирована выгрузка информации из баз данных на сервере компании. Выгружена была информация, связанная с пользователями иных финансовых организаций (полную схему см. на рис. 5).

СХЕМА АТАКИ ЗЛОУМЫШЛЕННИКОВ *Рис. 5*



Атака на разработчика веб-сайтов при помощи перебора паролей

Компания занимается разработкой веб-сайтов, мобильных приложений и интеграцией с использованием программного интерфейса, позволяющего связывать между собой приложения (далее – API). Также в сферу деятельности компании входит поддержка уже существующих сайтов заказчиков. Один из них – финансовая организация, информация об утечке персональных данных клиентов которой опубликовали на популярном интернет-ресурсе.

В ходе расследования инцидента было установлено, что произошла компрометация сервера, где располагается сайт-визитка организации. На сервере хранились сведения, заполняемые через форму обратной связи и не являющиеся персональными данными клиентов организации. Доступ к серверу осуществлялся при помощи Web shell, размещенного атакующими на сервере, а выгрузка данных из баз – при помощи программного обеспечения Adminer v. 4.8.1.

Когда пострадавшая финансовая компания стала разбираться, как Web shell[4] был загружен на сервер, установили, что его загрузка произошла с технической УЗ сотрудника организации, обслуживающей их сервер и сайт-визитку. После этого инициировали расследование инцидента в инфраструктуре компании с подозрением на более раннюю компрометацию системы.

Факт компрометации инфраструктуры компании подтвердился: было установлено, что атакующим удалось подобрать пароль от технической УЗ. Пароль состоял из комбинации букв и цифр – она была словарной, что упрощало атакующим процесс перебора пароля от технической УЗ. Таким образом, скомпрометировав инфраструктуру компании и выявив в ней авторизационные данные от инфраструктуры организации-заказчика, атакующие проникли во внутреннюю сеть финансовой организации и украли информационные данные с сервера.

Пример превентивного реагирования и противодействия на компьютерную атаку через инфраструктуру подрядных организаций

Приведенные выше атаки на финансовые компании через инфраструктуру и уязвимости подрядных организаций можно было бы избежать при комплексном, своевременном и более эффективном информационном обмене между всеми организациями не только финансовой сферы, но и подрядных организаций, провайдеров телекоммуникационных и облачных услуг, сервис-провайдеров по информационной безопасности и компаний ИТ-услуг и ИТ-решений.

С целью консолидации максимально полной информации о компьютерных атаках, совершаемых злоумышленниками на организации финансовой сферы, ФинЦЕРТ использует широкий набор инструментов, в том числе мониторинг открытых интернет-источников, посредством которых была получена информация о возможной компрометации компании – производителя корпоративного ПО и облачных сервисов. Для минимизации рисков ФинЦЕРТ Банка России принял решение параллельно запустить 2 процесса:

- организацию коммуникации с представителями подразделения ИБ компании для взаимодействия по произошедшему инциденту и оказания консультативной помощи для локализации КИ и ликвидации последствий;
- оповещение организаций финансовой сферы о возможной компрометации компании, являющейся для них поставщиком ИТ-решений.

Таким образом, в результате оперативного реагирования со стороны ФинЦЕРТ на полученную информацию было оповещено более 15 организаций финансовой сферы, среди которых были

[4] Web shell – командная оболочка для удаленного управления веб-сервером.

системно значимые организации, а также своевременно обнаружен и локализован инцидент внутри инфраструктуры компании, благодаря чему удалось избежать следующих последствий:

- утечки персональных данных;
- утечки иной чувствительной информации;
- шифрования инфраструктуры организаций;
- подмены и дискредитации сайтов организаций и иных серьезных последствий.

АТАКИ НА ФИНАНСОВЫЕ ОРГАНИЗАЦИИ СТАНОВЯТСЯ СЛОЖНЕЕ: ОСНОВНЫЕ ВЕКТОРЫ УГРОЗ 2024 ГОДА

В рамках реагирования на компьютерные атаки в финансовом секторе специалисты ФинЦЕРТ продолжают отслеживать и анализировать новые векторы угроз и методы, применяемые злоумышленниками.

С каждым годом методы атак становятся все более сложными и многоуровневыми, что требует от финансовых организаций постоянного совершенствования подходов к реагированию на них и обеспечению ИБ.

Злоумышленники развивают методы сокрытия своей деятельности, что позволяет обходить традиционные средства защиты информации и существенно усложняет выявление атак и их оперативное пресечение.

В этом разделе рассмотрим основные векторы атак, с которыми сталкивались финансовые организации в 2024 г., ключевые механизмы и техники, используемые злоумышленниками.

Атаки в традиционном понимании как прямое хищение денежных средств постепенно уступают место более сложным и многоэтапным схемам. С учетом высокой сложности инфраструктуры крупных финансовых организаций и усиленных систем защиты злоумышленники адаптируют свои цели и методы. Теперь приоритетными целями становятся не только материальные активы, но и подрыв доверия к организациям через манипуляцию данными и информационное давление.

В течение года наблюдались атаки злоумышленников, направленные на достижение следующих целей:

- **дестабилизация бизнеса** – утечка конфиденциальной информации, способная подорвать репутацию компании или вызвать юридические и регуляторные риски;
- **создание общественного резонанса** – распространение недостоверной или компрометирующей информации через социальные медиа и другие каналы для создания паники или формирования негативного восприятия как кредитно-финансовой сферы в целом, так и некой финансовой организации в частности;
- **осуществление информационного давления на сотрудников** – использование угроз раскрытия компрометирующей информации, демонстрация контроля над внутренними процессами компании или шантаж;
- **блокировка данных и вымогательство** – атаки с использованием шифровальщиков, направленные на блокировку доступа к критически важной информации.

Атаки на финансовую инфраструктуру, как правило, включают несколько этапов: от подготовки инфраструктуры нападения до проникновения, закрепления в инфраструктуре и организации скрытого канала вывода данных извлечения данных и их монетизации.

Современные методы все чаще включают элементы информационного воздействия, манипуляции восприятием событий и эксплуатации человеческого фактора, что делает противодействие таким атакам еще более сложным.

Злоумышленники используют тактику влияния на информационное поле организации и ее экосистему, усиливая давление через комбинацию технических и информационных инструментов.

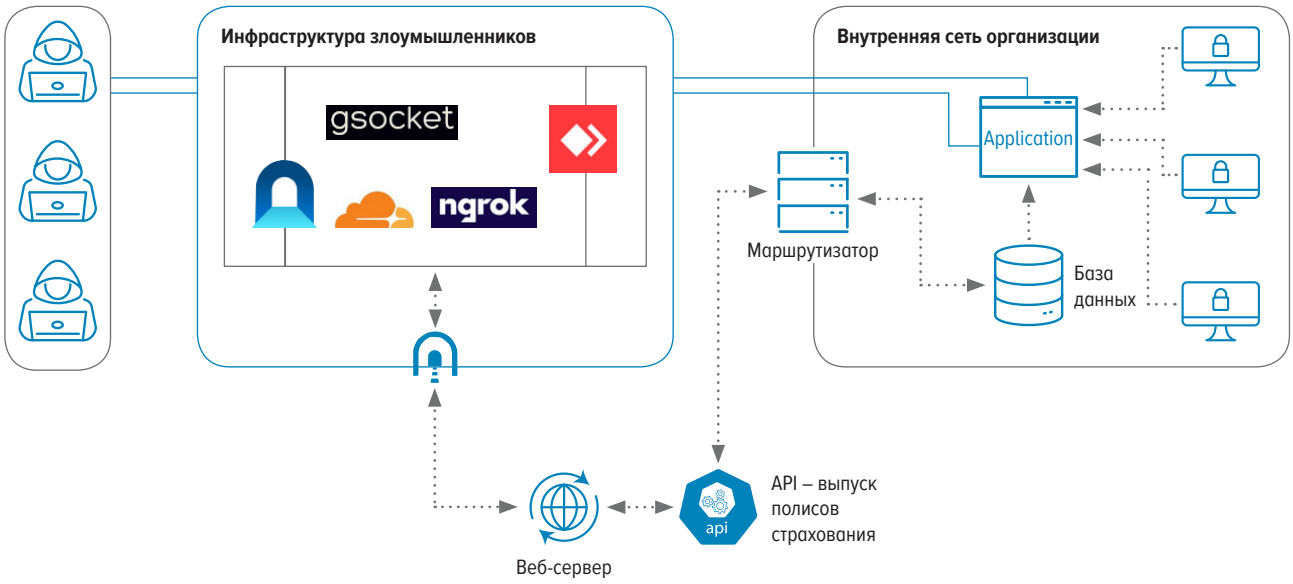
Ниже представлены обобщенные основные этапы проведения КА на инфраструктуру организаций, которые включают следующие шаги.

– **Подготовка инфраструктуры**. Злоумышленники создают инфраструктуру, которая позволит скрыть свои действия от систем защиты. Инфраструктура может включать арендованные серверы, компрометацию уязвимых серверов и прокси, а также использование VPN и мобильных прокси для маскировки реального местоположения.
– **Проникновение и эксплуатация уязвимостей**. Этот шаг подразумевает непосредственное проникновение в информационную систему. Злоумышленники могут использовать различные уязвимости – начиная от слабых паролей и заканчивая уязвимостями в веб-приложениях или в старых версиях серверных систем.
– **Закрепление в инфраструктуре, организация скрытого канала вывода данных.** После успешного проникновения в ИИ атакуемой организации злоумышленники выполняют этап закрепления. Его цель – обеспечить сохранение доступа и минимизировать вероятность обнаружения. Для этого устанавливаются механизмы и средства долгосрочного закрепления, такие как **Backdoor**[1], легитимные УЗ с повышенными привилегиями или вредоносные службы, которые маскируются под штатные процессы. Одновременно организуются скрытые каналы для вывода данных, использующие методы шифрования и обфускации[2] трафика. Эти каналы настраиваются с учетом особенностей сети жертвы, чтобы минимизировать аномалии в сетевом трафике. Закрепление и организация вывода данных реализуются параллельно, так как общие инструменты позволяют злоумышленникам сохранять контроль и обеспечивать кражу информации без лишних рисков. Длительность этапа определяется сложностью инфраструктуры и необходимостью тщательной маскировки действий.
– **Монетизация и извлечение данных**. На последнем этапе злоумышленники выбирают способы заработать на полученной в результате успешной атаки информации: продать украденные данные, использовать их для дальнейших атак (например, фишинга) либо извлечь финансовую выгоду путем шантажа.

Пример типовой схемы атаки

Один из самых частых, по мнению специалистов ФинЦЕРТ, сценариев в 2024 г. – **поэтапная атака с использованием веб-инфраструктуры организации** (рис. 6).

ПРИМЕР ПОПУЛЯРНОЙ СХЕМЫ АТАК НА ИНФРАСТРУКТУРУ ОРГАНИЗАЦИЙ *Рис. 6*



[1] Backdoor – намеренно встроенный злоумышленником дефект алгоритма.

[2] Обфускация – приведение данных путем преобразования к виду, затрудняющему технический анализ.

Сначала злоумышленники скомпрометировали сторонний веб-сервер, не относящийся напрямую к целевой организации. На этот сервер был установлен **GSocket**, который использовался для организации скрытого канала управления – C&C[3] – и туннелирования трафика. Указанный сервер стал промежуточной точкой для последующей атаки.

Далее злоумышленники провели атаку на **веб-сервер организации**, работающий на платформе **Bitrix**, используя уязвимости в конфигурации или устаревшей версии CMS. Получив доступ к серверу, они обнаружили, что этот узел связан с **внутренней инфраструктурой** организации через **API**, предназначенный для взаимодействия с базой данных. Этот API использовался для учета **и обработки финансовой документации**.

После проникновения злоумышленники закрепились на сервере, организовали скрытые каналы вывода данных и выгрузили **информацию** из базы данных. Полученные сведения потом были проданы на теневых рынках. Кроме того, злоумышленники воспользовались уязвимостью в API для совершения несанкционированных **финансовых операций**.

Таким образом, атака развивалась последовательно: от компрометации стороннего сервера до эксплуатации уязвимостей в веб-инфраструктуре и монетизации через манипуляции с внутренними данными организации.

Анализ сетевой архитектуры злоумышленников

Современные компьютерные атаки демонстрируют разнообразие тактик и подходов к организации атакующей инфраструктуры.

Основная цель действий злоумышленников – создание технической инфраструктуры, методов и средств организации телекоммуникационного взаимодействия, для маскировки и/или сокрытия профилей сетевого трафика под легитимные для организации-цели.

Компрометация серверов как плацдарм для старта

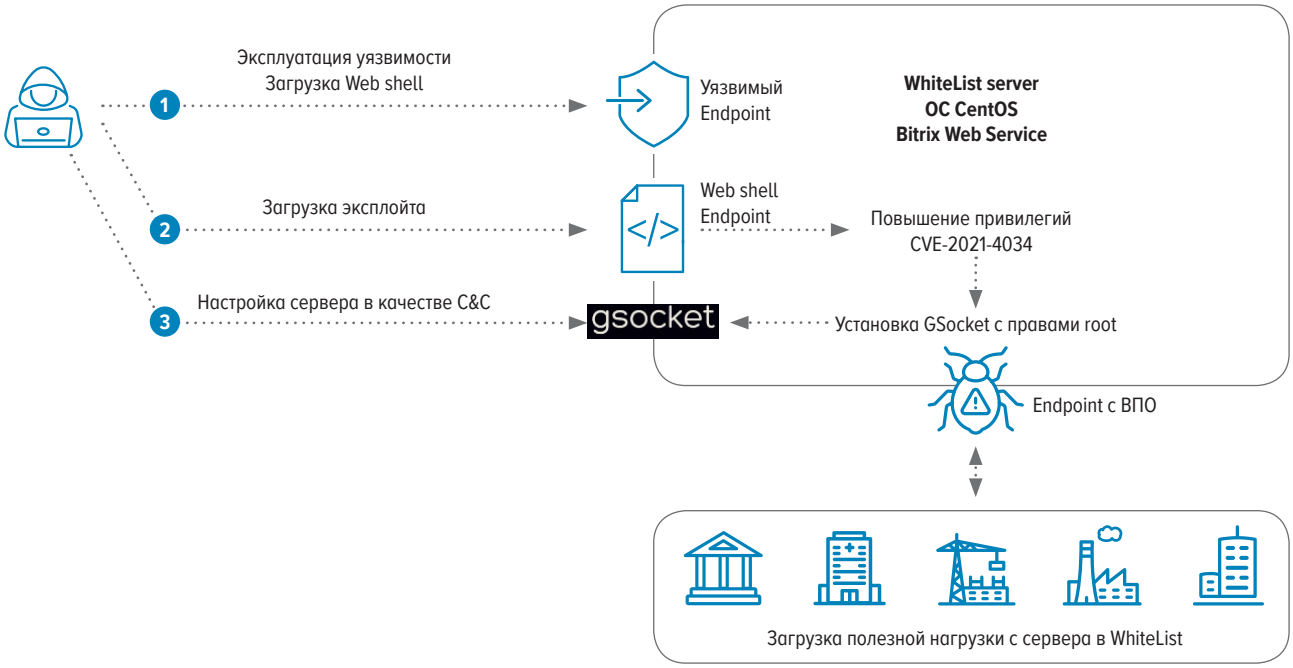
На начальном этапе при создании инфраструктуры, предназначенной для сокрытия действий и маскировки трафика под легитимный с целью минимизации вероятности обнаружения и блокировки атаки, злоумышленники часто выбирают компрометацию серверов, расположенных на территории России. Это обусловлено возможностью использования региональных IP-адресов, которые большинством систем защиты финансовых организаций воспринимаются как внутренние и безопасные. Особенно это характерно для небольших финансовых организаций, не обладающих достаточными ресурсами для обеспечения комплексной защиты информации.

Например, ФинЦЕРТ во взаимодействии с Национальным координационным центром по компьютерным инцидентам Федеральной службы безопасности Российской Федерации (НКЦКИ) зафиксировал случаи компрометации финансовых организаций через уязвимость в системе **1С-Битрикс**.

В одном из инцидентов после успешного вторжения злоумышленники использовали сервер организации как сервер приема/передачи команд управления (**C&C-сервер**). Предположительно, атакующие не полностью понимали, как можно эффективно использовать всю инфраструктуру финансовой организации, либо подходили к атаке автоматизированно. Злоумышленники оставили сервер управления в использовании на длительное время, что могло быть связано с попытками собрать дополнительные данные о системе. С него в дальнейшем произошла **утечка данных**.

[3] C&C – сервер управления и контроля, использующийся для отправки команд системам, скомпрометированным ВПО.

ИСПОЛЬЗОВАНИЕ СЕРВЕРА УЧАСТНИКА ИНФОРМАЦИОННОГО ОБМЕНА В КАЧЕСТВЕ C&C *Рис. 7*



Роль хостинг-провайдеров в увеличении атак

Поскольку компрометация серверов требует значительных усилий или времени, злоумышленники часто выбирают аренду серверов у хостинг-провайдеров. Это позволяет быстро развернуть необходимую инфраструктуру для атаки, избегая трудоемких этапов технической настройки, и снижает риски быть замеченным.

Сфера хостинг-услуг, несмотря на ее сравнительно давнюю историю, продолжает активно развиваться. Технологический прогресс, рост цифровизации экономики и увеличение объемов предоставляемых услуг способствуют появлению новых вызовов как для финансовой отрасли, так и для регулирующих органов.

При этом нормативно-правовая и регуляторная база в этой сфере все еще совершенствуется, что объясняет наличие определенных пробелов и сложностей, связанных с технологическим отставанием и обеспечением должного контроля ИБ. Основными проблемами являются:

– **идентификация клиентов:** в условиях растущего количества кибератак вопрос идентификации клиентов приобретает особую значимость. Несмотря на предпринимаемые меры по усилению контроля, на сегодня отсутствуют строгие требования к верификации клиентов. В частности, для аренды виртуальных частных серверов, особенно у мелких и региональных провайдеров, не предусмотрены обязательные процедуры подтверждения личности. Это создает риски для использования серверов злоумышленниками, которые могут действовать анонимно и без предоставления достоверных данных;

– **анонимность при оплате услуг:** в связи с развитием цифровых финансовых активов некоторые хостинг-провайдеры принимают криптовалюту в качестве средства оплаты, что затрудняет выявление нарушителей и их привлечение к ответственности. Это создает дополнительные сложности в выявлении и отслеживании финансовых транзакций.

Важно отметить, что развитие отрасли хостинг-услуг требует гибкого подхода к регулированию, чтобы обеспечить баланс между эффективным контролем и поддержкой роста инноваций.

Рост количества IP-адресов RU-сегмента в атаках

В последние годы наблюдается рост числа атак, исходящих с серверов, размещенных на территории Российской Федерации. Это связано с несколькими факторами.

Особенность блокировок трафика: государственные органы, такие как Федеральное государственное унитарное предприятие «Главный радиочастотный центр» (ФГУП «ГРЧЦ»), активно противодействуют атакам, внедряя механизмы фильтрации и блокировки, включая технологии глубокого анализа трафика (далее – DPI). Это значительно затрудняет использование зарубежных серверов злоумышленниками. В результате последние переходят на российские серверы, где сложнее организовать масштабную фильтрацию, не затрагивая легитимные сервисы.

Легитимный вид трафика: региональные IP-адреса, предоставляемые такими серверами, часто воспринимаются как безопасные системами защиты финансовых организаций, что требует со стороны служб ИБ повышенного внимания к трафику, идущему с IP-адресов, находящихся в юрисдикции Российской Федерации.

Современные вызовы, связанные с киберугрозами и ростом незаконной активности в цифровой среде, требуют высокой скорости реагирования. Для обеспечения безопасности информационных систем и повышения устойчивости инфраструктуры в 2023 г. были разработаны и утверждены ключевые нормативные акты, направленные на регулирование деятельности хостинг-провайдеров. Эти документы усиливают контроль за обработкой и хранением данных, а также взаимодействие провайдеров с государственными системами безопасности.

В рамках данной работы приказ Минцифры России от 01.11.2023 № 935 направлен на создание условий для проведения оперативно-разыскных мероприятий. Документ обязывает хостинг-провайдеров подключаться к системе оперативно-разыскных мероприятий и предоставлять вычислительные мощности для реализации этих мероприятий. В свою очередь правоохранительные органы своевременно реагируют на киберугрозы, включая пресечение преступлений, совершаемых с использованием цифровых ресурсов. Одна из ключевых целей – снижение уровня анонимности злоумышленников, использующих российскую инфраструктуру.

Комплексный подход к защите данных дополнен приказом Минцифры России от 01.11.2023 № 936, который устанавливает требования по защите информации в системах, подключенных к Интернету. Среди обязательств хостинг-провайдеров: взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), оперативное устранение уязвимостей, предотвращение DDoS-атак и хранение данных о взаимодействиях пользователей.

Эти меры направлены на предотвращение утечек информации и обеспечение стабильности работы критической информационной инфраструктуры.

Использование мобильных прокси-серверов

Злоумышленники стали чаще прибегать к использованию **прокси-серверов**, включая мобильные прокси, развернутые на арендуемых серверах, чтобы лучше скрыть свои действия. Это может быть сделано через использование **GoIP-устройств**[4] **(в случае с телефонным мошенничеством – для анонимизации входящего VoIP-трафика**[5]**),** и в связи с динамическим выделением IP-адресов для мобильных устройств злоумышленники прибегают к использованию модемов с сим-картами в качестве динамически изменяемого прокси (мобильный прокси).

[4] GoIP-устройство – аппаратное средство, предназначенное для передачи голосового трафика через IP-сети (VoIP) с использованием сим-карт сотовых операторов.

[5] VoIP-трафик – поток данных, передающих голосовую информацию через IP-сети.

МАРШРУТИЗАЦИЯ ТРАФИКА. МОБИЛЬНЫЕ ПРОКСИ *Рис. 8*

Использование злоумышленниками таких прокси-серверов направлено на сокрытие построенной инфраструктуры для атаки, в том числе ее регионального местоположения.

Основные причины использования мобильных-прокси для проведения атак:

– **высокая ротация IP-адресов:** мобильные прокси, как правило, обеспечивают высокую сменяемость IP-адресов, что затрудняет их блокировку, поскольку один адрес может использоваться десятками пользователей в течение дня;

– **трафик, не отличимый от легитимного:** использование мобильных прокси-сетей или автономных систем мобильных операторов (далее – ASN) позволяет сделать трафик практически не отличимым от обычного пользовательского. Это важно для финансовых организаций, поскольку часть их пользователей может использовать мобильные сети для доступа к сервисам;

– **доступность и низкая стоимость:** на теневых рынках злоумышленники могут легко приобрести доступ к мобильным прокси-сетям, которые предоставляются в аренду. Стоимость таких услуг относительно невысока, а доступ к ним предоставляется практически мгновенно.

В 2024 г. был принят ряд нормативных актов, предусматривающих новые правила регистрации сим-карт:

– с 01.01.2025 вступают в силу изменения в закон «О связи» (Федеральный закон 126-ФЗ), по которому иностранные граждане и лица без гражданства смогут заключать договоры на оказание услуг связи только при личном посещении салона связи с обязательной биометрической идентификацией;

– с 01.04.2025 для граждан Российской Федерации вводится ограничение на количество зарегистрированных сим-карт – не более 20 номеров на одно физическое лицо.

Эти меры направлены на предотвращение использования анонимных сим-карт в противоправных целях.

Использование VPN-решений и анонимизация трафика

В последние годы наблюдается рост атак, в которых злоумышленники используют скомпрометированные локальные серверы и аренду серверов у региональных хостинг-провайдеров. Это заметно усложняет расследование подобных инцидентов. Несмотря на такую тенденцию, VPN-решения продолжают оставаться одним из ключевых элементов инфраструктуры, обеспечивающих скрытность атак.

В ходе анализа инцидентов неоднократно фиксировались случаи аренды серверов злоумышленниками у таких провайдеров, как Hetzner, DigitalOcean, OVH, Linode, Vultr и AWS, и у российских региональных хостинг-компаний. Эти серверы часто используются в качестве промежуточных узлов для маскировки исходного IP-адреса и перенаправления трафика.

При расследовании цепочки взаимодействий и анализа инфраструктуры атакующей стороны в итоге выявляются или VPN-сервисы, или сеть Tor. Эти технологии используются для обеспечения анонимности и минимизации рисков идентификации источника атаки. Такой подход существенно усложняет получение информации, необходимой для точного установления причастных лиц или групп.

Злоумышленники активно применяют зашифрованные соединения и используют локации серверов, расположенных в юрисдикциях с высоким уровнем защиты персональных данных, что создает дополнительные сложности для правовых и технических мероприятий.

Организация скрытого канала передачи данных

В 2024 г. финансовый рынок столкнулся с изменением технических средств удаленного доступа. Злоумышленники стали использовать новые инструменты для организации скрытого канала приема-передачи данных – Ngrok, Cloudflare Tunnel и GSocket.

Самым ярким примером стал Microsoft Dev Tunnels. Этот инструмент, предназначенный для разработчиков, позволяет злоумышленникам создавать каналы связи, которые выглядят как легитимный трафик. Передавая информационные данные через серверы Microsoft, злоумышленники фактически используют репутацию компании для маскировки своих действий. Такая активность крайне затрудняет обнаружение компьютерных атак, поскольку аналитикам по безопасности приходится работать с потоком телекоммуникационного трафика, который выглядит как стандартное взаимодействие, организуемое продуктами Microsoft.

Ранее подобные подходы были связаны с инструментами TeamViewer и AnyDesk.

Самый популярный способ – это DNS-туннелирование, которое, несмотря на давнее применение, до сих пор востребовано благодаря своей адаптации к современным условиям. Этот метод стали использовать еще в эпоху лимитного Интернета – для обхода сетевых ограничений. Пример 2024 г. с вредоносным ПО Zloader, которое использует DNS для скрытого управления, подтверждает, что упомянутый способ не утратил своей актуальности.

Злоумышленники используют современные версии DNS-туннелирования, чтобы управлять зараженными системами и обходить защитные механизмы.

Скрытый канал передачи данных – это механизм, который маскирует исходные и конечные адреса и сам трафик, делая его практически неразличимым для стандартных систем защиты. Такие каналы используются:

- для удаленного управления зараженными системами;
- для кражи конфиденциальной информации;
- для обхода защитных механизмов – межсетевых экранов и систем обнаружения угроз.

В анализе ФинЦЕРТ термины «скрытый канал передачи данных» и «туннелирование трафика» используются как взаимодополняющие, раскрывающие как техническую, так и концептуальную сторону угрозы.

Типы скрытых каналов передачи данных

Существует 2 основных подхода к организации скрытых каналов передачи данных:

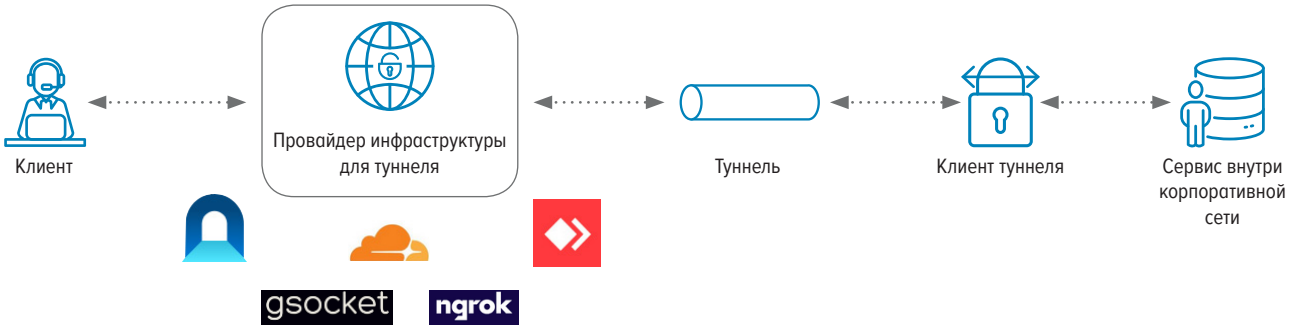
– **Использование готовой инфраструктуры**. Такие инструменты, как Ngrok, Cloudflare Tunnel, GSocket, Microsoft Dev Tunnels, TeamViewer и AnyDesk, предоставляют готовую инфраструктуру для туннелирования. Они устраняют необходимость в самостоятельной настройке серверов. Эти сервисы работают как коробочное решение, маскируя трафик под легитимные запросы и снижая риск обнаружения. Трафик, проходящий через серверы таких компаний, как Microsoft, скрыт за стандартными протоколами (например, HTTPS или DNS). Это делает его практически не отличимым от обычного сетевого взаимодействия. Благодаря маскировке и сложности анализа, такие туннели легко обходят межсетевые экраны, IDS/IPS и другие стандартные средства обнаружения. Подобный подход позволяет минимизировать затраты и время на внедрение.

– **Самостоятельная организация инфраструктуры.** Этот подход предполагает разработку и управление собственной инфраструктурой для туннелирования. Сюда входят такие методы, как DNS-туннелирование, или инструменты вроде Chisel. Однако самостоятельная настройка требует серьезной квалификации и оставляет больше следов, что повышает риск обнаружения злоумышленников. Например, при использовании DNS-туннелирования, как в случае с вредоносным ПО Zloader, требуется генерация собственных доменов и настройка серверов, что делает подход более уязвимым для детектирования.

Актуальные в 2024 году угрозы и подходы в организации скрытых каналов передачи данных

В 2024 г. активно использовался первый тип организации скрытого канала, то есть инструменты, предоставляющие готовую инфраструктуру как сервис (IaaS).

МАРШРУТИЗАЦИЯ ТРАФИКА ПРИ ИСПОЛЬЗОВАНИИ ТИПОВЫХ СЕРВИСОВ ТУННЕЛИРОВАНИЯ (NGROK, GSOCKET, ANYDESK, TEAMVIEWER, CLOUDFLARE TUNNEL, MICROSOFT DEV TUNNELS) *Рис. 9*



ФинЦЕРТ в 2024 г. сосредоточился на анализе методов туннелирования, разрабатываемых и применяемых злоумышленниками. Среди ключевых направлений проведенных работ следующие:

– подробный разбор инфраструктуры атак, в том числе выделение закономерностей в использовании IP-адресов и генерации доменов, характерных для этих туннельных систем;

– демонстрация механизмов работы туннелей, включая методы их детектирования и предотвращения;

– создание практических рекомендаций для повышения устойчивости систем к подобным атакам.

Противодействие угрозам организации скрытых каналов передачи данных

Организация скрытых каналов связи, используемых злоумышленниками, – одна из ключевых проблем для специалистов по информационной безопасности. Современные системы защиты информации (СЗИ) зачастую не способны эффективно идентифицировать трафик, создаваемый такими каналами. Злоумышленники используют протоколы, широко применяемые в легитимных бизнес-процессах (например, HTTPS, WebSocket или DNS), что затрудняет их детектирование стандартными средствами анализа трафика.

Для обеспечения превентивной защиты важно уделять внимание изучению механизмов организации скрытых каналов, включая используемые протоколы, методы маскировки и обхода межсетевых экранов. Эффективное противодействие таким угрозам невозможно без глубокого понимания сетевых технологий и принципов работы трафика внутри корпоративной инфраструктуры.

Стандартные инструменты, такие как IDS/IPS, часто не дают достаточных возможностей для обнаружения скрытых каналов, особенно если они замаскированы под легитимный трафик. Это требует использования адаптивных методов, включая:

- **анализ аномалий** для выявления отклонений в поведении сетевых узлов;
- **технологии машинного обучения**, которые позволяют определять скрытые паттерны трафика;
- **углубленный сетевой мониторинг** с сегментацией и выделением критически важных зон сети.

Решение этих задач требует привлечения специалистов с высоким уровнем квалификации в области сетевых технологий и анализа протоколов.

Только комплексный подход, включающий детальное изучение механизмов организации скрытых каналов, позволит снизить риск успешного использования злоумышленниками подобных методов.

Постинцидентный анализ и управление уязвимостями

В ходе анализа инцидентов, с которыми столкнулись специалисты ФинЦЕРТ в 2024 г., можно проследить следующие закономерности.

Время компрометации

В ряде случаев при проведении расследований инцидентов было выявлено, что информационные системы были скомпрометированы до того, как стали объектом расследования (от нескольких месяцев до года).

Этот факт подтверждается рядом инцидентов, когда уязвимости, в частности **RCE** (Remote Code Execution), были использованы злоумышленниками для первоначального проникновения и закрепления в системе, но не производили деструктивных действий. Следы их присутствия в инфраструктуре оставались незамеченными долгое время. Зачастую мошенники приступали к активным действиям после того, как публично стали доступны **PoC-эксплойты** (Proof of Concept)[6], что позволяло автоматизировать атаки и массово внедрять Shell и **Backdoor** в атакуемые системы.

Использование публичных PoC-эксплойтов

Публикация эксплойтов PoC (Proof of Concept) критичным образом влияет на масштабы и скорость реализации атак на уязвимости. Согласно данным компании Cloudflare, которая является одним из ведущих мировых провайдеров в области сетевой безопасности и доставки контента, от момента публикации PoC до первых зафиксированных атак проходит в среднем менее 22 минут.

[6] PoC-эксплойты (Proof of Concept) – эксплойты для эксплуатации уязвимостей.

Это позволяет злоумышленникам оперативно адаптировать эксплойты для использования в автоматизированных инструментах, таких как Nuclei[7] и Metasploit[8], которые регулярно обновляются за счет шаблонов и сценариев атак. Подобные инструменты упрощают поиск и эксплуатацию уязвимостей, делая их доступными для менее квалифицированных атакующих.

Кроме активного сканирования сетей, злоумышленники широко применяют специализированные платформы анализа интернет-ресурсов, такие как Fofa[9], Shodan[10], Censys[11], Netlas[12] и ZoomEye[13]. Эти сервисы предоставляют исчерпывающие данные о конфигурации, сетевой инфраструктуре и возможных уязвимостях целевых систем.

Таким образом, злоумышленникам зачастую не требуется инициировать собственное сканирование, поскольку бóльшая часть информации о целевых системах уже доступна в открытых источниках. Организациям крайне важно отслеживать информацию, которая может публиковаться на таких платформах, и своевременно принимать меры по устранению возможных рисков.

В текущей ситуации критична скорость применения обновлений безопасности. Согласно исследованию компании Mandiant, специализирующейся на исследованиях угроз, реагировании на инциденты и предоставлении аналитических данных о кибератаках, за период с 2018 по 2023 г. среднее время между выпуском обновлений в ПО и его внедрением сократилось с 63 до 5 дней. Однако этого недостаточно, поскольку атаки начинаются практически сразу после публикации PoC. Более того, статистика «Лаборатории Касперского» указывает на ежегодный рост атак с использованием публичных PoC на 2–3%, что подчеркивает критическую важность сокращения временно́го интервала между обнаружением уязвимости и ее устранением.

Эффективное управление уязвимостями должно стать ключевым направлением деятельности подразделений ИБ организаций. С развитием технологий искусственного интеллекта злоумышленники получают доступ к инструментам, которые упрощают разработку эксплойтов и автоматизацию атак.

Применение искусственного интеллекта позволяет ускорить адаптацию существующих PoC-эксплойтов и создавать новые методы атаки с минимальным участием человека. Это требует от организаций проактивного подхода к мониторингу угроз и внедрению современных средств защиты. Для достижения указанной цели необходимо внедрить комплексные процессы оценки и устранения уязвимостей, интегрировать методы активного поиска угроз, а также совершенствовать механизмы мониторинга инфраструктуры. Проактивный подход, включающий регулярный анализ, применение исправлений безопасности и контроль за потенциально доступной информацией, позволит минимизировать временные рамки для возможной атаки и обеспечить оперативное реагирование на них. Реализация этих мер способствует повышению устойчивости организаций перед лицом современных угроз и помогает предотвратить эксплуатацию уязвимостей.

---

[7] Nuclei – инструмент автоматизированного тестирования безопасности, который позволяет выполнять сканирование с использованием шаблонов для поиска уязвимостей и конфигурационных ошибок в инфраструктуре.

[8] Metasploit – платформа для разработки, тестирования и эксплуатации уязвимостей, широко используемая как исследователями безопасности, так и злоумышленниками.

[9] Fofa – платформа для пассивного анализа интернет-ресурсов, позволяющая обнаруживать открытые порты, сервисы и конфигурации сетевой инфраструктуры.

[10] Shodan – поисковая система для выявления подключенных к Интернету устройств и сервисов, включая IoT, серверы и системы управления.

[11] Censys – сервис, предоставляющий аналитические данные о безопасности интернет-ресурсов и помогающий выявлять уязвимости.

[12] Netlas – платформа для исследования сетевых ресурсов и анализа их доступности, конфигурации и уязвимостей.

[13] ZoomEye – платформа для сканирования и анализа интернет-ресурсов, включая устройства IoT и серверные приложения.

Повторные атаки и продажи доступа

В процессе расследования инцидентов 2024 г. ФинЦЕРТ выявил ряд повторных атак на ранее скомпрометированные системы финансовых организаций.

В процессе устранения уязвимости возникает важный момент: не всегда ликвидируются все следы компрометации. В одном из примеров, с уязвимостью CVE-2022-27228 в 1С-Битрикс, даже после исправления проблемы, злоумышленники могли оставить скрытые компоненты (Backdoor или веб-оболочки), которые затем использовались для повторных атак. Это означает, что устранение самой уязвимости не гарантирует безопасности системы, если не проведен тщательный постанализ.

В некоторых случаях доступ, оставленный злоумышленниками, может быть продан другим преступным группировкам. Иногда система остается скомпрометированной еще долгое время, пока не происходит расследования или регулярной проверки безопасности.

Постинцидентный анализ

В связи с возможностью повторных атак и последующей продажи доступа постинцидентный анализ системы после внедрения обновлений (патчей) и устранения уязвимостей становится крайне важным.

ФинЦЕРТ часто фиксирует, что после устранения уязвимости системы не проверяются на наличие следов компрометации, что приводит к повторным атакам. Например, многие специалисты занимаются исключительно установкой обновлений ПО и забывают про постинцидентный анализ, что становится основной причиной повторения инцидентов.

В еженедельных дайджестах ФинЦЕРТ всегда уделяет особое внимание не только описанию уязвимости и ее эксплуатации, но и тому, какие следы остаются после. Основная цель дайджеста – информировать специалистов ИБ о компонентах и файлах, которые злоумышленники могут оставить в системе, а также предоставить максимально подробные рекомендации о проверках в рамках постинцидентного анализа.

Такой подход позволяет не только закрыть уязвимость, но и защитить систему от будущих атак.

Рекомендации для улучшения процесса управления уязвимостями

Для повышения эффективности постинцидентного анализа и решения комплексных задач по управлению уязвимостями ФинЦЕРТ рекомендует выполнить следующие мероприятия:

- **Полный ретроспективный анализ системы.** После обнаружения уязвимости, особенно **PREAUTH RCE**[14], важно не ограничиваться только установкой обновлений системы или ПО. Следует дополнительно провести всесторонний анализ системы на наличие следов компрометации. Подход включает проверку конфигураций, журналов, поиск скрытых объектов или файлов, оставленных злоумышленниками, а также анализ аномальной активности.
- **Проверка PoC-эксплойтов.** Специалисты должны уделять внимание публичным **PoC** и проверять свои системы на наличие тех уязвимостей, которые уже были публично раскрыты. После публикации PoC следует не только обязательно установить обновления, но и проводить углубленный анализ на предмет возможного повторного использования уязвимости.

[14] PREAUTH RCE – уязвимость, которая позволяет выполнить код без аутентификации.

– **Раннее обнаружение следов компрометации.** Важно учитывать, что злоумышленники могут оставить следы компрометации, даже если саму уязвимость закрыли. Программы и утилиты, такие как **Backdoor**, могут быть использованы для повторного доступа. Поэтому регулярные сканирования и анализ активности в системе – обязательный элемент защиты.
– **Мониторинг прав доступа и настроек конфигураций.** В процессе конфигурации серверов необходимо тщательно контролировать права доступа, чтобы избежать избыточных привилегий, которые могут быть использованы для дальнейшего продвижения атакующего.

Проведение целевых компьютерных атак на информационную инфраструктуру финансовых организаций в 2024 г. – чаще всего следствие эксплуатации уязвимостей перебором словарных паролей, нередко забытых подрядчиками при проведении работ по обновлению инфраструктуры и так далее.

ИТОГИ 2024 ГОДА

В настоящем разделе предлагается более подробно разобрать причинно-следственную связь компьютерных инцидентов, вызванных эксплуатацией уязвимостей и последствия подобных атак.

Как уже ранее отмечалось, ФинЦЕРТ регулярно информирует участников финансового рынка об атаках и угрозах, актуальных для организаций финансовой сферы. Так, в 2024 г. одной из основных причин КИ стала эксплуатация уязвимостей CVE-2021-4034 (уязвимость в polkit), CVE-2022-27228 (Bitrix).

По имеющимся сведениям, большинства инцидентов можно было избежать при своевременном принятии финансовыми организациями мер реагирования с целью парирования рисков воздействия на инфраструктуру, а также при выполнении рекомендаций ФинЦЕРТ из оперативных бюллетеней и информационных дайджестов (см. табл.).

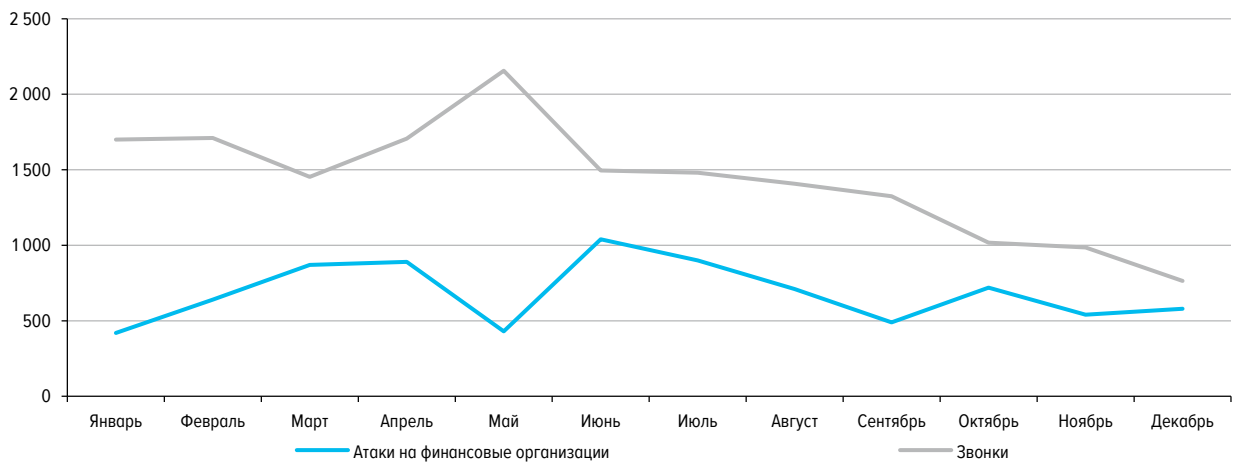
СВЕДЕНИЯ О БЮЛЛЕТЕНЯХ

Бюллетень	Дата публикации	Дата атаки, описанной в бюллетене (за 2024 год)	Временная разница между публикацией бюллетеня и атакой
Уязвимость в Bitrix (CVE-2021-4034)	7 июля 2024	22 июля 2024	Более 2 недель
Уязвимость в Bitrix (CVE-2022-27228)	29 мая 2023	9 марта 2024	Более 8 месяцев
Использование ПО GSocket	26 июля 2024	5 сентября 2024	Более 1 месяца

По результатам инцидентов были созданы условия, которые привели к утечке данных о клиентах скомпрометированных организаций, нарушению правильного функционирования технологических процессов и программно-технических комплексов; произведена подмена информации на сайтах.

Эффект от эксплуатации уязвимости злоумышленниками в инфраструктуре финансовой организации проявляется в течение следующих 2–3 месяцев в виде целевых атак на ее клиентов посредством использования похищенных данных клиентов и их средствах платежа (рис. 10).

КОРРЕЛЯЦИЯ АТАК НА ФИНАНСОВЫЕ ОРГАНИЗАЦИИ И КОЛИЧЕСТВА ОПЕРАЦИЙ БЕЗ ДОБРОВОЛЬНОГО СОГЛАСИЯ *Рис. 10*



Источник: данные Банка России.

В 2023 г. ФинЦЕРТ начал и в отчетном периоде продолжил активную работу по сбору и анализу информации об объектах информационной инфраструктуры, в том числе используемых центрах обработки данных, критических узлах технологических процессов, облачных вычислениях, процессинговых центрах и так далее.

В результате ФинЦЕРТ располагает актуальными данными об объектах ИИ. Они позволяют выявлять и анализировать информацию об угрозах для конкретных УИО или технологических инфраструктур и формировать рекомендации и перечни организационно-технических мер по реагированию на них.

Своевременная обработка сведений, получаемых от ФинЦЕРТ, – значимый бизнес-процесс, требующий учета со стороны финансовых организаций при ведении оперативной деятельности, наряду с другими ключевыми процессами, обеспечения информационной безопасности ИИ.

Практики мониторинга инцидентов операционной надежности

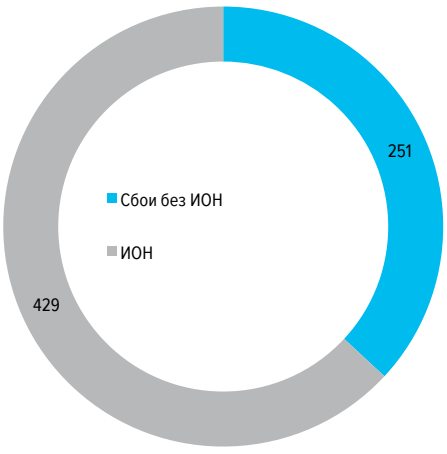
В 2024 г. ФинЦЕРТ в рамках мониторинга доступности услуг и сервисов, предоставляемых финансовыми организациями, выявил и направил в адрес участников финансовой сферы информацию более чем о 1500 событий, предположительно связанных со сбоями на различных технологических участках. 44% (680) выявленных событий были подтверждены финансовыми организациями как сбои в работе различных объектов ИИ. Инцидентами операционной надежности (ИОН) были определены 429 событий, что составляет 63% от общего объема выявленных сбоев.

В большей степени ИОН были связаны с ИТ-сбоями на объектах ИИ финансовых организаций (86,8%), при этом 13,2% таких инцидентов произошло в результате компьютерных атак, в частности DDoS-атак.

Работа онлайн-сервисов дистанционного обслуживания и доступ к осуществлению операций (47%), переводы денежных средств по поручению физических лиц по их банковским счетам (33%) – основные технологические процессы, на которые повлияли ИОН.

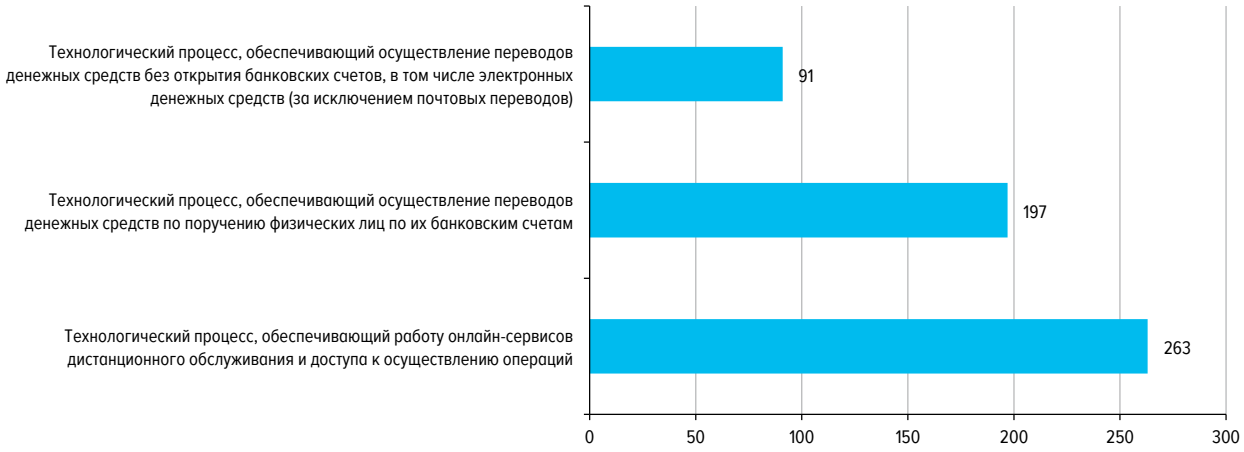
Самый крупный инцидент операционной надежности произошел в II квартале 2024 г. и составил 5 дней. Во время сбоя у финансовой организации наблюдались серьезные проблемы с обслуживанием клиентов, в том числе открытием продуктов, выдачей кредитов и так далее. Среднее время простоя сервисов в результате инцидента составило 5,6 часа.

ИНЦИДЕНТЫ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ *Рис. 11*



Источник: данные Банка России.

ТЕХНОЛОГИЧЕСКИЕ ПРОЦЕССЫ, ЧАЩЕ ВСЕГО ПОДВЕРГАВШИЕСЯ СБОЮ/НЕДОСТУПНОСТИ *Рис. 12*



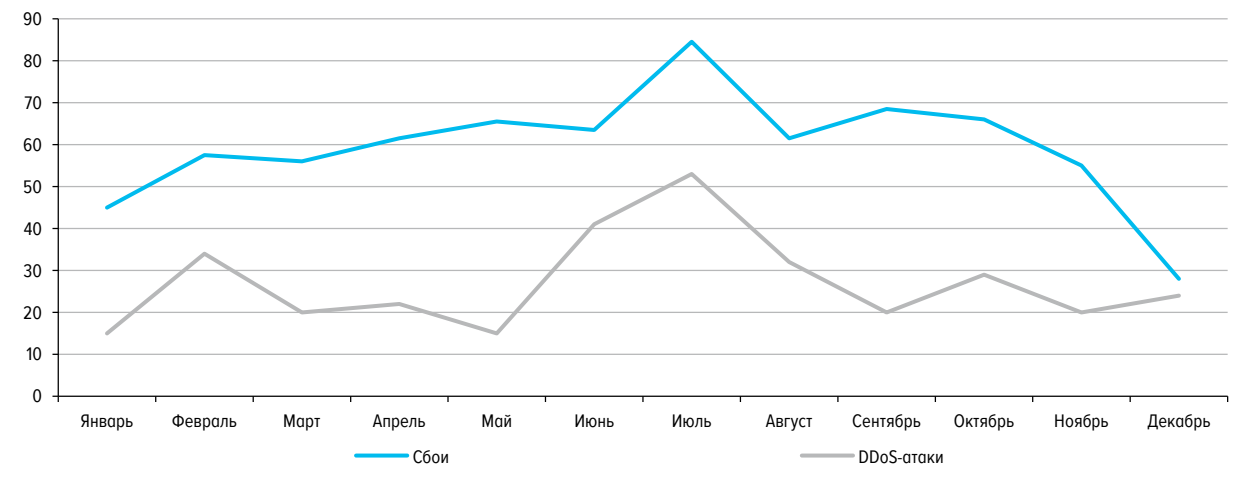
Источник: данные Банка России.

Отметим, что только в 8% случаях сбои были вызваны проведением атак на ИИ финансовых организаций. При этом взаимосвязь между событиями довольно высока. Таким образом, по косвенным признакам можно сделать вывод о прямой зависимости сбоев от КА, направленных на финансовые рынки.

Своевременное принятие мер по парированию возможных рисков возникновения сбоев, выхода из строя технологического оборудования на объектах ИИ, находящихся на критических технологических участках, позволит повысить уровень доступности услуг и сервисов, предоставляемых финансовыми организациями, и, как следствие, повысить доверие граждан к финансовым институтам.

При информировании ФинЦЕРТ о выявленных ИОН участники используют специальную форму, определенную стандартом Банка России СТО БР БФБО 1.5-2023. В ней участник указывает технологический процесс, объект, пострадавшие в результате ИОН, и причины инцидента.

КОРРЕЛЯЦИЯ СБОЕВ В ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ И КОМПЬЮТЕРНЫХ АТАК, НАПРАВЛЕННЫХ НА ФИНАНСОВЫЕ ОРГАНИЗАЦИИ *Рис. 13*



Источник: данные Банка России.

ФинЦЕРТ использует эту информацию в том числе для уведомления участников финансового рынка, имеющих схожие объекты информатизации о наличии проблем с оборудованием и/или ПО, для предупреждения рисков возникновения подобных ИОН у них.

Таким образом, своевременно актуализируя сведения по объектам информатизации, участники финансового рынка вносят весомый вклад в обеспечение стабильности предоставления услуг и сервисов финансовыми организациями на территории Российской Федерации.

Атаки на клиентов финансовых организаций

Последствиями успешных атак на коммерческие организации, обрабатывающие чувствительную информацию, являются утечки информации, используемой в дальнейшем для проведения целевых атак на граждан. Злоумышленники находят все более изощренные методы воздействия на выбранные цели, что неуклонно ведет к росту количества и объема хищений денежных средств у граждан.

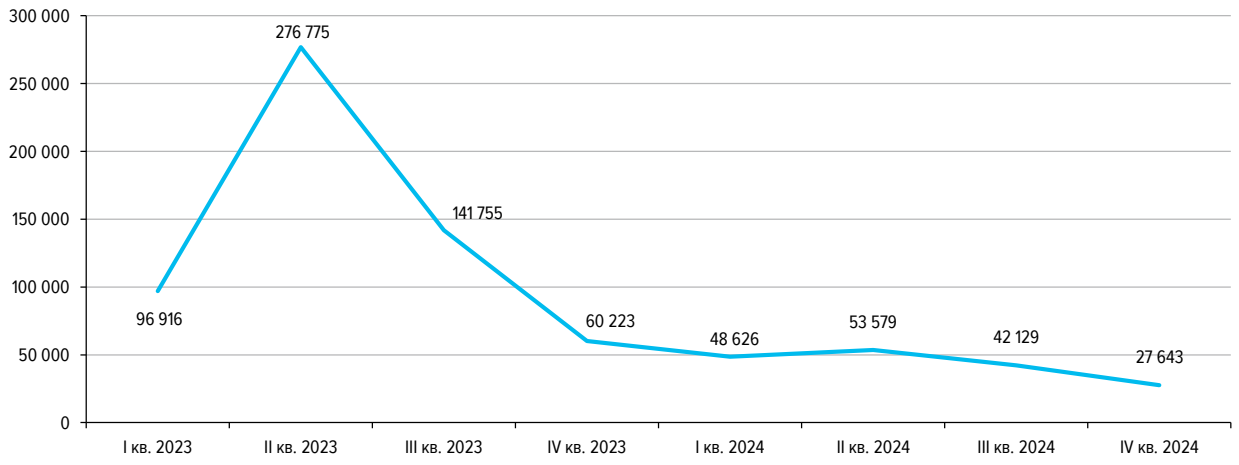
Противодействие атакам, в которых используются методы социальной инженерии, фишинга, требует совместных мер со стороны всех заинтересованных организаций.

ФинЦЕРТ отмечает снижение количества мошеннических звонков с использованием телефонной связи. Такое изменение сохраняется с середины предыдущего года (рис. 14).

Благодаря комплексному государственному регулированию и подходу в части обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования (ряд соответствующих изменений был внесен в течение 2023–2024 гг. в Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (Федеральный закон № 126-ФЗ), злоумышленникам становится все сложнее и дороже проводить массовые обзвоны граждан.

Так, начиная с 2023 г. все операторы связи должны проверять на достоверность сведения о проводимых вызовах при пропуске трафика через свои сети и прекращать оказывать услуги связи при выявлении нарушения соблюдения требований, установленных Федеральным законом № 126-ФЗ. Кроме того, в конце 2024 г. принято постановление Правительства Российской Федерации от 26.12.2024 № 1898 «О внесении изменений в некоторые акты Правительства Российской Федерации», ограничивающее возможности телефонного мошенничества.

КОЛИЧЕСТВО ТЕЛЕФОННЫХ НОМЕРОВ, НАПРАВЛЕННЫХ НА БЛОКИРОВКУ *Рис. 14*



Источник: данные Банка России.

Нормативный акт вносит изменения в перечень лицензируемых видов деятельности при оказании услуг связи. Так, из перечня лицензируемых видов деятельности исключаются пункты, связанные с услугами по передаче интернет-данных с наложением голосовой информации. Такой вид деятельности давал возможность с помощью Интернета выходить на связь с пользователем (организовывать телефонные звонки), использующим стационарную телефонную или мобильную связь.

Тем не менее проблема социальной инженерии продолжает оставаться одной из наиболее острых. На место классическим обзвонам с использованием телефонной связи пришли звонки через популярные мессенджеры.

Основные сценарии злоумышленников в 2024 г. можно разделить на тематические группы, представляющие собой целое направление воздействия:

1. Продление различных договоров

В этой группе сценариев можно выделить такие легенды, как:
– продление полиса обязательного медицинского страхования (ОМС) – мошенники представлялись работниками страховых компаний или медицинских организаций и сообщали, что нужно заменить полис ОМС;
– замена/продление договора на оказание услуг сотовой связи – злоумышленники выдавали себя за сотрудников компаний – операторов связи и сообщали, что договор на услуги связи необходимо незамедлительно продлить;
– истекший срок действия платежной банковской карты – аналогичные предыдущему сценарию звонки, менялась только должность и организация, которую представлял злоумышленник;
– полис каско или ОСАГО – повтор сценария с продлением полиса ОМС.

2. Звонки от имени служб безопасности финансовых организаций

Классическая схема продолжает оставаться актуальной. В 2024 г. были выявлены тенденции перехода злоумышленников от традиционного разговора «работника службы безопасности» на звонок от имени автоинформатора. После прохождения небольшого опроса по телефону происходило переключение на оператора или сотрудника правоохранительных органов.

3. Звонки из правоохранительных органов

Работая по этой схеме, мошенник представляется сотрудником МВД или федеральных служб, сообщает, что в отношении гражданина возбуждено уголовное дело или выявлен факт использования данных гражданина для хищения денежных средств и иных противоправных действий. Ему предлагают оказать содействие в поимке злоумышленников. В результате чаще всего у пострадавшего крадут кредитные (заемные) денежные средства, полученные им в финансовых учреждениях.

4. Государственные услуги, поддержка и компенсационные выплаты

Злоумышленники звонят и в зависимости от сценария сообщают о возможности получения социальных и иных выплат, участия в различных государственных и муниципальных программах поддержки, в волонтерских движениях, о необходимости проверки штрафов, проверки доступа к школьным электронным кабинетам и так далее.

В 2024 г. также были актуальны атаки на клиентов путем создания фишинговых сайтов, сайтов для ведения незаконной финансовой деятельности и так далее.

Так, за 2024 г. ФинЦЕРТ выявил и направил на блокировку более 46 000 доменов, которые использовались для проведения фишинговых атак, распространения информации о незаконной

ТИПЫ РЕСУРСОВ, ИСПОЛЬЗУЕМЫЕ ЗЛОУМЫШЛЕННИКАМИ *Рис. 15*

Источник: данные Банка России.

финансовой деятельности, а также деятельности финансовых пирамид. Это показатель превышает показатель 2023 г. на 20%.

Среди заблокированных ресурсов больше половины – фишинговые сайты (58%), копирующие название известных банков, инвестиционных компаний. Следующими по популярности идут финансовые пирамиды (23%). Чаще всего они маскируются под онлайн-игры, в которых при покупке персонажа или игровой атрибутики пользователю предлагают заработать до 1000% годовых. Остаются популярными и компании, осуществляющие безлицензионную деятельность на финансовом рынке. Их число составляет около 16% от общего объема заблокированных ресурсов.

Киберучения с представителями финансового рынка

В IV квартале 2024 г. ФинЦЕРТ организовал и провел киберучения с организациями финансовой сферы (далее – участники киберучений).

По результатам сканирования, было выявлено 3166 предполагаемых уязвимостей у 130 участников киберучений, что составляет 44% от общего количества участников этих мероприятий. Из общего количества выявленных уязвимостей 666 (21%) были высокими (с оценкой 7–8,9 по CVSS1) и 234 (7%) – критическими (с оценкой 9 и выше).

После проведенной рассылки практически все участники киберучений оперативно отреагировали на информацию, взяв в работу информацию о возможных уязвимостях на информационных ресурсах, находящихся в их ведении.

После проведения анализа информации об уязвимостях, направленной ФинЦЕРТ, участники реализовали соответствующие мероприятия по устранению уязвимостей и/или принятию компенсирующих мер.

В рамках второго этапа проведения киберучений с рядом финансовых организаций был отработан порядок направления заявления на приостановление обмена электронными сообщениями в платежных системах Банка России (ЭС в ПС БР).

На втором этапе проверялись знания финансовых работников о порядке приостановления обмена ЭС в ПС БР при выявлении несанкционированных операций в ПС БР, инициированных участником в результате возникновения инцидентов защиты информации при несоблюдении требований по обеспечению ИБ при осуществлении переводов денежных средств, а также актуальность перечня уполномоченных работников, информация о которых должна на регулярной основе обновляться финансовыми организациями по факту вносимых изменений.

Из 42 организаций у 8 (19%) выявлена неактуальная информация об уполномоченных на подписание и/или направление заявлений на приостановление обмена в ПС БР работниках, что в реальной ситуации может привести к существенным потерям при компрометации платежного контура ИИ участников ПС БР.

28 участников (67%) корректно заполнили заявление на приостановление / отмену приостановления обмена ЭС в ПС БР. При этом лишь 12 организаций справились с заданием и направили запрос на приостановление с первой попытки. Остальные участники направили корректную форму лишь со второй-пятой попытки. Как следствие, участники потеряли существенное количество времени на подготовку корректного заявления.

Остальные 14 участников не справились с заданием и не смогли подготовить корректное заявление, чтобы направить его в ФинЦЕРТ в установленные сроки проведения киберучений.

Всем участникам киберучений Банк России направил рекомендации по повышению защищенности ИИ, а также проведению необходимых работ по актуализации сведений в АСОИ ФинЦЕРТ.

Международное сотрудничество

Банк России в рамках международного сотрудничества в сфере ИБ и киберустойчивости в качестве ключевой цели определяет компетентное участие в формировании актуальной и отвечающей российским интересам повестки дня.

В соответствии с основными направлениями развития ИБ кредитно-финансовой сферы на 2023–2025 гг. в отчетный период ФинЦЕРТ продолжил развитие международного сотрудничества с национальными (центральными) банками, а именно:

1. **Осуществлял взаимодействие с центральными (национальными) банками иностранных государств по направлению информирования об актуальных угрозах ИБ с целью противодействия компьютерным атакам**

В рамках сотрудничества с центральными (национальными) банками стран – участниц Евразийского экономического союза (ЕАЭС), а также Таджикистана и Узбекистана ФинЦЕРТ направил более 470 бюллетеней с информацией о выявленных угрозах ИБ, включая индикаторы атак различных хакерских групп, атакующих организации финансовой сферы в юрисдикциях стран – участников ЕАЭС, Таджикистана и Узбекистана.

В период председательства Банка России в международном объединении БРИКС ФинЦЕРТ усилил работу по информированию центральных (национальных) банков объединения об актуальных угрозах ИБ путем направления бюллетеней в рамках специального канала по ИБ – BRICS Rapid Information Security Channel (Канал BRISC).

За 2024 г. было направлено 13 бюллетеней с информацией об актуальных КА и уязвимостях, выявленных ФинЦЕРТ.

2. Обеспечил участие экспертов Банка России в деятельности по направлению обмена лучшими практиками с целью гармонизации подходов к формированию требований по обеспечению ИБ и киберустойчивости, а также по повышению профессиональных навыков специалистов центральных (национальных) банков

В рамках мероприятий рабочей группы по вопросам обеспечения информационной безопасности финансового рынка и противодействия КА в кредитно-финансовой сфере, куда входят представители центральных (национальных) банков ЕАЭС, ФинЦЕРТ подготовил следующие документы:

– Рекомендации по ИБ при использовании технологии распределенного реестра, которые содержат описание типовых архитектур распределенных реестров, перечень возможных нарушителей, перечень специфичных угроз и меры, направленные на нейтрализацию этих угроз при использовании технологии распределенного реестра в банковском секторе.
– Регуляторный дайджест, который отражает основные изменения в области обеспечения ИБ в российском законодательстве.

По итогам взаимодействия внутри БРИКС при участии экспертов ФинЦЕРТ исследовал законодательство в сфере киберустойчивости финансового сектора стран объединения, а также лучшие практики в области анализа уязвимости и проведения тестирования на проникновение с последующей подготовкой 2 отчетов, а именно:
– Information Security Regulations in Finance, BRICS, 2024 (опубликовано на официальном сайте Банка России);
– Best Practices in Conducting Penetration Testing and Vulnerability Assessments of Information Infrastructure Facilities, 2024 (опубликовано на официальном сайте Банка России).

Содержание и ход работ над данными исследованиями регулярно обсуждались на встречах председателей центральных банков и министров финансов БРИКС, проходивших в 2024 г., в том числе на площадках Международного валютного фонда, Группы Всемирного банка, «Группы двадцати».

Дополнительно специалисты ФинЦЕРТ приняли участие в программе практико-ориентированного обучения по информационной безопасности Банка России «Киберкурс», в рамках которой поделились лучшими практиками реагирования на угрозы информационной безопасности с иностранными коллегами из стран – участниц ЕАЭС, БРИКС и представителями других государств в период проведения мероприятия в июне 2024 года.

3. Взаимодействовал с международными командами и группами реагирования на компьютерные инциденты государств – членов центральных (национальных) банков БРИКС с целью организации и проведения первых трансграничных киберучений

В III квартале 2024 г. ФинЦЕРТ организовал и провел первые трансграничные киберучения с представителями центральных банков стран БРИКС.

Киберучения проходили в 2 этапа. Первый, дистанционный, прошел в начале августа 2024 года. На этом этапе отрабатывалось взаимодействие участников в части обмена информацией о выявленной угрозе ИБ с использованием бюллетеней, подготовленных в соответствии с утвержденным форматом Канала BRISC.

Второй этап был проведен очно в период с 16.09.2024 по 19.09.2024 на площадке Университета Иннополис (Республика Татарстан). Участники на практике отрабатывали навыки реагирования на компьютерные атаки, использования различных средств их обнаружения, поиска следов злоумышленников (индикаторов компрометации) и ликвидации последствий атак.

По результатам киберучений участниками были приняты рассмотрены следующие перспективные направления развития Канала BRISC:

– Проведение киберучений БРИКС на ежегодной основе с целью расширения практики взаимодействия и обеспечения готовности Канала BRISC для противодействия актуальным угрозам информационной безопасности.
– Внедрение Канала BRISC и наполнение его новыми данными и практиками, нацеленными на повышение уровня обеспечения ИБ финансовой сферы стран – участниц БРИКС.
– Развитие трансграничной безопасности платежных инструментов, используемых гражданами стран БРИКС и повышение уровня доверия к данным инструментам.

По итогам 2 этапов киберучений представители стран БРИКС дали высокую оценку организации мероприятий, выразив надежду на углубление сотрудничества в рамках совместной работы по обеспечению ИБ финансовых секторов стран объединения.

В 2025 г. ФинЦЕРТ продолжит развивать практику проведения киберучения среди национальных (центральных) банков стран – участников межгосударственных союзов[1]. Основными направлениями взаимодействия будут:

– повышение качества и скорости взаимодействия между национальными (центральными) банками;
– практическая отработка действий национальных (центральных) банков по выявлению, идентификации и реагированию на операционные риски, причинами которых являются компьютерные атаки.

[1] ЕАЭС, АСЕАН, ШОС.

НАПРАВЛЕНИЯ ВЗАИМОДЕЙСТВИЯ ФИНЦЕРТ В 2025 ГОДУ

В 2024 г. завершены работы в рамках созданной рабочей группы по организации обмена машиночитаемым бюллетеням между участниками взаимодействия ФинЦЕРТ.

В результате проведенной работы ФинЦЕРТ сформировал и организовал публикацию на ежедневной основе машиночитаемых бюллетеней в 6 форматах, адаптированных для непосредственной загрузки в средства мониторинга и обеспечения ИБ.

На текущий момент ФинЦЕРТ продолжает улучшать публикуемые бюллетени с индикаторами компрометации, увеличивая количество поставщиков сведений о КА и дорабатывая формат публикуемых сведений.

В 2025 г. ФинЦЕРТ планирует разделить публикуемую информацию на отдельные группы по каждому типу индикатора компрометации, связывая их через единый ключ – идентификатор события.

Подобный подход позволит УИО собрать весь необходимый объем информации по КА по любому из индикаторов обнаружения в автоматическом или ручном режиме.

Появится возможность загружать индикаторы обнаружения непосредственно на конкретные средства защиты и мониторинга ИБ, удобно применять правила и коррелировать события на стороне участников информационного обмена без использования дополнительных мер по выделению отдельных типов индикаторов.

В 2025 г. на стороне ФинЦЕРТ запланированы работы по созданию единой базы индикаторов КА, доступ к которой позволит участникам видеть все исторические записи по всем индикаторам КА, публикуемых ФинЦЕРТ.

Своевременная актуализация со стороны участников финансовой сферы сведений по IP-адресам, доменным именам, URL-адресам, используемым в операционной деятельности, позволит ФинЦЕРТ повысить эффективность выявления подозрительной активности, предположительно связанной с КИ, и обеспечить информирование всех участников информацией.

ТЕНДЕНЦИИ 2025 ГОДА

Анализ уровня текущей информационной безопасности позволяет выделить ключевые тренды, которые вероятнее всего будут определять характер кибератак в 2025 году.

Рост атак через цепочку поставщиков

Одним из ключевых трендов в кибератаках будет увеличение числа атак через цепочку поставщиков. Это явление обусловлено отсутствием конкретных требований к уровню ИБ поставщиков ИТ-решений, предъявляемых со стороны заказчиков. Злоумышленники все чаще используют уязвимости в продуктах или инфраструктуре поставщиков для компрометации более крупных организаций. Этот подход позволяет атакующим обойти традиционные меры защиты, эксплуатируя доверительные отношения между компаниями и их подрядчиками.

Смещение фокуса на малые и средние организации

Злоумышленники продолжают адаптировать свои тактики, фокусируясь на компаниях, которые имеют ограниченные ресурсы для обеспечения ИБ. Малые и средние организации становятся основной мишенью по следующим причинам:

- **слабая защита:** ограниченные бюджеты на технические и организационные меры обеспечения ИБ не позволяют внедрять продвинутые системы мониторинга и предотвращения угроз, а также организации должного операционного контроля мер безопасности;
- **недостаток опыта и ресурсов:** небольшие компании часто имеют ограниченные возможности для выделения подготовленного персонала для управления ИБ и реагирования на инциденты либо опыта в качественной организации и сопровождения таких работ по сервис-контрактам;
- **удобство компрометации:** типовые атаки (фишинг, перебор паролей, эксплуатация устаревших или неправильно настроенных систем) особенно эффективны против малых организаций.

Особенно уязвимы небольшие **региональные компании** либо дочерние подразделения крупных компаний. У них ниже уровень осведомленности о современных киберугрозах, а операционный контроль мер ИБ может быть не гармонизирован в рамках общей стратегии ИБ. Такие компании инвестируют в кибербезопасность либо недостаточно, либо не придерживаясь общего риск-ориентированного подхода, и становятся легкой добычей для атакующих.

Усиление тренда на деструктивное воздействие кибератак

1. Рост репутационно-ориентированных атак: ожидается увеличение атак, нацеленных на подрыв доверия к организациям. П**рогнозируются у**течки данных, манипуляции с корпоративными системами и публикация данных, вызывающих общественное недоверие (например, компрометация финансовой отчетности).

2. Эволюция атак с использованием Ransomware[1]**.** В 2025 г. Ransomware останется одной из главных угроз, но с новым акцентом:

- **деструктивное вымогательство:** вместо шифрования данных злоумышленники могут удалять их, используя угрозу полного уничтожения как рычаг давления;

[1] Ransomware – программа-вымогатель.

– **усложнение атак:** с учетом утечки исходного кода ряда шифровальщиков, в том числе Babuk, Conti и LockBit 3 (Black), прогнозируется появление новых, более сложных и разрушительных модификаций Ransomware, разработанных даже небольшими группами злоумышленников с низким уровнем подготовки.

3. Усиление шифровальщиков как сервиса (RaaS): утечка исходных кодов в 2024 г. приведет к усложнению экосистемы Ransomware. Более продвинутые версии программ будут распространяться через платформы как сервис, где злоумышленники смогут арендовать инструменты для атаки, минимизируя собственные затраты на разработку.

Трудности с обнаружением и атрибуцией

Злоумышленники активно используют сложные цепочки промежуточных узлов, таких как скомпрометированные серверы, VPN и мобильные прокси, для маскировки атак. Это затрудняет следующие процессы:

– **детектирование атак:** злоумышленники мимикрируют под легитимный пользовательский трафик, разделяют во времени этапы атакующего воздействия, используют разнородные векторы атак;

– **атрибуцию:** цепочка из российских адресов, мобильных ASN, а также использование средств туннелирования трафика не позволяет выявлять истинного инициатора атаки.

Более того, компании со сложной организационной структурой, обширным парком ИТ-активов, на которые будет направлен основной поток атак, зачастую не располагают инструментами мониторинга для выявления сложных схем компьютерных атак и соответствующим опытом противодействия им.

Рост атак с долгосрочным присутствием (dwell time)

Одна из ключевых тактик, ожидаемых в 2025 г., – увеличение времени незаметного присутствия злоумышленников в системах. Цели этого подхода:

– **сбор информации об инфраструктуре:** злоумышленники будут оставаться в системах как можно дольше, чтобы изучить сетевую инфраструктуру системы, определить технические характеристики средств защиты информации и выявить слабые места всей инфраструктуры в целом;

– **отложенная эксплуатация:** Backdoor и закладки, которые оставляют злоумышленники, будут использоваться спустя месяцы или даже годы после первоначальной компрометации.

Такой подход особенно эффективен против компаний, не проводящих регулярного аудита информационной безопасности компьютерных систем.

РЕКОМЕНДАЦИИ ДЛЯ ПОДГОТОВКИ К УГРОЗАМ 2025 ГОДА

Малым и средним организациям, включая региональные компании, следует:

– инвестировать в базовые системы мониторинга и защиты; внедрить системы мониторинга событий безопасности (EDR / антивирусные решения с централизованным управлением);
– усилить обучение персонала, особенно в вопросах противодействия фишингу;
– проводить регулярные аудиты информационной безопасности, привлекать сертифицированных специалистов для проверки защиты периметра, конфигураций сетей и серверов.

Атаки на цепочку поставок требуют повышенного внимания к подрядчикам и партнерам, поэтому необходимо:

– оценивать уровень зрелости процессов ИБ у поставщиков;
– убедиться, что подрядчики используют защищенные каналы связи и обновляют ПО;
– устанавливать строгие правила доступа к внутренним системам для внешних партнеров;
– использовать изолированные среды для работы с данными, полученными от подрядчиков.

Для противодействия атакам с российских IP-адресов надлежит:

– внедрить поведенческую аналитику на основе репутации источника для выявления сетевых аномалий;
– ограничить доступ пользователей и сервисов из сети общего назначения к критически важным сегментам.

Для защиты от долгосрочного присутствия требуется:

– регулярно проводить аудит информационных активов;
– регулярно проводить киберучения как для операционного персонала организации, так и для соответствующих служб ИБ;
– проводить регулярный анализ систем на наличие Backdoor и вредоносного ПО, а также постинцидентный анализ компьютерных систем.

Для противостояния атакам с использованием шифровальщиков следует:

– изолировать резервные копии и проводить регулярное тестирование их восстановления;
– настроить централизованное управление обновлениями для устранения уязвимостей;
– внедрить многофакторную аутентификацию и ограничить доступ к критически важным данным.