ПО ДАННЫМ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Компьютерные атаки остаются одним из ключевых операционных и финансовых рисков для бизнеса по всему миру. В 2025 году их влияние проявилось в полной мере: от масштабных парализующих атак на критическую инфраструктуру до приводящих к многомиллионным убыткам целенаправленных операций против коммерческих компаний. Киберпреступность сегодня — высокоорганизованный бизнес с чёткой направленностью, где вредоносное программное обеспечение, эксплуатация уязвимостей и методы социальной инженерии используются как инструменты для финансового обогащения, шпионажа, дестабилизации или достижения иных целей.

В этом контексте в случае успешной компьютерной атаки на организацию многократно возрастает причинённый ей ущерб, складываясь не только из прямых финансовых потерь (выплаты вымогателям, штрафы регуляторов, затраты на восстановление), но и ущерба для репутации, потери доверия заказчиков либо утраты конкурентных преимуществ. Сегодня возросло и количество инцидентов, когда злоумышленники длительное время находились внутри системы до того, как были обнаружены, и исходящая от них угроза была нейтрализована.

На этом фоне услуги круглосуточного мониторинга и реагирования на инциденты перешли из категории «желательных» в категорию «необходимых» для обеспечения устойчивости функционирования организации. Способность не только предотвращать и анализировать причины возникновения негативных последствий, но и оперативно обнаруживать и ликвидировать последствия атак в режиме реального времени становится критически важным компонентом корпоративной защиты организации.

В данном отчёте приведена статистика об инцидентах в коммерческом и государственном секторах, выявленных командой центра мониторинга информационной безопасности АО «ПМ» в 2024 и 2025 годах, предназначенная для выработки превентивных мер по укреплению защищённости организаций.

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

ПО — программное обеспечение

ВПО — вредоносное программное обеспечение

ИР — информационные ресурсы

КИ — компьютерный инцидент

КА — компьютерная атака

НСД — несанкционированный доступ

ОС — операционная система

ИБ — информационная безопасность

ЗИ — защита информации

SOC — Security Operation Center

Событие ИБ — зафиксированное состояние информационной (автоматизированной) системы, сетевого, телекоммуникационного, коммуникационного, иного прикладного сервиса или сети, указывающее на возможное нарушение безопасности информации, сбой средств ЗИ или ситуацию, которая может быть значимой для безопасности информации.

Инцидент ИБ — это событие, которое может нанести ущерб конфиденциальности, целостности или доступности информационных ресурсов организации. Инцидент может включать в себя несанкционированный доступ, утечку данных, повреждение систем, использование вредоносного ПО, а также любые действия, которые нарушают установленные политики безопасности или могут угрожать защищённости информационных систем.

Классификация инцидентов позволяет эффективно управлять рисками и реагировать на угрозы. Инциденты могут быть классифицированы по следующим уровням критичности:

- Низкий уровень критичности — инцидент вызывает незначительные перебои в работе организации.
- Средний уровень критичности — инцидент может вызвать умеренные перерывы в работе организации при некритичных финансовых и юридических последствиях.
- Высокий уровень критичности — инцидент может оказать значительное влияние на безопасность компьютеров и корпоративную локальную сеть.
- Критический инцидент — содержит сведения, которые могут оказать критическое влияние на технологический процесс и требуют немедленной реакции.

РЕЗУЛЬТАТЫ МОНИТОРИНГА

В 2025 году командой центра мониторинга информационной безопасности «Перспективного мониторинга» зарегистрировано и обработано 6 326 инцидентов информационной безопасности, что на 45,2% превышает показатель 2024 года. Данная динамика свидетельствует как о высокой эффективности процессов мониторинга и детектирования в команде SOC ПМ, позволяющих выявлять угрозы в масштабируемой инфраструктуре, так и о повышении активности злоумышленников в отношении информационных систем заказчиков.

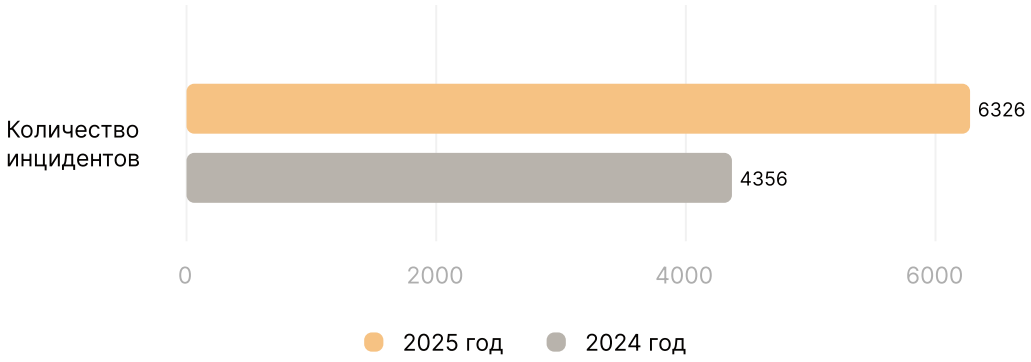


Рисунок 1 — зарегистрированные инциденты ИБ

Наибольший рост зафиксирован среди инцидентов низкого и среднего уровней критичности. Инциденты высокого уровня критичности демонстрируют уже менее интенсивный рост, который составил 24,4%, а среди критических инцидентов наблюдается снижение на 40,5%.

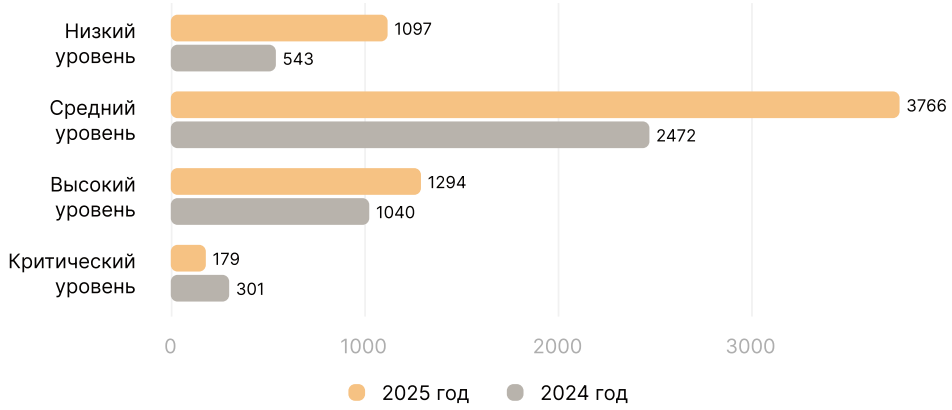


Рисунок 2 — статистика инцидентов с разделением по уровням критичности

При рассмотрении статистики по типам инцидентов лидирующую позицию занимает заражение ВПО. Наиболее часто ВПО применяется при КА, позволяя злоумышленникам проникнуть в систему, закрепиться, повысить привилегии и совершить другие действия в среде заказчика, что является одной из причин его широкого распространения. В 2025 году был зафиксирован рост числа КИ с использованием ВПО на 17,2%.

На втором месте по количеству КИ находится сетевое сканирование — один из элементов КА, в ходе которого злоумышленники осуществляют разведку и собирают важную для них информацию. Такой разведкой может быть, например, сканирование активных устройств или открытых портов. В 2025 году число инцидентов, связанных с сетевым сканированием, выросло на 21,7%.

На третьем месте по количеству инцидентов — попытки эксплуатации различных уязвимостей, вызванных неверными конфигурациями устройств или сети и использованием устаревшего ПО. За 2025 год было зарегистрировано увеличение КИ, связанных с попытками эксплуатации уязвимостей, на 112,3%.

Также наблюдается рост количества инцидентов, связанных с нарушением политик информационной безопасности. К их числу относятся использование прикладного ПО для удалённого управления устройствами, размещение в явном виде чувствительной информации, доступность панелей авторизации и т. д. Рост числа таких инцидентов за 2025 год составил 8,5%.

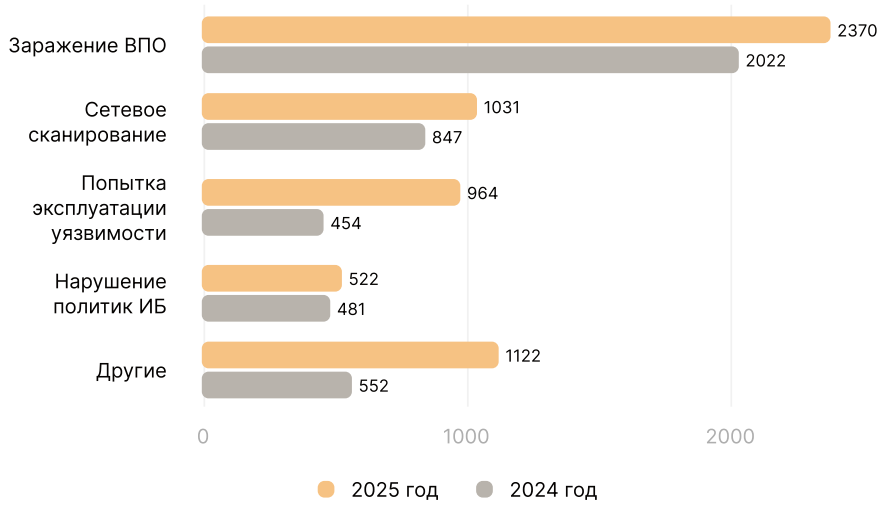


Рисунок 3 — статистика инцидентов с разделением по видам

В ходе анализа КИ, зафиксированных в 2024 и 2025 годах, была выявлена чёткая картина разделения определённых категорий ВПО.

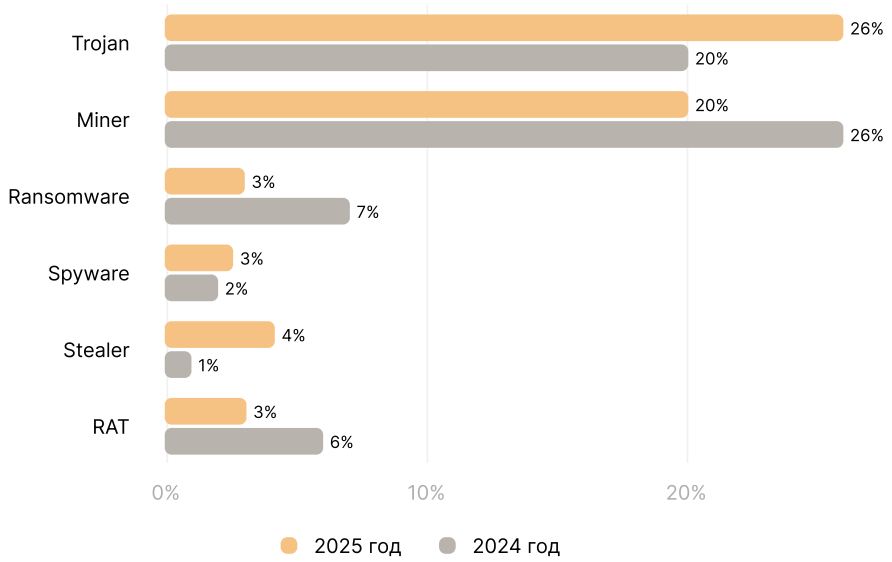


Рисунок 4 — наиболее часто встречающиеся типы ВПО

Троянские программы (Trojan). Данный тип ВПО продемонстрировал наибольшую активность, став причиной каждого четвёртого инцидента. Общая доля заражений данным типом ВПО в 2025 году составила 26% от общего числа зафиксированных инцидентов против 20% в 2024 году, что позволяет выделить их как наиболее распространённую и значимую угрозу информационной безопасности.

Высокий процент объясняется использованием их в качестве основного вектора атаки и широким спектром деструктивных функций.

Майнеры криптовалюты (Miner). На втором месте по частоте обнаружения в 2025 году находятся майнеры криптовалюты. Инциденты, связанные с этим типом ВПО, составили 20% от общего числа, формируя вторую по величине группу угроз, при этом по сравнению с 2024 годом их число уменьшилось на 6%.

Распространённость такого ВПО обусловлена прямой финансовой мотивацией злоумышленников, которые используют вычислительные ресурсы организации для скрытого майнинга, что приводит к потере производительности, повышенному износу оборудования и росту затрат на электроэнергию.

Отдельно стоит выделить некоторые категории ВПО, которые занимают меньшую долю среди всего обнаруженного ВПО, но при этом представляют собой существенный риск для функционирования организаций.

Стилеры (Stealers). В 2024 году стилеры составляли 1% от общего числа инцидентов, связанных с ВПО, в 2025 году фиксируется рост числа КИ с использованием стилеров до 4%. Их использование направлено на похищение конфиденциальных данных (учётные записи, данные браузеров, ключи и т. д.).

Шифровальщики (Ransomware). В 2024 году общее число КИ с использованием шифровальщиков составило 7%, в 2025 году — 3%. Однако, несмотря на относительно низкую частоту, шифровальщики представляют собой угрозу, которая несет высокие операционные и финансовые риски для организации.

Троянские программы удалённого доступа (Remote Access Trojan). За 2024 год специалистами SOC ПМ было зафиксировано 6% КИ с использованием данного типа ВПО, в 2025 году их доля в общем количестве инцидентов снизилась до 3%. Данный тип ВПО обеспечивает злоумышленникам полный удалённый контроль над заражённой системой.

Шпионское ПО (Spyware). Основная задача этого типа ВПО — максимально долго и скрытно находиться в системе и собирать конфиденциальные данные. В 2025 доля обнаруженного шпионского ВПО составила 3% от общего числа КИ, в 2024 году данный показатель составлял 2%. Несмотря на небольшой рост количества инцидентов, связанных с данным типом ВПО, ущерб от него может оказаться значительным.

Помимо угроз, связанных с распространением ВПО, 15,2% инцидентов вызваны попытками эксплуатации уязвимостей. Специалисты «Перспективного мониторинга» зафиксировали 3 наиболее распространённых типа эксплуатируемых уязвимостей.

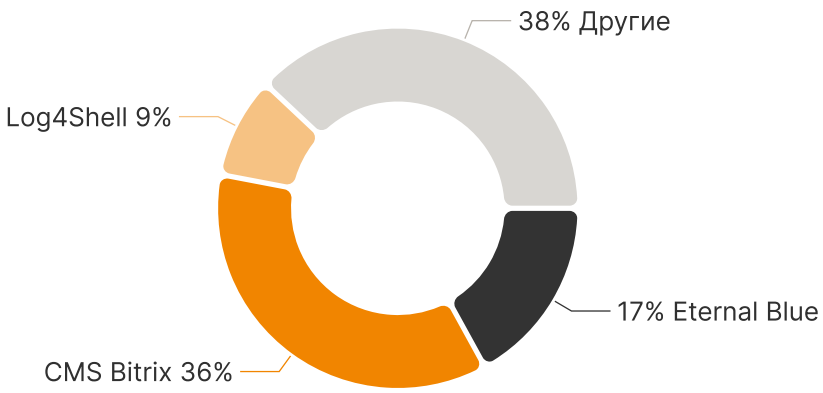


Рисунок 5 — инциденты, связанные с эксплуатацией уязвимостей

Большинство инцидентов с долей в 36% составили уязвимости, связанные с CMS Bitrix.

В 17% случаев были зафиксированы попытки эксплуатации уязвимости EternalBlue, связанной с ВПО WannaCry. Данная уязвимость была закрыта специально выпущенными обновлениями для операционных систем, однако злоумышленники не перестают эксплуатировать старые уязвимости, зная, что не везде установлены соответствующие обновления.

Также в 9% инцидентов были зафиксированы попытки использования уязвимости CVE-2021-44228 (также известна как Log4Shell или LogJam).

Несмотря на большое число попыток эксплуатации уязвимостей, количество успешных эксплуатаций уязвимостей среди заказчиков SOC ПМ в 2025 году составило 3 случая против 13 в 2024 году. Среди причин кратного снижения успешных эксплуатаций — оперативное принятие мер реагирования, выработанных SOC.

Важный аспект при рассмотрении деятельности специалистов по мониторингу — среднее время реагирования на инциденты информационной безопасности. Для расчёта временных метрик измерялось среднее время, затраченное специалистами на различных этапах реагирования на инцидент с разделением на кварталы за 2024 и 2025 годы. Однако стоит учитывать, что время реагирования на инцидент с момента открытия инцидента до его закрытия зависит от того, насколько быстро и эффективно осуществляется обратная связь с заказчиком, времени реализации ответственными специалистами рекомендаций, полученных от экспертов SOC.

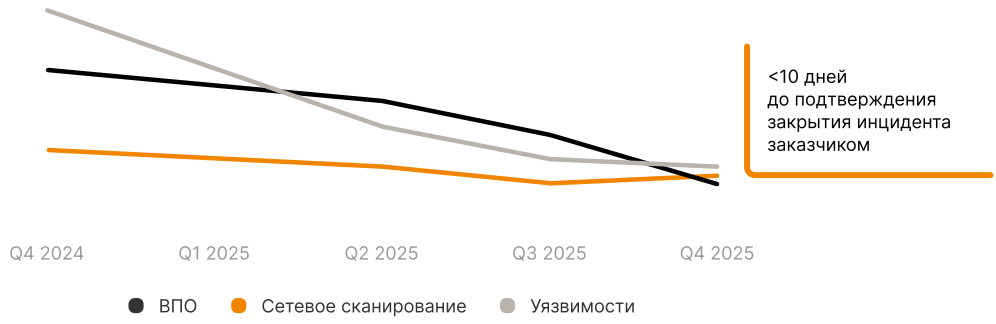
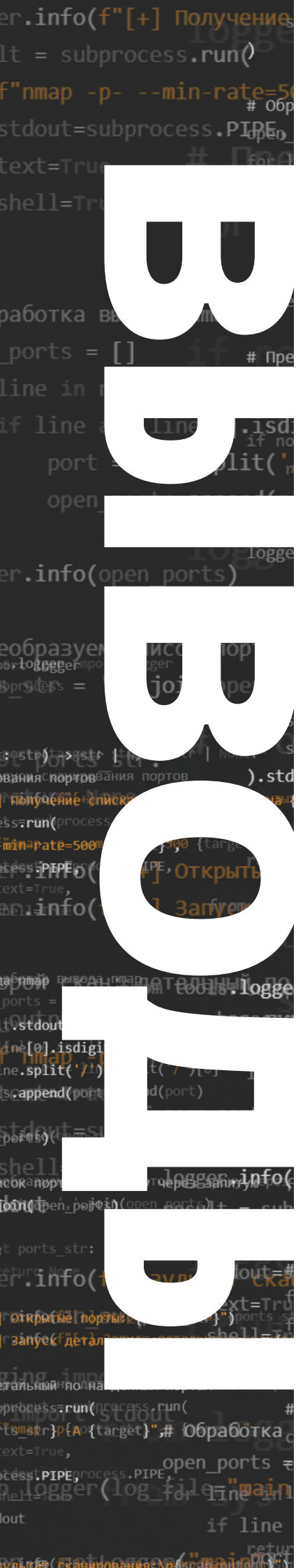


Рисунок 6 — время расследования инцидента

Приведённый ниже график демонстрирует устойчивую тенденцию снижения среднего времени, затраченного на расследование одного инцидента, с разделением на инциденты, связанные с ВПО, сетевым сканированием и уязвимостями.

Такая тенденция стала возможной благодаря постоянной оптимизации процессов взаимодействия с заказчиками, а также своевременному внедрению заказчиками рекомендаций, выработанных специалистами «Перспективного мониторинга» по каждому конкретному случаю.



ВЫВОДЫ

МАСШТАБИРОВАНИЕ И ЭФФЕКТИВНОСТЬ

Несмотря на значительный рост числа компьютерных инцидентов, скорость реагирования на них возросла. Это связано с ростом эффективности взаимодействия и повышением оперативности выполнения рекомендаций специалистами заказчиков.

ИЗМЕНЕНИЕ ПРОФИЛЯ УГРОЗ

Наблюдается уход от массовых атак к более направленным и опасным действиям. Это демонстрирует резкое увеличение (+112,3%) попыток эксплуатации уязвимостей и рост числа сложных киберугроз, таких как использование троянских программ (+6%) и стилеров (рост с 1% до 4%).

Наиболее значимым достижением является снижение на 40,5% числа инцидентов критического уровня, а также резкое сокращение успешных эксплуатаций уязвимостей (с 13 в 2024 году до 3 в 2025 году), несмотря на рост числа попыток их эксплуатации. Последнее указывает на высокую эффективность предпринятых превентивных мер и рекомендаций, предоставленных заказчикам.

ОСНОВНЫЕ УГРОЗЫ

Абсолютный лидер по количеству инцидентов — ВПО. Троянские программы стали инструментом № 1 (26% от общего числа инцидентов), что подчеркивает их роль как ключевого вектора для закрепления в инфраструктуре.

Наиболее динамично растущий вектор атаки — это эксплуатация уязвимостей. Основные цели — уязвимости в CMS Bitrix (36%), до сих пор актуальные уязвимости (EternalBlue — 17%) и критические уязвимости в популярных компонентах (Log4Shell — 9%).

Также высокий рост (+21,7%) инцидентов сетевого сканирования подтверждает, что злоумышленники активно проводят подготовку к более серьёзным атакам.

На основании выявленных тенденций, статистики инцидентов и анализа актуальных векторов атак специалисты SOC ПМ рекомендуют реализовать следующие меры по повышению уровня информационной безопасности:

УСИЛЕНИЕ ВОЗМОЖНОСТИ ОБНАРУЖЕНИЯ

С учётом преобладания троянских программ в структуре выявленного ВПО рекомендуется усилить возможности обнаружения аномальной активности пользователей и систем, не выявляемой сигнатурными методами. Для этого целесообразно использовать поведенческие механизмы защиты, включая контроль подозрительных процессов, механизмов закрепления в системе и нетипичной сетевой активности. Особое внимание следует уделять обработке инцидентов с низкой критичностью, так как они могут являться признаком скрытого присутствия злоумышленника.

ДОПОЛНИТЕЛЬНОЕ ОБУЧЕНИЕ

В связи с тем, что основной вектор проникновения ВПО связан с фишинговыми атаками, рекомендуется дополнительное обучение сотрудников заказчиков методам противодействия социальной инженерии. Обучение должно включать регулярные тренировки с имитацией фишинговых рассылок, разбор типовых сценариев атак и анализ допущенных ошибок. Дополнительно рекомендуется внедрение технических мер защиты почтовых систем.

РЕГУЛЯРНОЕ ОБНОВЛЕНИЕ ПО

Рекомендуется проводить регулярное обновление эксплуатируемого ПО с целью своевременного закрытия выявляемых уязвимостей. Организациям, использующим платформу Bitrix, необходимо обновить ПО до актуальных версий, а также провести аудит конфигурации и настроек безопасности веб-приложений.

ПОИСК И ОБНОВЛЕНИЕ СИСТЕМ

Рекомендуется регулярно проводить поиск и обновление систем, уязвимых к актуальным критическим уязвимостям, включая EternalBlue (MS17-010) и Log4Shell. Несмотря на давность исправлений, данные векторы по-прежнему активно используются злоумышленниками для первичного проникновения и развития атаки.

РЕГЛАМЕНТ РЕГУЛЯРНОГО ОБНОВЛЕНИЯ

Рекомендуется внедрить регламент регулярного обновления программного обеспечения с приоритизацией уязвимостей на основании данных SOC о фактической эксплуатации уязвимостей в атаках. Такой подход позволит сосредоточить усилия на закрытии наиболее актуальных рисков, а не формально оценивать уязвимости только по уровню критичности.

УСИЛЕНИЕ МОНИТОРИНГА И РЕАГИРОВАНИЯ

Рекомендуется усилить мониторинг и реагирование на попытки сетевого сканирования и разведки ИТ-инфраструктуры. Для этого требуется внедрять механизмы выявления источников сканирования, их автоматической блокировки и раннего обнаружения злоумышленников на подготовительной стадии компьютерной атаки.

АВТОМАТИЗАЦИЯ И СТАНДАРТИЗАЦИЯ

Для сокращения времени реагирования на инциденты рекомендуется автоматизировать и стандартизировать процессы взаимодействия между специалистами внешнего SOC и сотрудниками заказчика. Для этого необходимо регламентировать сценарии взаимодействия на всех этапах обработки инцидента.

РЕГУЛЯРНЫЕ ТРЕНИРОВКИ

Рекомендуется регулярно проводить тренировки по реагированию на инциденты информационной безопасности на основе типовых сценариев, выявляемых SOC. Проведение таких мероприятий позволит сократить общее время реагирования и минимизировать последствия инцидентов.

ФОРМИРОВАНИЕ ПЕРЕЧНЯ ИСПОЛНИТЕЛЕЙ

С учётом роста числа сложных и целевых атак рекомендуется сформировать план реагирования на инциденты с исполнителями, обладающими компетенциями в области глубокого анализа инцидентов, восстановления цепочек атак и расследования сложных компрометаций.

SOC MARKET

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

«Перспективный мониторинг» — один из лидеров российского рынка коммерческих SOC, исследований защищённости и расследования инцидентов, а также разработчик собственных продуктов в области информационной безопасности.

Компания более 10 лет оказывает услуги центра мониторинга информационной безопасности и коммерческого центра ГосСОПКА. SOC ПМ аккумулирует в себе знания о киберугрозах от всех направлений деятельности компании, выстраивая надёжную защиту от компьютерных атак.

Среди заказчиков — крупные государственные и коммерческие организации. В штате компании — 150 квалифицированных специалистов, работающих в нескольких подразделениях по всей стране, что позволяет оказывать услуги мониторинга 24/7/365 в одном часовом поясе с заказчиком.

УСЛУГИ SOC АО «ПМ»

- Мониторинг событий 24/7/365
- Мобильная группа быстрого реагирования
- Услуги центра ГосСОПКА класса А
- Compromise Assessment
- Мониторинг АСУ ТП
- Расследование инцидентов
- Экспертная (3-я) линия SOC
- Тестирование на проникновение информационных систем
- Сопровождение SIEM
- OSINT

ПРОДУКТЫ

AML — AML Web Protection для защиты веб-ресурсов от компьютерных атак на основе поведенческого анализа логов

AMPIRE — Киберполигон Ampire для регулярных тренировок по противодействию компьютерным атакам

AMTIP — AM Threat Intelligence Portal для получения актуальных сведений о компьютерных угрозах