Ганхуяг Батсайд , студент,
Краснодарское высшее военное училище

Кубенко Егор Георгиевич, Старший преподаватель,
Краснодарское высшее военное училище

Шеин Сергей Леонидович, Преподаватель,
Краснодарское высшее военное училище

РАЗРАБОТКА И ОБОСНОВАНИЕ КОМПЛЕКСА МЕРОПРИЯТИЙ ПО СНИЖЕНИЮ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Аннотация. В статье рассматривается системный подход к построению защиты информации на основе риск-ориентированной методологии. Представлен комплекс организационных, технических и управленческих мер, направленных на снижение вероятности реализации актуальных угроз. Особое внимание уделяется принципу эшелонированной защиты («защита в глубину»), автоматизации процессов реагирования на инциденты, а также внедрению современных технологий, таких как NGFW, EDR, PAM, SIEM и SOAR.

Ключевые слова: Информационная безопасность, угрозы, эшелонированная защита, организационные меры, технические средства защиты, SIEM, PAM, реагирование на инциденты, управление доступом.

Современный этап развития информационных технологий характеризуется не только ростом производительности и доступности сервисов, но и качественным усложнением ландшафта угроз безопасности информации. Кибератаки становятся целенаправленными, автоматизированными и многоступенчатыми. В этих условиях фрагментарное внедрение отдельных средств защиты - антивирусов, межсетевых экранов или систем обнаружения вторжений - перестаёт быть достаточным. Практика показывает, что большинство инцидентов происходит не из-за отсутствия технических средств, а вследствие системных проблем: человеческого фактора, неэффективных процессов управления доступом, отсутствия координации между средствами защиты.

В связи с этим особую актуальность приобретает разработка и обоснование комплексных мероприятий по снижению вероятности реализации угроз, охватывающих организационно-распорядительный, технический и управленческий уровни. Настоящая статья посвящена именно такому комплексному подходу, базирующемуся на принципе эшелонированной защиты («защита в глубину»), при котором отказ или преодоление одного рубежа обороны не приводит к компрометации всей системы.

1.Организационно-распорядительные меры как фундамент защиты.

Организационные меры нередко недооцениваются, хотя именно они формируют основу любой системы защиты информации, поскольку большинство инцидентов связано с человеческим фактором: ошибками персонала, нарушением регламентов, недостаточной квалификацией или злонамеренными действиями. Без правильно выстроенной нормативной базы и культуры безопасности даже самые дорогие технические средства оказываются малоэффективными.

Первым шагом является приведение нормативной базы в соответствие с актуальными требованиями. Для конкретного объекта информатизации разрабатываются следующие ключевые документы:

Политика информационной безопасности – документ верхнего уровня, определяющий цели, задачи, распределение ответственности между подразделениями, классификацию активов по уровням конфиденциальности и порядок реагирования на инциденты.

Модель угроз – детализированный перечень актуальных угроз, оценка вероятности их реализации, описание возможных каналов атак.

Система документов по управлению доступом – положения и инструкции, регламентирующие назначение паролей, работу с внешними носителями, порядок предоставления и прекращения доступа к ресурсам.

План реагирования на инциденты – сценарии действий персонала при обнаружении компьютерной атаки, состав группы реагирования, порядок эскалации и оповещения.

Повышение квалификации персонала.

Анализ статистики свидетельствует: более 70% успешных кибератак начинаются с фишинговых писем, открытых сотрудниками. Социальная инженерия остаётся одним из наиболее эффективных инструментов злоумышленников. В связи с этим обязательной является программа повышения осведомлённости, включающая:

Вводный инструктаж для новых сотрудников (основные угрозы, правила работы с паролями, действия при подозрительной активности).

Регулярное обучение и тестирование (не реже одного раза в квартал) с практическими занятиями по распознаванию фишинга.

Фишинговые симуляции – контролируемые рассылки для проверки бдительности, выявления уязвимых групп пользователей и адресного дополнительного обучения.

Усиление физической защиты и режимных мер.

Несанкционированный физический доступ к серверным, коммутационным шкафам и рабочим местам может полностью нивелировать любые технические средства. Комплекс мер включает:

Модернизацию системы контроля и управления доступом (СКУД) с использованием биометрических считывателей и двухфакторной аутентификации.

Организацию зон безопасности, ведение журналов посетителей, контроль проноса фото- и видеотехники.

Физическую защиту оборудования: запирающиеся шкафы, крепление к стойкам, замки на корпусах рабочих станций.

Внедрение процесса управления инцидентами.

Системный подход к выявлению, регистрации и устранению инцидентов включает этапы: обнаружение (срабатывание средств обнаружения вторжений, жалобы пользователей), регистрация (фиксация в системе учёта в течение 15 минут), анализ и классификация (оценка критичности, сбор доказательной базы), локализация (изоляция затронутых систем за 30 минут), устранение и восстановление из резервных копий. Важнейшим требованием является интеграция с системами автоматизации, поскольку в ходе активной фазы атаки счёт идёт буквально на минуты.

2. Технические и программно-аппаратные средства защиты

Технические меры составляют основу активной обороны.

Разработанный комплекс охватывает все уровни – от периметра сети до конечных рабочих станций.

Защита сетевого периметра (NGFW и IPS).

Традиционные межсетевые экраны, работающие на уровне пакетной фильтрации, недостаточны. Предлагается внедрение межсетевых экранов нового поколения (NGFW) с функциями глубокого анализа трафика до 7-го уровня модели OSI, выявления SQL-инъекций, контроля анонимайзеров и блокировки нежелательных категорий сайтов. Дополнительно развёртывается система обнаружения и предотвращения вторжений (IPS) с поведенческим

анализом и автоматической блокировкой IP-адресов источников атаки. Особое внимание уделяется «восток-запад» защите – изоляции критических сегментов (АСУ ТП, СУБД) от общедоступных сегментов сети, реализации политики минимально необходимого доступа.

Защита конечных точек (EDR).

Современные целевые атаки всё чаще нацелены непосредственно на рабочие станции и серверы. Традиционных сигнатурных антивирусов недостаточно. В рамках комплекса предлагается внедрение рекласс EDR (Endpoint Detection and Response), обеспечивающих:

Обнаружение угроз на основе поведенческого анализа и машинного обучения.

Расследование инцидентов с детальной телеметрией о векторе атаки.

Возможность удалённой изоляции заражённого хоста, завершения процессов и карантина файлов.

Проактивный поиск скрытых угроз (Threat Hunting).

Антивирусная защита организуется на всех уровнях: почтовый шлюз (с технологией «песочницы»), файловые серверы, рабочие станции, серверы баз данных.

Средства криптографической защиты информации (СКЗИ).

Для защиты конфиденциальных данных при передаче по открытым каналам и хранении на съёмных носителях внедряются сертифицированные криптосредства. Основные направления: организация VPN-соединений между удалёнными подразделениями с использованием криптошлюзов, полнодисковое шифрование ноутбуков, защита съёмных носителей (USB-флеш, внешние диски) с контролем доступа по паролю или сертификату, а также использование электронной подписи для обеспечения целостности критически важных документов и конфигурационных файлов.

Защита веб-приложений (WAF) и резервное копирование.

Для организаций, предоставляющих веб-сервисы, критически важна защита от атак на уровне HTTP/HTTPS. Web Application Firewall (WAF) выявляет и блокирует SQL-инъекции, межсайтовый скриптинг (XSS), подделку запросов (CSRF), защищает от автоматизированных атак (bruteforce), ограничивает скорость запросов. Обеспечивается кластерная конфигурация для отказоустойчивости.

Особого внимания заслуживает резервное копирование в условиях атак программ-шифровальщиков (ransomware), которые нацелены не только на данные, но и на уничтожение копий. Реализуется политика 3-2-1: три копии, два типа носителей, одна офлайн-копия, физически изолированная от сети. Дополнительно внедряются неизменяемые (immutable) бэкапы и сегментация сети резервного копирования.

3. Реинжиниринг процессов управления доступом и мониторинга.

Технические средства защиты неэффективны без правильно выстроенных процессов. Во многих организациях предоставление и отзыв доступа остаются ручными, что приводит к накоплению «мёртвых душ» (учётных записей уволенных сотрудников) и избыточным правам.

Управление идентификационными данными и доступами (IDM/IGA).

Внедрение системы Identity Management автоматизирует полный жизненный цикл учётных записей: создание при приёме на работу (на основании кадрового приказа через API), изменение прав при перемещении сотрудника, мгновенную блокировку при увольнении. Реализуется ролевая модель доступа (RBAC) с исключением прямого назначения прав пользователям. Пользователи получают портал самообслуживания для подачи заявок на изменение прав, а руководители электронно согласовывают их. Проводятся автоматические кампании аттестации прав доступа (ежеквартально) с отзывом неподтверждённых прав.

Управление привилегированным доступом (PAM).

Привилегированные учётные записи (администраторы, root) – наиболее привлекательная цель. Система PAM включает:

Централизованное хранилище паролей в зашифрованном виде.

Автоматическую ротацию паролей после каждой сессии.

Управление сессиями с записью всех действий.

Just-in-Time доступ – предоставление привилегий только на время задачи.

Мониторинг подозрительной активности с интеграцией в SIEM.

Централизованный сбор и корреляция событий (SIEM).

Без SIEM-системы невозможно своевременно выявлять медленные, распределённые во времени атаки. SIEM обеспечивает консолидацию событий от сетевых устройств, ОС, антивирусов, IDS/IPS, WAF, DLP, прикладных систем; нормализацию и обогащение данных контекстом; корреляцию и поведенческий анализ для обнаружения аномалий (например, сотрудник, скачивающий аномально большой объём данных); построение временных линий атаки и графических графов для расследования.

Автоматизация реагирования на инциденты (SOAR).

Для сокращения времени реагирования и разгрузки дефицитных специалистов внедряются платформы SOAR (Security Orchestration, Automation and Response). Типовые сценарии:

Фишинг: при жалобе на письмо → автоматический карантин во всех почтовых ящиках → блокировка ссылок на шлюзе → уведомление отправителя.

Вредоносное ПО: срабатывание антивируса → автоматическое отключение сетевого порта коммутатора → отключение учётной записи → сканирование соседних хостов.

Подозрительная активность привилегированного пользователя: аномальное число неудачных входов → временная блокировка учётной записи → уведомление администратора → смена пароля.

SOAR-платформы не только автоматизируют реагирование, но и стандартизируют процессы, сохраняя экспертизу внутри системы, что особенно важно в условиях дефицита квалифицированных кадров на рынке информационной безопасности.

Разработанный и обоснованный комплекс мероприятий охватывает все три уровня системы защиты информации: организационно-распорядительный, технический и управленческий. В отличие от фрагментарного подхода, предполагающего установку отдельных средств защиты без системной увязки, предлагаемый комплекс базируется на четырёх ключевых принципах.

Эшелонированность («защита в глубину»). Система защиты строится с несколькими рубежами обороны. Преодоление одного уровня не ведёт к компрометации всей инфраструктуры, поскольку последующие рубежи сохраняют контроль.

Автоматизация процессов. Рутинные операции по управлению доступом, реагированию на типовые инциденты и формированию отчётности автоматизированы. Это высвобождает ресурсы специалистов по информационной безопасности для решения более сложных, нестандартных задач (Threat Hunting, анализ новых векторов атак).

Проактивность. Система ориентирована не только на отражение известных атак, но и на выявление скрытых угроз и аномалий. Поведенческий анализ, корреляция событий в SIEM, регулярные фишинговые симуляции и тестирование восстановления из резервных копий позволяют обнаруживать угрозы на ранних стадиях.

Интеграция. Все компоненты системы защиты – NGFW, EDR, PAM, IDM, SIEM, SOAR, система резервного копирования – интегрированы между собой через общие API и протоколы. Это обеспечивает единое пространство мониторинга, унифицированное управление политиками и автоматическую оркестрацию действий при реагировании на инциденты.

Список литературы:

1.Политика информационной безопасности организации (стандарт верхнего уровня).

2.Модель угроз безопасности информации (методика ФСТЭК России).

3.NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations.

4.Рекомендации Банка России по обеспечению информационной безопасности при осуществлении переводов денежных средств.

5.Современные подходы к внедрению SIEM и SOAR (аналитический обзор).