Дидилика Евгений Ренатович
Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М.Буденного» Министерства обороны Российской Федерации
Кузьмич Александр Александрович
Кандидат технических наук
Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М.Буденного» Министерства обороны Российской Федерации
Мереуца Дмитрий Павлович
Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М.Буденного» Министерства обороны Российской Федерации
Сидоренко Иван Дмитриевич
Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М.Буденного» Министерства обороны Российской Федерации

РАЗРАБОТКА КОМПЛЕКСА ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИХ ПРЕДЛОЖЕНИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛОКАЛЬНЫХ СЕТЕЙ

Аннотация. Локальная вычислительная сеть является кровеносной системой современной организации, обеспечивая взаимодействие между сотрудниками, доступ к критически важным данным и приложениям. Возрастающая сложность сетевой инфраструктуры, интеграция мобильных и интернет-технологий, а также изощренность киберугроз делают задачу обеспечения информационной безопасности (ИБ) ЛВС одной из наиболее актуальных

Ключевые слова: Локальная вычислительная сеть, сетевая инфраструктура, критически важные данные и приложения

Многие организации ограничиваются внедрением базовых технических средств защиты, таких как антивирусное программное обеспечение и межсетевой экран, пренебрегая организационной составляющей. Однако, как показывают исследования, значительная часть инцидентов информационной безопасности связана с человеческим фактором. Таким образом, для построения устойчивой системы защиты необходим комплексный подход, объединяющий как технические, так и организационные меры. Целью данной работы является разработка такого комплекса предложений.

1. Анализ угроз безопасности локальных сетей

Угрозы информационной безопасности ЛВС можно классифицировать по нескольким критериям. По природе возникновения их принято делить на внутренние и внешние.

Внешние угрозы исходят извне периметра защищаемой сети. К ним относятся:

· Сетевые атаки: сканирование портов, DDoS-атаки, проникновение через уязвимости в сетевых службах.

· Вредоносное программное обеспечение: вирусы, черви, трояны, программы-шифровальщики (ransomware), распространяемые через интернет или электронную почту.

· Фишинг и целевые атаки (APT-атаки), нацеленные на хищение учетных данных сотрудников.

Внутренние угрозы представляют не меньшую, а зачастую и большую опасность, так как исходят от легальных пользователей сети. Среди них:

· Умышленные действия инсайдеров: хищение или уничтожение данных сотрудниками.

· Непреднамеренные действия персонала: случайное удаление файлов, разглашение паролей, заражение рабочих станций по неосторожности.

· Несанкционированная установка программного обеспечения, создающая уязвимости.

· Подключение к сети неавторизованного оборудования (ноутбуков, точек доступа).

Тип инцидента Доля от общего числа, %:

· Заражение вредоносным ПО 45

· Непреднамеренные действия персонала 25

· Нарушения политики использования ресурсов 15

· Сетевые атаки извне 10

· Умышленные действия инсайдеров 5

2. Комплекс организационно-технических предложений

Предлагаемый комплекс мер строится на принципе эшелонированной (многоуровневой) обороны и включает три основных блока: организационный, технический и административный.

2.1. Организационные меры

Данный блок направлен на регламентацию процессов, связанных с обеспечением ИБ, и управление персоналом.

1. Разработка и внедрение Политики информационной безопасности. Этот документ является основополагающим. Он должен регламентировать:

· Правила использования сетевых ресурсов и интернета.

· Требования к парольным фразам и периодичность их смены.

· Процедуры обработки конфиденциальной информации.

· Порядок реагирования на инциденты ИБ.

2. Регулярное обучение и повышение осведомленности персонала. Проведение тренингов и инструктажей по основам кибергигиены, моделирование фишинговых атак для проверки бдительности сотрудников.

3. Разделение обязанностей и минимизация привилегий. Предоставление пользователям только тех прав доступа, которые необходимы для выполнения их должностных обязанностей.

4. Формирование плана восстановления после инцидентов (Disaster Recovery Plan). Документ, описывающий последовательность действий для минимизации ущерба и скорейшего восстановления работоспособности сети.

2.2. Технические меры

Технические меры являются материальной основой системы защиты и реализуются с помощью программных и аппаратных средств.

1. Защита периметра сети.

· Внедрение межсетевых экранов (Firewall) нового поколения (NGFW) для фильтрации входящего и исходящего трафика.

· Использование систем обнаружения и предотвращения вторжений (IDS/IPS).

2. Защита сетевой инфраструктуры.

· Сегментация сети с помощью VLAN для ограничения распространения угроз.

· Настройка безопасных протоколов для управления сетевым оборудованием (например, SNMPv3 вместо SNMPv1/2c).

· Реализация портов безопасности (Port Security) на коммутаторах для предотвращения подключения неавторизованных устройств.

3. Защита рабочих станций и серверов.

·Обязательное использование лицензионного антивирусного программного обеспечения с регулярным обновлением сигнатур.

· Своевременное применение заплаток и обновлений безопасности (патч-менеджмент).

· Шифрование дисков на компьютерах, обрабатывающих конфиденциальные данные.

· Настройка правил групповых политик (GPO) в средах Windows для ограничения возможностей пользователей.

4. Защита от утечек данных (DLP-системы). Внедрение систем для мониторинга и блокировки попыток несанкционированной передачи конфиденциальной информации за пределы корпоративной сети.

3. Административное управление и мониторинг

Для обеспечения непрерывности и эффективности системы защиты необходимо организовать процессы постоянного администрирования и контроля.

1. Централизованное ведение журналов событий и аудит (SIEM-системы). Сбор и корреляция событий с различных устройств (серверов, рабочих станций, сетевого оборудования) для оперативного выявления аномалий и инцидентов.

2. Регулярное тестирование на проникновение (Penetration Testing). Проведение внешних и внутренних аудитов безопасности для выявления скрытых уязвимостей.

3. Назначение ответственных лиц. Закрепление ответственности за реализацию и соблюдение политики ИБ за конкретными сотрудниками или подразделением.

Заключение

В результате проведенного исследования был разработан комплексный набор организационно-технических предложений по обеспечению информационной безопасности локальных сетей. Ключевой вывод работы заключается в том, что только симбиоз организационных регламентов и современных технических средств позволяет создать устойчивую к современным угрозам систему защиты.

Внедрение предложенных мер, таких как разработка политики безопасности, сегментация сети, внедрение NGFW, DLP и SIEM-систем, а также регулярное обучение персонала, позволит организациям перейти от реактивной к проактивной модели безопасности. Это минимизирует риски финансовых потерь, репутационного ущерба и нарушений требований законодательства в области защиты информации.

Дальнейшие исследования могут быть направлены на адаптацию предложенного комплекса для специфических отраслей, таких как финансовая сфера или здравоохранение, где предъявляются дополнительные требования к конфиденциальности и целостности данных.

Список литературы:

1. Галатенко В.А. Основы информационной безопасности. – М.: Интернет-Университет Информационных Технологий, 2015. – 264 с.

2. Петренко С.А., Курбатов В.А. Политики безопасности компании при работе в сетях. – М.: ДМК Пресс, 2018. – 400 с.

3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. – М.: ИД Форум, 2016. – 432 с.

4. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

5. Cybersecurity Ventures. 2023 Official Annual Cybercrime Report. – 2023.