УДК 004

Кириллов В.С.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Сенцова А.Ю.
Уфимский университет науки и технологий, Уфа

МОДЕЛИ УГРОЗ И ПОСТРОЕНИЕ СИСТЕМ ЗАЩИТЫ В КОРПОРАТИВНЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Аннотация. В статье раскрыты особенности разработки модели угроз на предприятии, а также построения систем защиты в корпоративных автоматизированных системах. Рассматриваются и анализируются проблемы информационной безопасности при защите информации в системах защиты в корпоративных АС.

Ключевые слова: информация, система защиты информации, угроза информационной безопасности, модели угроз, автоматизированная система.

В настоящее время защита корпоративных автоматизированных систем (АС) является крайне актуальной задачей и тому есть определенные причины: организации все больше подвергаются различным сетевым атакам со стороны злоумышленников, которые могут нарушить бизнес-процессы и нанести финансовый и репутационный ущерб, поскольку организации хранят огромное количество важной и ценной информации - от клиентских баз и финансовых документов до интеллектуальной собственности. Защита корпоративных автоматизированных систем становится важнейшей частью стратегии развития любой современной компании, обеспечивая ее безопасность, стабильность и конкурентоспособность.

Для обеспечения безопасности организации очень важно выделить актуальные угрозы безопасности информации, которые оцениваются в ходе моделирования угроз на предприятии. Модель угроз необходима для эффективного управления рисками и разработки мер по защите информационных активов компании. Модель угроз – это формализованное представление возможных сценариев реализации угроз безопасности информационных ресурсов организации [1]. То есть модель угроз представляет собой систематический подход к идентификации возможных рисков и потенциальных уязвимостей, связанных с нарушением информационной безопасности (ИБ) в организации.

Модель угроз включает в себя:

– классификацию угроз: определение типов атак и уязвимостей системы;

– анализ вероятности возникновения угроз: оценка реализуемости различных сценариев атак;

– оценку последствий реализации угроз: рассмотрение возможного ущерба от реализации угроз нарушения ИБ.

Главная цель построения модели угроз заключается в выявлении слабых мест информационной инфраструктуры организации и разработке эффективных мер противодействия потенциальным угрозам, которые могут нанести ущерб компании. Существует определенный сценарий разработки модели угроз корпоративной АС, он основывается на Методике оценки угроз безопасности информации, разработанной ФСТЭК 5 февраля 2021г [2].

Этапами разработки модели угроз корпоративной АС являются:

1. Сбор исходных данных: идентификация активов, анализ используемых технологий и протоколов передачи данных, обзор существующих политик безопасности.

2. Идентификация потенциальных угроз от внутренних и внешних источников угроз.

3. Анализ уязвимости и оценка рисков: классификация уязвимых элементов инфраструктуры, проведение анализа влияния угроз на бизнес-процессы компании.

4. Разработка мероприятий по защите информации на основе проведенного анализа, уточнение набора мер защиты: создание политики управления доступом, развертывание антивирусных решений и межсетевых экранов, регулярная проверка и обновление программного обеспечения и др.

5. Мониторинг и контроль эффективности принятых мер по защите информации.

Стоит отметить, что в настоящее время появились специальные сервисы для автоматизированной разработки моделей угроз безопасности информации в соответствии с требованиями регуляторов (ФСТЭК России). Примером такого сервиса является «Цифровая модель угроз».

«Цифровая модель угроз» – это комплексное решение, позволяющее быстро разрабатывать модели угроз, учитывающие специфику различных отраслей и детально описывающие потенциальные риски для информационных систем и систем АСУ ТП [3]. Это специализированное программное обеспечение позволяет вести разработку сценариев реализации угроз, основанных на комбинации тактик и техник, представленных в матрице MITRE ATT&CK, и техник, определенных ФСТЭК в качестве актуальных для защиты информации.

Рассматривая методы и подходы к защите корпоративной АС, которые помогут увеличить защищенность системы от актуальных угроз, можно выделить: физическую защиту: защиту помещений и оборудования от несанкционированного доступа; техническая защиту: межсетевые экраны (firewalls), VPN-туннели, шифрование каналов связи и хранящихся данных, антивирусные программы и др.; организационную защиту: управ-

ление информационными потоками внутри компании посредством строгих регламентов и инструкций (например, Политика разграничения прав доступа пользователей); правовую защиту: нормативно-правовые акты.

Основными рекомендациями по повышению уровня защищенности корпоративной АС являются:

1. Постоянное обучение персонала вопросам, связанным с информационной безопасностью.

2. Регулярные обновления ПО: своевременное применение обновлений и исправление обнаруженных уязвимостей минимизирует вероятность успешных атак злоумышленников.

3. Использование многоуровневой защиты: применение комплексного подхода обеспечивает надежность даже при нарушении одного слоя защиты.

4. Постоянный аудит и тестирование: периодическое проведение тестов на проникновение и внутренний аудит информационной безопасности позволяют своевременно выявить слабые места и устранить уязвимости информационной безопасности.

Таким образом, разработка эффективной модели угроз и реализация соответствующих мер защиты от актуальных угроз является важным этапом в обеспечении устойчивости и надежности корпоративной автоматизированной системы.

Список использованных источников:

1. Прохорова О.В. Информационная безопасность и защита информации: учебник для СПО / О.В. Прохорова. 6-е изд., стер. СПб.: Лань, 2025. 124 с. Электрон. версия // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/445250 (дата обращения: 17.04.2025).

2. Методический документ Федеральной службы по техническому и экспортному контролю от 05.02.2021 г. «Методика оценки угроз безопасности информации»: URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 16.04.2025).

3. Цифровая модель угроз. URL: https://digital-threat-model.ru/#about (дата обращения: 16.04.2025).

Kirillov V.S.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Sentsova A.Yu.
Ufa University of Science and Technology, Ufa

THREAT MODELS AND CONSTRUCTION OF PROTECTION SYSTEMS IN CORPORATE AS

Abstract. The article reveals the features of developing threat models, as well as construction of protection systems in corporate automated systems. The problems of information security in protecting information in protection systems in corporate AS are considered and analyzed.

Keywords: information, rights, information protection, information protection system, information security threat, threat models, automated system.