



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Колледж программирования и кибербезопасности

Отчет о выполнении практического задания
по дисциплине «МДК.01.04 Эксплуатация автоматизированных
(информационных) систем в защищенном исполнении»
на тему «Анализ угроз безопасности информации.»

Практическое задание № 4

Специальность – 10.05.02 Информационная безопасность
автоматизированных систем

Выполнил студент:

_____ Маркаров М. О.

Группа: ИБ-32

Руководитель:

_____ Герасин В. Ю.

Работа защищена с оценкой _____

Дата защиты _____

Москва

2024

Цель: Анализ угроз безопасности информации в информационной системе управлении складом.

Введение: Эффективность управления складом зависит от использования информационных систем. Однако с ростом обрабатываемых данных увеличивается и количество угроз безопасности информации.

Ход работы: Проведение анализа угроз безопасности для выявления уязвимостей в системе управления складом, для того чтобы обеспечить защиту конфиденциальной информации и предотвратить финансовые потери, связанные с утечками данных.

1. Идентификация угроз: Проведите исследование и выявите основные угрозы безопасности информации, с которыми может столкнуться компания (например, внутренние угрозы, внешние угрозы, угрозы, связанные с программным обеспечением и т. д.).

В информационной системе управления складом существуют внешние угрозы и внутренние угрозы.

Внешними угрозами, которыми может столкнуться компания это кибератаки в информационной системе управления складом являются взломы, DDoS-атаки или атаки типа «человек посередине», направленные на доступ к информации или её блокировку. Фишинг Приманка сотрудников для получения конфиденциальных данных путем обмана через электронные письма или поддельные сайты.

Для того чтобы противодействовать всем этим угрозам рекомендуется проводить совещания сотрудникам для того чтобы информировать о существующих угроз системы и проводить регулярное обновления для того чтобы запутать проникновение в информационную систему нежелательных программ.

Внутренними угрозами в информационной системе с которыми компания может столкнуться это управления складом являются злонамеренные действия и неосторожные действия сотрудников.

Неосторожные действия сотрудников пользователи могут случайно удалить важные данные или предоставить несанкционированный доступ.

Злонамеренные действия прямые угоны данных или их манипуляции со стороны недовольных сотрудников.

Для того чтобы решить угрозу с неосторожными действиями сотрудников необходимо проведение аудитов безопасности и тестирования на проникновение. Создание резервных копий данных и внедрение планов по восстановлению после сбоев. Регулярное обучение сотрудников правилам безопасности.

2. Оценка рисков: Оцените потенциальные последствия каждой угрозы и вероятность их возникновения.

Кибератаки это внешние угрозы, которые вызывают последствия:

Утрата конфиденциальных данных (например, утечка персональных данных клиентов).

Финансовые потери из-за кражи средств или выплаты выкупа.

Снижение доверия клиентов и деловых партнеров.

Приостановка или остановка работы бизнеса.

Вероятность навредить информационной системе управлении складом высокая. Потому что с увеличением числа атак кибератак, вероятность их возникновения возрастает. Широкое распространение технологий делает организации уязвимыми.

Последствия для информационной системе управления складом при внешней угрозе фишинга:

Утрата учетных данных (логины и пароли), что может привести к проникновению в корпоративные учетные записи.

Финансовые потери в результате мошенничества.

Уничтожение или компрометация корпоративной информации.

Вред репутации компании.

Вероятность успешной атаки средняя. Фишинг остается одной из самых распространенных тактик среди киберпреступников. С учетом роста

использования электронной почты и онлайн-сервисов, вероятность успешной атаки средняя.

Последствия от Злонамеренные действия сотрудников могут включать в себя:

Утечка конфиденциальной информации (намеренные действия могут привести к передаче данных конкурентам).

Вред системе путем внедрения вредоносного ПО или разрушительными действиями.

Снижение морального духа среди других сотрудников и ухудшение климата в коллективе.

Юридические последствия и потенциальные иски.

Вероятность повредить систему управления складом средняя. Вероятность внутренних угроз ниже чем внешних они могут произойти, особенно если у сотрудников есть доступ к критически важным системам и данным.

Последствия неосторожные действия сотрудников вызывают утечку данных из-за случайного отправления информации не тому адресату или потери устройств (например, ноутбуков или мобильных телефонов).

Вирусные атаки из-за скачивания подозрительных файлов или посещения небезопасных веб-сайтов.

Понижение производительности из-за необходимости восстановления систем после инцидентов.

Вероятность появление данной угрозы и вред для организации высокая: сотрудники могут не осознавать риск, связанный с их действиями. Недостаток обучения по кибербезопасности увеличивает вероятность неосторожных действий.

3. План мер по предотвращению: На основе выявленных угроз разработайте план мер по предотвращению и минимизации рисков. Ваш план может включать технические, организационные и обучающие меры.

На основе выявленных угроз таких как кибератаки, фишинг, злонамеренные действия и неосторожные действия сотрудников.

Для создания мер по предотвращению кибератак и фишингов необходимо создать меры по защите от этой угрозы необходимо устанавливать межсетевые экраны и настроить виртуальные частные сети VPN для удалённого доступа и шифровать данные для того чтобы реализовать управление ключами для обеспечения безопасности данных.

Для создания мер по предотвращению злонамеренные действия и неосторожные действия сотрудников.

Необходимо организовать:

Обучение персонала компании основам информационной безопасности. Сюда должны войти принципы работы с информацией, использование безопасных каналов для передачи, применение стандартных и специализированных средств защиты информации.

Ограничение доступа к важным данным. Для этого оптимально подходит ролевая модель управления с использованием принципов минимальных привилегий. Помогает контролировать доступ и минимизировать возможный ущерб при выявлении мошеннических действий со стороны персонала.

Введение контроля за носителями и источниками информации. В идеале совсем отказаться от сменных носителей, чтобы исключить возможность кражи данных или внедрения в систему вредоносных программ.

4. Контрольные вопросы.

1. Понятие угрозы безопасности информации.

Угроза безопасности информации — это потенциальное событие или действие, которое может привести к несанкционированному доступу, изменению, уничтожению или раскрытию информации.

2. Виды угроз безопасности информации.

Включают в себя:

1. Автоматизированные угрозы

2. Неавтоматизированные угрозы

3. Технические угрозы

4. Природные угрозы

5. Социальные угрозы

3. Источники угроз безопасности информации.

Внешние источники: хакеры, конкуренты, недоброжелательные лица.

Внутренние источники: сотрудники, которые могут случайно или преднамеренно создать угрозы.

Технические источники: устаревшее программное обеспечение, недостаточная конфиденциальность данных.

4. Предпосылки появления угроз безопасности информации.

Технические недоработки: устаревшие системы, недостаточные меры защиты, уязвимости в программном обеспечении.

Человеческий фактор: недостаточная квалификация сотрудников, ошибки, халатность, злонамеренные действия.

Организационные недостатки: отсутствие четких политик безопасности, недостаточный контроль за доступом, нехватка ресурсов для обеспечения безопасности.

Вывод в ходе проделанной работы, анализ и понимание угроз безопасности информации в системе управления складом неотъемлемая часть управления рисками и защиты активов компаний. Регулярный пересмотр и обновление мер безопасности помогут обеспечить защиту информации и минимизировать возможные последствия в случае инцидентов.