РАЗРАБОТКА МЕТОДИКИ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЛОГИСТИЧЕСКОЙ КОМПАНИИ СДЭК

Шабалин Александр Дмитриевич

магистрант, Московский институт электронной техники, РФ, г. Москва

Информационная безопасность является важным аспектом в современном мире бизнеса, особенно для логистических компаний, которые работают с конфиденциальной информацией своих клиентов и партнеров. Конфиденциальность, целостность и доступность данных являются ключевыми показателями безопасности информации, которые должны быть обеспечены в рамках бизнес-процессов любой логистической компании. Несоблюдение требований информационной безопасности может привести к серьезным последствиям, таким как утечка конфиденциальной информации, потеря доверия клиентов и партнеров, а также негативное влияние на репутацию компании [1].

Данная работа имеет большое значение для логистических компаний, так как поможет улучшить безопасность информации и снизить риски утечки, которые могут негативно сказаться на доверии клиентов и имидже компании в целом. В настоящее время информационная безопасность становится все более актуальной проблемой, ведь современные технологии позволяют киберпреступникам получить доступ к защищенной информации. Из-за этого компании теряют конфиденциальность своих данных, что приводит к финансовым потерям и ущербу для бизнеса в целом.

Важно учитывать, что проведение аудита информационной безопасности является необходимым шагом для обеспечения безопасности информационных ресурсов компании и защиты от потенциальных угроз [2].

Аудит информационной безопасности является важным инструментом, который позволяет определить уровень защищенности информации в компании. Разработка методики проведения аудита информационной безопасности в логистической компании СДЭК включает в себя несколько этапов.

Шаг 1. Определение целей и задач аудита

Первым шагом при разработке методики проведения аудита информационной безопасности в логистической компании СДЭК является определение целей и задач аудита. Цели аудита могут быть различными, например, определение уровня защищенности информации, выявление уязвимых мест в информационной системе, оценка эффективности мер по защите информации и т.д.

Шаг 2. Определение объема и границ аудита

На этом этапе определяется, какие именно информационные системы и данные будут аудитироваться, а также устанавливаются границы аудита. В логистической компании СДЭК это могут быть системы управления складом, программы для отслеживания грузов, системы связи с клиентами и т.д.

Шаг 3. Оценка рисков и угроз

Для определения наиболее уязвимых мест в информационной системе компании СДЭК необходимо провести оценку рисков и угроз. Эта оценка может включать в себя анализ угроз

внешних и внутренних пользователей, оценку уязвимостей системы, оценку возможных последствий нарушения безопасности и т.д.

Шаг 4. Определение методов и инструментов аудита

На этом этапе определяются методы и инструменты, которые будут использоваться при проведении аудита. Это могут быть различные программные средства для автоматизации аудита, методы тестирования на проникновение, методы анализа логов и т.д.

Шаг 5. Разработка плана проведения аудита

На последнем этапе разрабатывается план проведения аудита, в котором определяются конкретные шаги, необходимые для проведения аудита информационной безопасности в логистической компании СДЭК. План должен включать в себя описание методов и инструментов аудита, список проверяемых систем и данных, а также описание последовательности действий при проведении аудита [3].

План проведения аудита информационной безопасности в логистической компании СДЭК должен включать в себя следующие шаги:

1. Определение целей и задач аудита.

2. Определение объема и границ аудита.

3. Оценка рисков и угроз.

4. Определение методов и инструментов аудита.

5. Подготовка программного обеспечения и оборудования для проведения аудита.

6. Проведение аудита.

7. Анализ результатов аудита и подготовка отчета.

8. Разработка рекомендаций по устранению выявленных уязвимостей и улучшению системы безопасности.

9. Контроль и внедрение рекомендаций.

В заключение можно сказать, что разработка методики проведения аудита информационной безопасности в логистической компании СДЭК является важным шагом для обеспечения безопасности информации и защиты от угроз. Применение разработанной методики позволит определить уязвимые места в системе безопасности компании и разработать меры по их устранению.

Результаты аудита показали наличие ряда уязвимостей в системе информационной безопасности компании СДЭК, связанных с недостаточной защитой и управлением доступом, отсутствием контроля за целостностью данных и защитой персональных данных, а также с наличием уязвимостей в сетевой инфраструктуре компании. Были разработаны рекомендации по устранению этих уязвимостей, а также по улучшению процедур управления информационной безопасностью в целом [4].

Общая эффективность разработанной методики проведения аудита информационной безопасности в логистической компании СДЭК может быть оценена как высокая. Она позволила выявить ряд уязвимостей в системе информационной безопасности компании и разработать рекомендации по их устранению. Более того, методика может быть использована не только в компании СДЭК, но и в других логистических компаниях, что делает ее универсальной.

Таким образом, разработанная методика проведения аудита информационной безопасности в

логистической компании СДЭК позволила выявить ряд уязвимостей в системе информационной безопасности компании и разработать рекомендации по их устранению. Дальнейшее развитие методики может быть направлено на расширение ее функционала, улучшение инструментальных средств и повышение квалификации персонала.

Список литературы:

1. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.

2. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - М.: ГЛТ, 2018. - 586 с.

3. Ерохин, В. В. Безопасность информационных систем. Учебное пособие / В.В. Ерохин, Д.А. Погонышева, И.Г. Степченко. - М.: Флинта, Наука, 2018. - 184 с.

4. Малюк, А.А. Введение в информационную безопасность. Учебное пособие для вузов. Гриф УМО МО РФ / А.А. Малюк. - М.: Горячая линия - Телеком, 2021. - 853 с.