17. КОНТРОЛЬ ЭЛЕМЕНТОВ СИСТЕМЫ БИЗНЕС-РАЗВЕДКИ

17.2. Аудит информационной безопасности

Аудит информационной безопасности (ИБ) – это ключевой инструмент обеспечения контроля уровня защиты предприятия. ИБ обеспечивает защиту информационных активов [1].

Существует несколько видов аудита информационной безопасности:

1) экспертная проверка – данный аудит подразумевает, что работу выполняют специалисты. Комплекс мероприятий базируется на опыте экспертов, которые проводят диагностику уязвимостей;
2) проверка соответствия комплекса международным стандартам качества;
3) комплексный аудит – это перечень опций, включающих весь список задач по ИБ;
4) инструментальный анализ – диагностика программно-аппаратной части комплекса, обнаружение уязвимостей и нарушений.

Для того, чтобы провести проверку, приглашают специалистов из других организаций. Преимущественно это консалтинговые компании, которые проводят независимый аудит и специализируются на информационной безопасности.

Комплекс мер по анализу системы ИБ начинается с **разработки алгоритма действий и уточнения необходимого объема работ** у заказчика. Проводятся уточняющие мероприятия [2]:

1. Дислокация объектов, которые подлежат проверке, а также перечень информации, необходимой для аудита.
2. Состав рабочих групп по стороны исполнителя и заказчика.
3. Моделирование потенциальных угроз.
4. Перечень ресурсов, которые выступают в качестве объекта защиты.
5. Категории потенциальных пользователей, которые могут выступать нарушителями.

Главная задача регламента работ – определить рамки, в которых будет проводится аудит. Четкий алгоритм пошаговых действий позволяет исключить бесполезные мероприятия и оптимизирует затраты времени, ресурсов. Кроме того, заранее оговоренный комплекс задач, исключает возникновение разночтений и спорных ситуаций по завершению аудита.

Аудит ИБ компании в процессе анализа и ознакомления с информацией является, по сути, сбором данных и показателей, которые необходимы для оценки.

Среди ключевых вопросов на этапе подготовки – разбор мер, что направлены на реализацию политики конфиденциальности компании. А также проводится тщательный анализ работы всех элементов системы защиты, технические возможности оборудования, условия обеспечения соединений и обмена информацией. Особое внимание уделяется узлам с повышенной уязвимостью, так как чаще всего именно они подвергаются атакам мошенников.

Для обеспечения комплексной и тщательной диагностики элементы рассматриваются по отдельности:

1) структура программного обеспечения;
2) механизмы и инструменты для реализации принципов безопасности и конфиденциальности;
3) конфигурации сетевых устройств, серверной части.

В процессе исследования выявляются ключевые элементы риска для информационной безопасности конкретного предприятия.

Риск – формирование интегральной оценки на основании анализа. Оценивается существующая модель обеспечения безопасности и ее эффективность. А также то, насколько действенны защитные механизмы компании в ситуации противодействия и информационным атакам [3].

Для того, чтобы упростить классификацию, используют **два метода расчета рисков безопасности:**

1. Выявление вероятности атак, степени их воздействия, уровня потенциального ущерба для компании.
2. Выявление уровня риска методом соотношения действующих инструментов и рекомендуемых международных стандартов.

В итоге, приглашенные специалисты вычисляют вероятность атаки на основании данных. А потенциальный ущерб оценивается собственником бизнеса, как более компетентным лицом. В этом случае вероятность представляет собой как специализированная мера для достижения определенных целей во время атаки и причинения вреда предприятию [4].

Аудиторский отчет – заключительный этап. Он характеризуется большим количеством письменной работы. Так как тут формируется выводы и общая аналитика по проведенными мероприятиям. Дается экспертное заключение по уровню защищенности информационной безопасности. Также анализируется текущая ситуация и даются рекомендации по общей эффективности работы информационно-технологической системы. В отчете содержится информация о всех потенциальных угрозах, а также моделируется «портрет» потенциального злоумышленника и отмечаются основные уязвимости и методы возможного воздействия.

Стандарты аудита в ИБ – в рамках проведенного аудита информационной безопасности дается оценка общему состоянию и формируется перечень рекомендаций. Рекомендации выдает экспертная комиссия на основании полученной во время диагностики информации.

Список использованных источников

1. Козьминых С. И. Козьминых П.С. Аудит информационной безопасности // Вестник Московского университета МВД России. №1. 2016. с.181-186. – Режим доступа: https://www.elibrary.ru/item.asp?id=25518488
2. Макаренко С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. С. 1–29. – Режим доступа: URL: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf

3. Сердюк В.А. Аудит информационной безопасности как мера защиты компании // T-Comm – Телекоммуникации и Транспорт. Специальный выпуск по ИБ. 2009. с.24-36. – Режим доступа: https://cyberleninka.ru/article/n/audit-informatsionnoy-bezopasnosti-kak-mera-dlya-ovysheniya-urovnya-zaschity-kompanii
4. Панасенко А. Аудит информационной безопасности – основа эффективной защиты предприятия. 28.05.2006. – Режим доступа: https://www.anti-malware.ru/node/46