Сальников Иван Денисович, студент, Финансовый университет при правительстве Российской Федерации, г. Москва

ОСНОВНЫЕ ТРЕБОВАНИЯ И ПРИНЦИПЫ, УЧИТЫВАЕМЫЕ ПРИ РАЗРАБОТКЕ И ВНЕДРЕНИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Построение организации – сложный и многогранный процесс, включающий в себя определение ее целей, задач, структуры, правовой формы и, конечно же, разработку документальной базы, неотъемлемым элементом которой является политика информационной безопасности.

Ключевые слова: система управления информационной безопасностью, политика информационной безопасности, серия стандартов ISO/IEC 27001.

В современном мире информация играет огромную роль и становится все более ценным активом для компаний независимо от рода их деятельности. Невероятные темпы распространения сети «Интернет» и повсеместное внедрение информационных технологий увеличивают риски хищения или изменения критически важной информации, что ставит под удар интересы бизнеса и благополучие граждан.

В связи с неуклонно растущим числом инцидентов, связанных с нарушением конфиденциальности, целостности или доступности информации, и влекущих за собой репутационные и финансовые потери, организации вкладывают все больше средств в построение собственной системы управления информационной безопасностью (СУИБ).

Создание, функционирование и обслуживание надежной СУИБ невозможно без разработки и внедрения политики информационной безопасности организации (ПИБ) – руководящего документа, представляющего собой совокупность правил, процедур, практических методов и руководящих принципов, используемых компанией в своей деятельности. Иерархия документации ИБ представлена на рисунке 1.

Рис. 1. Иерархическая структура документации информационной безопасности

В соответствии с содержанием серии международных стандартов ISO/IEC 27001 и их отечественных аналогов ГОСТ Р ИСО/МЭК 27001, можно выделить следующие принципы и требования, которые необходимо учитывать при разработке и внедрении ПИБ:

1. Участие высшего руководства.

Высшее руководство должно принимать на себя ответственность за безопасность информации в организации, устанавливать цели и задачи, разрабатывать стратегии и определять бюджеты. Оно также должно обеспечивать поддержку и содействие внедрению ПИБ, убедиться, что все сотрудники понимают важность ИБ и следуют соответствующим политикам и процедурам.

2. Определение угроз.

При разработке политики, необходимо определить потенциальные угрозы для информации, которую организация хранит, обрабатывает и передает. Это позволяет оценить риски и принять меры для её защиты. Одним из способов определения угроз является проведение анализа уязвимостей и угроз (AVT), который позволяет выявить слабые места в системах безопасности.

3. Разработка регламентов и инструкций.

Регламенты устанавливают общие правила и принципы, которые должны соблюдаться всеми сотрудниками и включают в себя такие вопросы, как управление паролями, контроль доступа и обработка конфиденциальной информации. Инструкции регламентируют конкретные шаги и процедуры, которые необходимо выполнить для сохранения конфиденциальности, целостности и доступности информации.

4. Информирование сотрудников.

ПИБ должна быть известна всем работникам организации. Обучение может быть проведено в форме онлайн-курсов, тренингов, семинаров или индивидуальных консультаций. Важно убедиться, что все сотрудники понимают важность ИБ и знают свои права и обязанности в этой области.

5. Проведение мониторинга и аудита.

Такие методы контроля позволяют отслеживать соблюдение ПИБ, а также выявлять нарушения и уязвимости. Мониторинг может быть автоматизирован с помощью специальных систем, которые позволяют отслеживать доступ к информации, аудит может быть проведен как внутренними, так и внешними аудиторами.

Конечно, в зависимости от специфики технологических процессов организации, принципы, на которых построена политика информационной безопасности, могут разниться. Но неизменным остается факт того, что успешный руководитель уделяет пристальное внимание грамотному построению политики ИБ и строгому соблюдению обозначенных требований.

Список литературы:

1. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013.

2. Запечинков, С.В. Информационная безопасность открытых систем в 2-х томах т.2 / С.В. Запечинков. - М.: ГЛТ, 2008.

3. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017.