УДК 004.056

Александрова В.М.
Уфимский университет науки и технологий, Уфа

Научный руководитель:
Шагапов И.А.
Уфимский университет науки и технологий, Уфа

МЕРЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПРИ ВЗАИМОДЕЙСТВИИ СОТРУДНИКОВ СО СТОРОННИМИ ОРГАНИЗАЦИЯМИ

Аннотация. В статье рассматриваются угрозы информационной безопасности, возникающие при взаимодействии сотрудников организации со сторонними организациями. Особое внимание уделяется обоснованию и этапам разработки мер организационной защиты конфиденциальной информации при взаимодействии сотрудников организации со сторонними организациями.

Ключевые слова: информация, организационная защита информации, риски информационной безопасности, конфиденциальная информация.

Обеспечение безопасности конфиденциальной информации является важным составляющим деятельности для любой организации, особенно это касается вопросов взаимодействия со сторонними организациями. Для эффективной защиты конфиденциальности необходимо разработать комплекс мер организационного характера, направленных на минимизацию рисков утечки и несанкционированного доступа (НСД) к важной информации при взаимодействии со сторонними организациями.

Рассматривая в общем организационные угрозы, по характеру воздействия их можно разделить на:

- угрозы воздействия на персонал заинтересованными лицами;
- действия самого персонала [1].

Воздействие на сотрудников может быть как физическим, так и психологическим. Действия персонала, которые могут создавать угрозы безопасности защищаемой информации, могут быть преднамеренными или непреднамеренными (случайными). Таким образом, организационные угрозы либо направлены против персонала компании, либо реализуется через них, т. е. сами сотрудники компании рассматриваются как источник организационных угроз информационной безопасности.

Воздействие на сотрудников, как отмечалось ранее, может быть двух видов:

1. Физическое. Физическое воздействие на сотрудников заключается в том, что злоумышленник действует на самого сотрудника, чтобы заставить его или косвенно через других людей получить конфиденциальную

информацию или нарушить работу определенных организационных процессов компании. Эти инциденты расследуются службой информационной безопасности организации и правоохранительными органами.

2. Психологическое. При психологическом воздействии на работников можно рассматривать такие распространенные методы влияния в области информационной безопасности, как шантаж, взяточничество, социальная инженерия и многие другие.

Современные организации регулярно взаимодействуют с различными контрагентами – поставщиками, клиентами, подрядчиками и др. При этом происходит постоянный обмен информацией различного уровня секретности. Это взаимодействие несет потенциальные риски ИБ, такие как утечка коммерческих тайн, нарушение законодательства о защите персональных данных, компрометации репутации предприятия и др. Для предотвращения негативных последствий необходимы меры организационно-правового регулирования процессов обмена конфиденциальной информацией между сотрудниками и представителями сторонних организаций.

Основные направления разработки мер организационной защиты:

1. Разработка внутренней политики информационной безопасности. Необходимо создать политику ИБ, регламентирующую правила обращения с конфиденциальной информацией внутри организации и при работе с внешними субъектами. Документально закрепленные положения позволят сотрудникам четко понимать требования и последствия нарушения данных правил обработки информации. Важно включить и задокументировать следующие положения: классификацию уровней секретности документов; порядок допуска сотрудников к закрытой информации; процедуры передачи информации внешним организациям; запрет разглашения конфиденциальной информации третьим лицам без согласования руководства [2].

2. Организация контроля доступа сотрудников к защищаемым данным. Следует внедрить систему ограничения доступа к документам и ресурсам, содержащим коммерческую тайну или персональные данные. Только сотрудники, непосредственно вовлеченные в процесс взаимодействия с партнерами, должны иметь возможность получать доступ к такому виду сведениям. Примерами методов реализации являются: использование паролей и многоуровневой аутентификации пользователей; установка автоматизированных систем мониторинга действий сотрудников с файлами; периодическое обновление инструкций по использованию защищенных каналов связи. Система Аккорд-АМДЗ предназначена для комплексного разграничения доступа сотрудников к защищенной информации на различных уровнях сетевых и аппаратных компонентов организации. Она представляет собой специализированное решение, ориентированное на российские стандарты информационной безопасности и применяемое преимущественно государственными учреждениями и предприятиями оборонно-промышленного комплекса.

3. Регулирование процесса обмена конфиденциальной информацией. Все процессы взаимодействия сотрудников организации со сторонними организациями должны быть строго формализованы. Передача важных сведений должна осуществляться исключительно в рамках установленных процедур и с соблюдением соответствующих требований закона. Меры включают: подписание соглашений о неразглашении (NDA), контроль сроков хранения переданных материалов, применение шифрования электронной почты и иных каналов коммуникации [3].

4. Повышение осведомленности персонала. Сотрудники должны осознавать важность соблюдения норм безопасности информацию и ответственности за возможные негативные последствия несоблюдения регламентов ИБ. Рекомендуется проведение регулярных тренингов и семинаров по вопросам информационной безопасности.

5. Мониторинг эффективности защитных мероприятий. Постоянная оценка качества существующих мер защиты информации позволяет своевременно выявлять слабые места системы защиты и вносить необходимые изменения. Эффективность измеряется показателями, такими как количество случаев попыток взлома, уровень информированности сотрудников, скорость реакции службы информационной безопасности на инциденты [4].

Подводя итог, можно сделать вывод, что организационные уязвимости практически всегда появляются из-за отсутствия или неправильного применения механизмов контроля. Если уменьшить количество организационных уязвимостей, уменьшится и количество организационных угроз и атак. Организационные угрозы либо направлены против персонала компании, либо реализуется через них, поэтому защита от организационных угроз должна быть направлена на обучение сотрудников организации информационной безопасности, определение их ответственности в случае нарушения требований информационной безопасности.

Список использованных источников:

1. Баланов А.Н. Комплексная информационная безопасность: учебное пособие для СПО / А.Н. Баланов. 2-е изд., стер. Санкт-Петербург: Лань, 2025. 284 с. Электрон. версия. // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/463001 (дата обращения: 20.04.2025).

2. Ерохин В.В. Безопасность информационных систем: учебное пособие / В.В. Ерохин, Д.А. Погонышева, И.Г. Степченко. 4-е изд., стер. М.: ФЛИНТА, 2022. 184 с. Электрон. версия. // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/232457 (дата обращения: 19.04.2025).

3. Тимофеева Т.Ф. Защита интеллектуальной собственности и информационная безопасность: учебно-методическое пособие / Т.Ф. Тимофеева. Чебоксары: ЧГУ им. И.Н. Ульянова, 2023. 172 с. Электрон. версия. // Лань: электронно-библиотечная система. URL: https://e.lanbook.com/book/388823 (дата обращения: 20.04.2025).

4. Шагапов И.А. О некоторых вопросах при работе с персоналом, допущенным к конфиденциальной информации предприятия / И.А. Шагапов // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов V Всероссийской молодежной научно-практической конференции, Уфа, 20–21 мая 2022 г. Уфа: Башкирский государственный университет, 2022. С. 39–41. URL: https://confbsu.bashedu.ru/itokbo-2022-05-20/9/ (дата обращения: 20.04.2025).

Aleksandrova V.M.
Ufa University of Science and Technology, Ufa

Scientific supervisor:
Shagapov I.A.
Ufa University of Science and Technology, Ufa

MEASURES TO PROTECT CONFIDENTIAL INFORMATION WHEN EMPLOYEES INTERACT WITH THIRD-PARTY ORGANIZATIONS

Abstract. The article examines the threats to information security that arise when employees of an organization interact with third-party organizations. Special attention is paid to the justification and stages of the development of organizational measures for the protection of confidential information in the interaction of the organization's employees with third-party organizations.

Keywords: information protection rights, organizational information protection, information security risks, confidential information.