

Шибанова Д.А.

студентка

4 курс, Факультет Экономики

ФГБОУ ВО «Ульяновский Государственный Университет»

Россия, г. Ульяновск

Хусаинова Э.Э.

студентка

4 курс, Факультет Экономики

ФГБОУ ВО «Ульяновский Государственный Университет»

Россия, г. Ульяновск

Кузнецова А.С.

студентка

4 курс, Факультет Экономики

ФГБОУ ВО «Ульяновский Государственный Университет»

Россия, г. Ульяновск

ОЦЕНКА ОСНОВНЫХ ЗАДАЧ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: в статье рассмотрены задачи по обеспечению информационной безопасности, оценка рисков информационной безопасности, основные задачи по обеспечению информационной безопасности.

Ключевые слова: информационная безопасность, основные задачи обеспечения безопасности информационных данных, оценка рисков информации.

***Annotation:** The article discusses the tasks of ensuring information security, assessing information security risks, and the main tasks of ensuring information security.*

***Key words:** information security, the main tasks of ensuring the security of information data, information risk assessment.*

В современных условиях хозяйствования при осуществлении финансово-хозяйственной деятельности у предприятия имеется информация, которую необходимо защитить от третьих лиц. Защита информации зависит от уровня эффективности задействованных средств, которые определяются как ресурс системы.

Под ресурсом может пониматься количество людей, сотрудников, привлекаемых для защиты данных, в виде программных, цифровых или инженерно-технических средств используемых для защиты информации.

На любом хозяйствующем субъекте необходимо разрабатывать и внедрять политики информационной безопасности. Использование методов защиты информации обычно на предприятиях бывает эпизодическим и сводится к установке бесплатных антивирусных программ и физической защите (запирание служебных помещений на ночь и т.д.).

Данная халатность со стороны информационно-технического персонала может привести к разным инцидентам, представляющим угрозу для деятельности организации в целом.

Поэтому в обязанности руководства предприятия входит разработка политики информационной безопасности. Основные правила защиты закрепляются в «Положении о информационной безопасности».

Защита информационной безопасности обеспечивается с двух точек зрения:

- программного обеспечения;

- технического обеспечения.

Хозяйствующий субъект можно обследовать на предмет выполнения основных задач информационной безопасности (см. таблицу 1).

Таблица 1 – Оценка основных задач по обеспечению информационной безопасности хозяйствующего субъекта

Основные задачи по обеспечению информационной безопасности	Степень выполнения
1)Обеспечение безопасности деятельности, защита информации и сведений, являющихся коммерческой тайной;	Низкая/ Высокая/ Отсутствует
2)Организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;	Низкая/ Высокая/ Отсутствует
3)Организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;	Низкая/ Высокая/ Отсутствует
4)Предотвращение необоснованного допуска и открытого доступа к сведениям и работам, составляющим коммерческую тайну;	Низкая/ Высокая/ Отсутствует
5)Выявление и локализация возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (авария, пожар и др.) ситуациях;	Низкая/ Высокая/ Отсутствует
6)Обеспечение режима безопасности при осуществлении таких видов деятельности, как различные встречи, переговоры, совещания, заседания и другие мероприятия, связанные с	Низкая/ Высокая/ Отсутствует /

деловым сотрудничеством на национальном и международном уровне.	
---	--

Если данные таблицы 1 будут больше склоняться к отрицательным ответам, очевидно, что положение компании по отношению к стандартам защиты информации весьма низкое, т.е. в случае их хищения хозяйствующий субъект может понести колоссальные потери.

Задачи информационной безопасности указанные в таблице 1 показывают, что выбранное направление разработки является актуальным и крайне необходимым.

Самым трудным аспектом, который влияет на увеличение стоимости работ по анализу рисков, оказывается необходимость знание бизнеса. К сожалению, подразделения ИТ и безопасности, находящихся внутри организации, не всегда обладают достаточными знаниями. Очень важно определить, как будут выполняться работы по оценке рисков силами сотрудников организации или специалистами.

В задачи сотрудников отдела ИБ входят обязанности оповещения руководящих лиц организации о имеющихся и потенциальных угрозах. Отчёты должны сопровождаться аналитическими выкладками, показателями, фактами. Это самый эффективный метод довести информацию до глав предприятия.

Анализ рисков состоит в том, чтобы определить имеющиеся риски и оценить их величины.

Процесс анализа предусматривает решение следующих задач:

1. Определение основных ресурсов ИС.
2. Определение Важности различных ресурсов для организации
3. Идентификация имеющихся угроз и уязвимостей безопасности, возможные осуществления угроз.
4. Расчёт рисков, связанных с реализацией угроз безопасности.

Средства ИС выделяются на следующие категории:

- Ресурсы ИС
- Программное обеспечение
- Техническое обеспечение (сетевое оборудование, сервера, дата центр, рабочие компьютеры и.т.п)
- Человеко-ресурсы

Таким образом, можно сделать вывод, что любой хозяйствующий субъект нуждается в разработке собственной политики информационной безопасности, и выбранные решения будут являться актуальными только для него.

Использованные источники:

1. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция от 09.03.2021г. N 43-ФЗ)).
2. Баранова Е.К., Мальцева Л.Н. Анализ рисков информационной безопасности для малого и среднего бизнеса // Директор по безопасности. — 2015. — № 9. — С. 58—63.
3. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Вестник Московского университета им. С.Ю. Витте. Серия 3: Образовательные ресурсы и технологии. – 2015. – № 1(9). – С. 73-79.
4. Сабанов А.Г. Многоуровневый анализ угроз безопасности процессов аутентификации //Вопросы защиты информации. – 2014. – № 1(104).