МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Гладковская Ю.И., студент гр.973601

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Горностай Л.Ч. – старший преподаватель

Аннотация. В данной работе рассмотрены основные понятия информационной безопасности. Оценены преимущества использования менеджмента информационной безопасности для компаний.

Ключевые слова. Менеджмент, информационная безопасность, конфиденциальность информации.

Система менеджмента информационной безопасности – часть общей системы менеджмента, которая основана на подходе бизнес-рисков при создании, внедрении, функционировании, мониторинге, анализе, поддержке и улучшении информационной безопасности [1].

Информационная безопасность – сохранение конфиденциальности, целостности и доступности информации.

Конфиденциальность – обеспечение доступности информации только для тех, кто имеет соответствующие полномочия (авторизированные пользователи).

Целостность – обеспечение точности и полноты информации, а также методов её обработки.

Доступность – обеспечение доступа к информации авторизированным пользователям, когда это необходимо (по требованию) [2].

Информационная безопасность компании, общественной организации или производственного предприятия – это комплекс мероприятий, направленных на предотвращение несанкционированного доступа к внутренней IT-инфраструктуре, незаконного завладения конфиденциальной информацией и внесения изменений в базы данных.

Учитывая важность информации в современном мире, защите от утечек конфиденциальной информации в адрес конкурентов необходимо уделять повышенное внимание. Возможный ущерб может быть намного большим, чем стоимость всех материальных активов предприятия.

Скоординированные действия, выполняемые с целью повышения и поддержания на требуемом

уровне информационной безопасности организации, называются управлением (менеджментом) информационной безопасностью. В рамках системы менеджмента информационной безопасности рассматривают структуру системы, политики, действия по планированию, обязанности, практики, процедуры, процессы и ресурсы организации.

Обеспечение информационной безопасности должно быть направлено прежде всего на предотвращение рисков, а не на ликвидацию их последствий. Именно принятие предупредительных мер по обеспечению конфиденциальности, целостности, а также доступности информации и является наиболее правильным подходом. Любая утечка информации может привести к серьезным проблемам для компании – от значительных финансовых убытков до полной ликвидации. С появлением персональных компьютеров и интернета возникли новые приемы незаконного получения информации. Если раньше конфиденциальные данные хранились на большом количестве бумажных носителей, то сейчас огромные объемы важной информации можно мгновенно получить, используя современные технологии, либо просто уничтожить посредством вирусов. Чаще всего «крадут» из компаний документы финансового характера, технологические и конструкторские разработки, логины и пароли для входа в сеть других организаций. Но серьезный вред может нанести и утечка персональных данных сотрудников.

Целями менеджмента информационной безопасности являются защита от атак на сеть компании; оценка слабых мест, которые могут возникнуть в результате доступа некорпоративного персонала к корпоративной сети, и принятие мер предосторожности; предотвращение слабых мест в системе безопасности, возникающих из-за программ удаленного доступа; ограничение доступа в офисы уполномоченным лицам для обеспечения информационной безопасности; проведение обучения персонала информационной безопасности и информационным программам с целью предотвращения утечки информации; защита от уничтожения стратегически важных документов, хранящихся в физических архивах; обеспечение непрерывной деятельности и предотвращение возможных перебоев в обслуживании.

Список использованных источников:

1. Дорофеев, А.В. Менеджмент информационной безопасности: основные концепции / Дорофеев А.В., Марков А.С. // Вопросы кибербезопасности. – 2014. – №1(2). – С.67-73.

2. Баранова, Е.К. Информационная безопасность и защита информации : учеб. пособие / Е.К. Баранова, А.В. Бабаш. – М. :РИОР : ИНФРА-М, 2018 – 336 с.

3. Князькова, В. С. Оценка уровня знаний и навыков населения Республики Беларусь в сфере информационной безопасности в условиях перехода к электронной экономике / В. С. Князькова // Цифровая трансформация. - 2018. - № 3 (4). - С. 34-45.

4. Лыньков, Л. М. Методика оценки рисков информационной безопасности в системах электронной экономики / Л. М. Лыньков, Т. Н. Беляцкая, В. С. Князькова // Докл. БГУИР. – 2017. – № 2. – С. 69–76.

5. Беляцкая, Т. Н. Концепция электронной экономики / Т. Н. Беляцкая // Электронная экономика: теория, модели, технологии / Т. Н. Беляцкая [и др.] ; под общ. ред. Т. Н. Беляцкой, Л. П. Князевой. – Минск, 2016. – С. 5–10.

6. Беляцкая, Т. Н. Экономика информационного общества : учеб.-метод. пособие / Т. Н. Беляцкая. – Минск : Белорус. гос. ун-т информатики и радиоэлектроники, 2016. – 200 с.