Секция «Информационное общество, цифровая экономика и информационная безопасность»

Повышение уровня информационной безопасности сервера на примере предприятия

Научный руководитель – Калмыкова Анастасия Дмитриевна

Боброва Е.О.[1], *Бобров К.Р.*[2]

1 - Московский городской педагогический университет, Юридический институт, Москва, Россия, *E-mail: cat.katrin@rambler.ru*; 2 - Московский технический университет связи и информатики, Москва, Россия, *E-mail: kirr2012@yandex.ru*

Введение: Защита нематериальных активов (НМА) т.е. информационных ресурсов предприятия является одной из приоритетных задач защиты информации, так как НМА позволяют:

1. приносить организации экономические выгоды (доход) в будущем;
2. получать компании данные экономических выгод в будущем;
3. структурировать имущество компании.

Верный выбор структуры и состава защиты информации и ее компонентов является ключевым вопросом в обеспечении защиты большинства активов предприятия.

Актуальность: Защита информации на сервере является одной из важных составляющих в процессе обеспечения информационной безопасности предприятия. Однако со временем, из-за развития информационных технологий способы построения защиты изменились, что требует их адаптации к конкретному объекту.

Практическая значимость комплексной защиты информации (КСЗИ) в отличие от раздельных систем обеспечения защиты информации состоит в их модульности и информативности. Программно-аппаратные комплексы такого типа разрабатываются индивидуально для каждой конкретной цели. Не существует единого или идеального способа создания КСЗИ. Однако, специалисты, обладающие большим опытом и знанием, могут создать наиболее эффективную систему.

Создание и реализация методологического обеспечения единого центра слежения и управления системой защиты в крупных компаниях позволяет работникам службы безопасности эффективнее координировать свои действия по обеспечению ИБ на предприятии. Возможность просмотра деталей событий с одного рабочего места и передача на него достоверной информации также облегчает работу сотрудников службы ИБ.

Цель работы: обеспечение защиты информации в ЛВС предприятия от угроз, возникающих при передаче, обработке и хранении информационных ресурсов предприятия на сервере.

В каждом конкретном случае имеется сложившаяся организационная структура предприятия, в которой могут возникнуть некоторые инциденты (которые смогут нарушить основные бизнес-процессы, а также негативно повлиять на эффективность и результативность его деятельности).

Исходя из этого существуют возможные шаги по решению проблемы минерализации негативных последствий инцидентов для реализуемых бизнес-процессов предприятия:

1. анализ теоретических источников по проблемам исследования управленческой деятельности в условиях факторов неопределенности и риска;

2. определение теоретико-методологических и ресурсных основ для выработки оптимальных управленческих решений для сложившихся условий функционирования предприятия;

3. разработка (либо коррекция) сложившейся организационной структуры управления, состава, форм и методов реализации бизнес-процессов;

4. систематизация, обобщение и обработка накопленных теоретических и практических материалов для дальнейшего практического использования, обучения персонала и др.

Проблема обеспечения конфиденциальности данных крайне актуальна. Общество прогрессирует, совершенствуются частнособственнические отношения, происходит активная борьба за власть. Расширение масштабов деятельности человека приводит к повышению ценности информации и особенно тех сведений, которые дают ее обладателю преимущество - материальное или политическое.

Информация представляет собой важнейший ресурс предприятия. Владение конкретной информацией имеет главенствующее значение для организации, для ее деятельности и приоритета перед конкурентами, поэтому очень значимым является сохранение и защита этой информации.

Таким образом, обеспечение защиты информации на сервере предприятия от угроз, возникающих при передаче, обработке и хранении информационных ресурсов предприятия на сервере.

Были решены следующие задачи:

1. Выполнен анализ рассматриваемой предметной области (на основе данных из литературных и интернет источников);

2. Рассмотрены угрозы (методы и средства) негативного воздействия на информационные ресурсы организации в целях уменьшения её НМА;

3. Разработаны мероприятия по нейтрализации или минимизации негативных воздействий на информационные ресурсы организации, хранящиеся на сервере и циркулирующие в сети предприятия;

4. Приведено обоснование выбранных методов и средств защиты информации;

5. Оценена практическая экономическая эффективность предложенных мероприятий.

Источники и литература

1) Бачило И.Л. Информационное право: учебник для вузов / И.Л. Бачило. – М.: Высшее образование, Юрайт-издат, 2013. – с. 72-73

2) Вершинина Д.Д. Обеспечение комплексной безопасности организации /Вершинина Д.Д., Тюменев А.В.//Теория и практика проектного образования. 2019. № 2 (10). С. 21-24.

3) Рубцов А.М. Комплексная информационная безопасность в России и за рубежом /Рубцов А.М., Тюменев А.В.//Теория и практика проектного образования. 2017. № 4 (4). С. 40-44.