

Пушников Д.Э.

Научный руководитель: д.т.н., доцент, заведующий каф. ИС Д.Е. Андрианов

Научный руководитель: д.т.н., доцент, зав. каф. ИС Д.Е. Андрианов

602264, г. Муром, Владимирская обл., ул. Орловская, 23

E-mail: maddoxh_93@mail.ru

Комплексная защита информационной системы ООО «Модус»

В настоящее время появляются все новые и новые информационные технологии, которые улучшают и облегчают работу человека. Информация представляет наибольшую ценность. Доступ к необходимой информации открывает неограниченные возможности. В то же время интенсивная информатизация общества ведет к увеличению преступлений, связанных с использованием вычислительной техники, в том числе и преступлений, связанных с несанкционированным доступом и всевозможных воздействия на информацию и ее носители. В связи с этим появляется необходимость защиты информации.

Для обеспечения наиболее эффективной защиты информационных систем, необходимо руководствоваться приказами ФСТЭК России от 11 февраля 2013 г. N 17 и ФСТЭК России от 18 февраля 2013 г. N 21.

Объектом исследования исследовательской работы является информационная система (ИС) ООО «Модус».

Целью работы является анализ защищенности информационных ресурсов ООО «Модус».

Являясь оператором связи по городу Мурому и Муромскому району, компания обеспечивает телекоммуникационную инфраструктуру, предоставляет широкий спектр качественных услуг связи населению, государственным учреждениям и ведомствам, промышленным и сельскохозяйственным предприятиям, активно работает с бизнес-клиентами.

Среди услуг, предоставляемых ООО «Модус» — местная и внутризональная телефонная связь, проводное и эфирное радио, интерактивное телевидение, подвижная радиотелефонная связь, услуги передачи данных в Интернет, услуги интеллектуальной сети связи.

ООО «Модус» является муниципальным предприятием по оказанию услуг населению. На предприятии ведётся обработка персональных данных сотрудников и клиентов, следовательно, есть необходимость реализации мер по защите персональных данных. Получив доступ к данной информации, злоумышленник может нанести ущерб как самой организации и ее сотрудникам, так и части населения города. В связи с этим появляется необходимость защиты информации.

В то же время растет количество преступлений, связанных с использованием вычислительной техники, в том числе и преступлений, связанных с несанкционированным доступом и всевозможных воздействия на информацию и ее носители, а значит, становится все сложнее не дать злоумышленнику завладеть, уничтожить, повредить или изменить конфиденциальные данные. Следовательно, средства защиты, чтобы соответствовать требованиям современности, должны постоянно обновляться. Так же появляется необходимость регулярных проверок по оценке эффективности уровня защищенности информационных ресурсов на предприятии как от внешних, так и от внутренних угроз.

Чтобы понять какие меры по защите информации необходимо применить на предприятии, нужно:

- Проанализировать объект исследования;
- Проанализировать защиту объекта, выявить текущие недостатки;
- Выявить основные уязвимости и угрозы на объекте;
- Составить план мероприятий на основе документов регулятора по защите информационных ресурсов.