КЛАССИФИКАЦИЯ МЕР ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Мартынчук М. Н.

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

Давыдовский А. Г. – канд. биол. наук, доц. каф ИПиЭ

Согласно Закону Республики Беларусь от 10.11.2008 г. №455-З «Об информации, информатизации и защите информации», защита информации – это комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации. В статье 29 указанного Закона, выделяют три группы мер по защите информации, способные обеспечить требуемый уровень информационной безопасности:

1. правовые – заключаемые обладателем информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий;
2. организационные – обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации;
3. технические – меры по использованию средств технической и криптографической защиты информации, а также меры по контролю защищенности информации.

Согласно Положению о технической и криптографической защите информации в Республике Беларусь (утверждено Указом Президента Республики Беларусь от 16.04.2013 №196):

– техническая защита информации – это деятельность, направленная на обеспечение конфиденциальности, целостности, доступности и сохранности информации техническими мерами без применения средств криптографической защиты информации,

– криптографическая защита – это деятельность, направленная на обеспечение конфиденциальности, контроля целостности и подлинности информации с использованием средств криптографической защиты.

В свою очередь технические меры защиты информации можно разделить на программные и аппаратные. Использование различных устройств характеризует группу аппаратных методов защиты информации, а использование специальных программ – группу программных.

Приведённую классификацию можно дополнить морально-этическими и физическими мерами, не определёнными на законодательном уровне, но позволяющими достигнуть оптимального уровня защиты информации.

Морально-этические меры защиты информации включают в себя различные моральные, нравственные, этические нормы использования, распространения, обработки информации, сложившиеся в коллективе, организации, государстве, обществе. Эти нормы, как правило, не являются законодательно утвержденными, их нарушение не влечёт за собой административное, уголовное или иное преследование. Однако они являются обязательными к соблюдению индивидуумами как моральный и нравственный базис в определенных социальных или профессиональных группах.

Главной задачей комплекса физических мер является обеспечение безопасности самой информации, а так же ее носителей.

Таким образом, классификация мер по защите информации имеет вид:

1. Правовые меры.
2. Организационные меры.
3. Технические меры: программные и аппаратные.
4. Криптографические меры.
5. Физические меры.
6. Морально-этические меры.

Список использованных источников:

1.InfoWatch / Сайт группы компаний-разработчиков программных продуктов и решений для обеспечения информационной безопасности организаций, противодействия внешним и внутренним угрозам [Электронный ресурс] – Режим доступа: http://www.infowatch.ru

2.ИТ-защита / Сайт-проект «ИТ-защита» [Электронный ресурс] – Режим доступа: http://itzashita.ru.

3.Компьютерные вести / Обзор DLP-систем [Электронный ресурс] – Режим доступа: http://www.kv.by/content/obzor-dlp-sistem.