УДК 005.21:334.012.42

Авраменко Т. О.

ассистент кафедры экономической информатики, учёта и коммерции

Гомельский государственный университет имени Франциска Скорины

Республика Беларусь, г. Гомель

СОВРЕМЕННОЕ СОСТОЯНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ РЕСПУБЛИКИ БЕЛАРУСЬ

Аннотация:

В статье рассмотрены вопросы, касающиеся юридического, технического и технологического обеспечения информационной безопасности в коммерческих организациях Республики Беларусь. В частности, проанализированы основные тематические законодательные акты. Рассмотрены современные инженерно-технические и программные способы защиты данных коммерческих организаций.

Ключевые слова: информационная безопасность, коммерческие организации, юридическое обеспечение информационной безопасности, техническое обеспечение информационной безопасности, технологическое обеспечение информационной безопасности.

Avramenko T.

Assistant, Department of Economic Informatics, Accounting and Commerce

Gomel State University named after Francis Skorina

Republic of Belarus, Gomel

THE CURRENT STATE OF INFORMATION SECURITY IN ORGANIZATIONS OF THE REPUBLIC OF BELARUS

Annotation:

The article deals with issues related to the legal, technical and technological support of information security in commercial organizations of the Republic of Belarus. In particular, the main thematic legislative acts are analyzed. Modern engineering and software methods for protecting the data of commercial organizations are considered.

Key words: information security, commercial organizations, legal support of information security, technical support of information security, technological support of information security.

Согласно Концепции национальной безопасности Республики Беларусь под информационной безопасностью понимается состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере[1].

Основным законодательным актом в сфере обеспечения информационной безопасности в коммерческих организациях Республики Беларусь является Закон «О коммерческой тайне». Согласно данному закону, под коммерческой тайной следует понимать сведения любого характера (технического, производственного, организационного, коммерческого, финансового и иного), в том числе секреты производства (ноу-хау), соответствующие требованиям Закона «О коммерческой тайне», в отношении которых установлен режим коммерческой тайны [2].

Кроме того, правовое обеспечение информационной безопасности и в том числе защиты информации в коммерческих организациях базируется на следующих нормативно-правовых актах [3]:

1. Гражданский кодекс Республики Беларусь содержит нормы, касающиеся служебной и коммерческой тайны, закрепляет такие формы отношений, как информационные услуги, электронную подпись признает как средство, подтверждающее подлинность сторон в сделках, предусматривает ответственность за незаконное использование информации (статья 140, часть 2 статьи 161, статья 1011 и другие).

2. Кодекс Республики Беларусь об административных правонарушениях, в котором определяются административно-правовые санкции за правонарушения в информационной сфере. К таким правонарушениям относятся: несанкционированный доступ к

компьютерной информации (статья 22.6), нарушение правил защиты информации (статья 22.7) и другие.

3. Уголовный кодекс Республики Беларусь закрепляет ответственность за преступления против порядка осуществления экономической деятельности (глава 25, статьи 252, 254, 255 и другие) и информационной безопасности (глава 31, статьи 349, 350, 352 и другие).

4. Трудовой кодекс Республики Беларусь, в соответствии с которым для работников устанавливается обязанность хранить государственную и служебную тайну, не разглашать коммерческую тайну нанимателя, коммерческую тайну третьих лиц, к которой наниматель получил доступ (п.10 части 1 статьи 53).

5. Налоговый кодекс Республики Беларусь (общая часть) включает нормы, определяющие порядок защиты различных видов конфиденциальной информации.

6. Законы, среди которых следует отметить:

- Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»;

- Закон Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи»;

7. Государственная программа «Цифровое развитие Беларуси» на 2021-2025 годы, утвержденную постановлением Совета Министров Республики Беларусь от 2 февраля 2021 г. № 66.

8. Указы Президента Республики Беларусь и постановления Совета Министров Республики Беларусь, а также приказы и постановления Оперативно-аналитического цента при Президенте Республики Беларусь, касающиеся обеспечения информационной безопасности в коммерческих организациях.

Что касается технических и технологических средств защиты информации, то к ним относится вся линейка инженерно-технических,

электрических, электронных, оптических и других устройств, технических систем, а также иных изделий, применяемых для решения различных задач по защите информации. Объектами системы технической защиты информации являются: базы данных, документация в электронном виде и на бумажных носителях, любые сведения, составляющие коммерческую тайну, технологическая, техническая и производственная информация.

В целом средства защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

1. Технические (аппаратные) средства защиты информации – на уровне оборудования решают задачи информационной защиты. Они или предотвращают физическое проникновение, или препятствуют доступу к данным. К техническим средствам относят устройства, способные проводить исследования на наличие вероятных каналов утечки, выявлять и перекрывать их, локализовывать места утечки информации, обнаруживать шпионские программы и(или) приборы, противодействовать стороннему доступу к конфиденциальным сведениям.

2. Программные и технические средства защиты информации включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и другие. Для этой цели используются антивирусы, менеджеры паролей, программы, обеспечивающие безопасность на уровне каналов связи и предотвращающие несанкционированный доступ к ним, программы-блокираторы доступа во всемирную сеть и другие.

3. Инженерно-технические средства защиты информации подразумевают наличие криптографических средств шифрования данных, позволяя сохранить тайну телефонных переговоров, телеметрических и компьютерных данных, сообщений. Математический метод преобразования

передаваемой информации делает их нераспознаваемыми для сторонних лиц. Криптографическая защита бывает с открытым либо симметричным ключом.

4. Организационные средства защиты информации складываются из организационно-технических и организационно-правовых мер обеспечения информационной безопасности. Их совокупность означает подбор, проверку, инструктаж персонала, обеспечение программно-технических работ, назначение лиц, отвечающих за конкретные участки (оборудование), осуществление режимности (в том числе секретной), физическую охрану объектов, а также оборудование помещений физическими средствами защиты.

Научное исследование выполнено в рамках темы «Информационная безопасность учётно-аналитической системы стратегического управления в бизнесе» при финансовой поддержке Белорусского республиканского фонда фундаментальных исследований.

Использованные источники

1. Концепция национальной безопасности Республики Беларусь: Указ Президента Респ. Беларусь, 9 ноября 2010 г., № 575.

2. О коммерческой тайне: Закон Респ.Беларусь от 5 янв.2013г. №16-З.

3. Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: http://www.pravo.by. – Дата доступа: 24.02.2023.