УДК 004.01; 340.14

ЗАКОНОДАТЕЛЬНАЯ БАЗА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СЕТЕЙ

Р.А. Божко, магистрант факультета информационной безопасности,
Т.А. Пулко, канд. техн. наук, доц., доц. кафедры защиты информации
Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь

Проведен подбор и анализ законодательной базы в области информационной безопасности, рассмотрены основные термины и определения, способы организации информационной безопасности предприятия, полномочия организаций регулирующих информационную безопасность предприятий.

Ключевые слова: *информационная безопасность, несанкционированный доступ, средства технической защиты информации, информационные технологии, информационные системы.*

Информационная безопасность предприятий является составной частью экономической независимости и благосостояния государства. Если в организации вовремя не внедрить систему безопасности, то это может привести к утечке информации (данных), необратимым последствиям (техногенной катастрофе), ликвидации (прекращению оказания услуг) предприятия. Тогда под «информационной безопасностью предприятия» можно рассматривать выполнение следующих критериев: работоспособность сервисов (сайта) предприятия; защиту важной информации (персональные данные, служебные и коммерческие тайны); требования регуляторов (нормативно-правовых актов).

Так на законодательном уровне определяются основные направления деятельности республиканских и местных органов власти и управления в области защиты интересов государства в информационной сфере.

Функции государственной системы в сфере обеспечения информационной безопасности:

- оценка состояния информационной безопасности в государстве;
- выявление и учет внешних и внутренних источников угроз информационной безопасности, проведение их мониторинга;
- организация проведения фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности;
- разработка и принятие нормативных правовых актов;
- разработка единой системы лицензирования и сертификации в данной области;
- информирование общества о реальном состоянии безопасности общества;
- защита прав и свобод человека.

Важнейшим специализированным нормативным правовым актом в области информационной безопасности является Указ Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации», которым

утверждено Положение о технической и криптографической защите информации в Республике Беларусь (далее Положение) [1]. Данное Положение дает определение важных терминов в сфере защиты информации, а именно:

1) несанкционированное воздействие на информацию – изменение или уничтожение информации, осуществляемое с нарушением установленных прав или правил;

2) несанкционированный доступ к информации – доступ к информации, осуществляемый с нарушением установленных прав или правил разграничения доступа;

3) средства технической защиты информации – технические, программные, программно-аппаратные средства защиты информации, предназначенные для защиты информации от ее утечки по техническим каналам, несанкционированного доступа, несанкционированных воздействий на информацию, блокирования правомерного доступа к ней, иных неправомерных воздействий на информацию, а также для контроля эффективности ее защищенности;

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

5) утечка информации по техническим каналам – неконтролируемое распространение информации от объекта информатизации через физическую среду до технического средства, осуществляющего перехват информации и другие термины [1].

Можно рассмотреть несколько способов в организации информационной безопасности предприятия:

– Неправильный – когда средства равномерно расходуются на защиту всех составных частей информационной безопасности предприятия.

– Частичный– когда обеспечивается безопасность тех составляющих, которые определены нормативно-правовыми актами, заключается в следовании нормативам регуляторов, когда компания обеспечивает безопасность тех узлов ИТ-инфраструктуры, которые требует государство.

– Правильный– когда на предприятии определяются основные угрозы безопасности и выстраивается последовательность мероприятий по их нейтрализации.

Опасность атаки определяют по специальной модели угроз, которая может решить вопросы: какими ресурсами располагают злоумышленники и сколько времени они готовы потратить на атаку?

В Республики Беларусь действует специально уполномоченный государственный орган, который осуществляет регулирование деятельности по защите информации – Оперативно-аналитический центр при Президенте Республики Беларусь. Деятельность данного государственного органа регламентирована Положением, которое устанавливает следующие полномочия:

1) определяет приоритетные направления технической и криптографической защиты информации;

2) координирует деятельность организаций по применению мер технической и криптографической защиты информации;

3) осуществляет контроль за технической и криптографической защитой информации в организациях и другие полномочия;

4) определяет порядок: технической защиты государственных секретов; технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам; аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам;

5) организует и осуществляет техническое нормирование и стандартизацию по вопросам технической и криптографической защиты информации;

6) осуществляет: лицензирование деятельности по технической и (или) криптографической защите информации; подтверждение соответствия и проведение государственной экспертизы средств технической и криптографической защиты информации, за исключением криптографических средств защиты государственных секретов, определяет порядок проведения такой экспертизы…

На сегодня созданы десятки решений информационной безопасности предприятия, в том числе и технические.

Система обеспечения информационной безопасности Республики Беларусь является частью системы обеспечения национальной безопасности страны.

Так, решением Всебелорусского народного собрания от 25.04.2024 №6 была утверждена Военная доктрина Республики Беларусь (далее Доктрина) [2], где определены военные опасности, угрозы, конфликты в области информационной сферы:

– космическое пространство и информационная сфера используются в борьбе за ресурсы и пути перемещения финансов, услуг и интеллектуальных продуктов… (Раздел II, гл. 3, ст. 18).

Одной из потенциальных внешних военных опасностей для Республики Беларусь является:

– декларация в доктринальных документах иностранных государств (коалиций государств) возможности вредоносного информационно-технического воздействия на критически важные объекты инфраструктуры Республики Беларусь (Гл. 4, § 2, ст.26.4).

– создание и подготовка другими государствами (коалициями государств) специализированных центров по вредоносному информационно-техническому воздействию на критически важные объекты инфраструктуры Республики Беларусь (Гл. 4, § 2, ст. 27.4);

– явное или скрытое вредоносное информационно-техническое воздействие на критически важные объекты инфраструктуры Республики Беларусь (Гл. 4, § 2, ст.28.4).

Кроме того в Доктрине определены военная политика государства и ее реализация, где сказано, что для пресечения или предотвращения вредоносного информационно-технического воздействия, ведущего к нарушению устойчивой работы критически важных объектов инфраструктуры государства, Республика Беларусь будет использовать все силы и средства как несилового, так и силового характера в соответствии с законодательством, регламентирующим вопросы информационной безопасности (раздел III, гл.7, ст.60, абз.2) [2].

Также в Республике Беларусь принят Закон от 10.11.2008 №455-З «Об информации, информатизации и защите информации» (с изменениями и дополнениями) (далее Закон) [3]. В данном Законе глава 7 полностью посвящена защите информации.

Целями защиты информации (в соответствии со ст. 27 Закона) являются:

– обеспечение национальной безопасности, суверенитета Республики Беларусь;

– сохранение и неразглашение информации о частной жизни физических лиц и персональных данных, содержащихся в информационных системах;

– обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем и информационных сетей, использовании информационных технологий, а также формировании и использовании информационных ресурсов;

– недопущение неправомерного доступа, уничтожения, модификации (изменения), копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий [3].

Также, Положение определяет порядок технической защиты информации (глава 3 Положения), порядок криптографической защиты информации (глава 4 Положения), осуществление контроля за технической и криптографической защитой информации (глава 5 Положения) [1].

С 1 января 2014 года введен в действие Технический регламент Республики Беларусь "Информационные технологии. Средства защиты информации. Информационная безопасность" (ТР 2013/027/BY) (далее Регламент) [4], который распространяется на выпускаемые в обращение на территории Республики Беларусь средства защиты информации независимо от страны происхождения, за исключением средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов (п. 1 ст. 1 Регламента). Регламент дает определения наиболее важным понятиям в регулируемой им сфере, в том числе и самой защите информации, под которой понимается комплекс правовых, организационных и технических мер по обеспечению целостности, конфиденциальности, доступности и сохранности информации (абз. 3 ст.2 Регламента) [3, 4].

Следует отметить, что Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 17.12.2013 № 94 «О перечне технических нормативных правовых актов, взаимосвязанных с техническим регламентом ТР 2013/027/BY» устанавливает обширный перечень технических нормативных правовых актов, взаимосвязанных с Регламентом и регулирующих вопросы информационной безопасности, например: СТБ 34.101.37-2011 Информационные технологии. Методы и средства безопасности. Профиль защиты программных средств. Система управления сайта и др. [4].

Исходя из требований руководящих документов внедрение системы безопасности на предприятии можно разделить на несколько этапов: 1) определение угроз; 2) определение основных элементов, на которые направлены угрозы; 3) определение мероприятий по защите этих элементов.

Для предотвращения утечки информации необходимо принимать организационные меры (введение регламентов и инструкций, которые бы структурировали работу

с ИТ-системами; необходимо соблюдать режим коммерческой (служебной) тайны на предприятии; принимать технические меры по защите информации.

За нарушение общественного порядка в сфере информационной безопасности в соответствии с Кодексом Республики Беларусь об административных правонарушениях установлена административная ответственность за следующие виды правонарушений: несанкционированный доступ к компьютерной информации; нарушение законодательства о защите персональных данных; нарушение правил оборота специальных технических средств, предназначенных для негласного получения информации [5].

За более серьезные нарушения общественного порядка, повлекшее значительный ущерб, в соответствии с Уголовным кодексом Республики Беларусь установлена уголовная ответственность: несанкционированный доступ к компьютерной информации; уничтожение, блокирование или модификация компьютерной информации; неправомерное завладение компьютерной информацией; разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств; нарушение правил эксплуатации компьютерной системы или сети [6].

Тогда под информационной безопасностью предприятия можно рассматривать комплекс мероприятий, которые ограничиваются регуляторами и направлены на исключение несанкционированного доступа, утечки, изменения, и т.д. какого-либо рода данных (информации).

ЛИТЕРАТУРА

1. «О некоторых мерах по совершенствованию защиты информации», Указ Президента Республики Беларусь от 16.04.2013 № 196. – Режим доступа: https://pravo.by/.
2. Решение Всебелорусского народного собрания от 25.04.2024 №6 об утверждении Военной доктрины Республики Беларусь. – Режим доступа: https://pravo.by/.
3. Закон от 10.11.2008 №455-З «Об информации, информатизации и защите информации» (с изменениями и дополнениями). – Режим доступа: https://pravo.by/.
4. Постановление совета министров Республики Беларусь об утверждении с 1 января 2014 года технического регламента Республики Беларусь "Информационные технологии. Средства защиты информации. Информационная безопасность" (ТР 2013/027/BY). – Режим доступа: https://pravo.by/.
5. Кодекс Республики Беларусь об административных правонарушениях от 6.01.2021 №91-з (с изменениями и дополнениями). – Режим доступа: https://pravo.by/.
6. Уголовный кодекс Республики Беларусь от 9.07.1999 №275-з (с изменениями и дополнениями. – Режим доступа: https://pravo.by/.