УДК-351.746.1

Е.Е. Оспанов

Докторант Академии Комитета национальной безопасности РК, Казахстан, г. Алматы
E- mail: erlos@mail.ru

Правовые аспекты обеспечения защиты электронных информационных ресурсов

В данной статье рассмотрены правовые аспекты обеспечения защиты электронных информационных ресурсов. Проанализированы законодательные нормы защиты информационных ресурсов. Автором предложена формулировка цели защиты электронных информационных ресурсов и информационных систем. Обозначены понятия конфиденциальности, целостности и доступности информации. В статье рассмотрены определения защиты информации и ее правовой охраны.
Ключевые слова: информация, информационная безопасность, электронные информационные ресурсы, защита информации, меры защиты информации.

Y.E. Ospanov

Legal aspects of the protection of electronic information resources

This article discusses the legal aspects of the protection of electronic information resources. Analyzed legislation norms of protection of information resources. The author it is offered the formulation of the purpose of protection of electronic information resources and information systems. Designated the concepts of confidentiality, integrity and availability of information. The article describes the determination of information security and legal protection.
Key words: information, information security, electronic information resources, information security measures.

Е.Е. Оспанов

Электронды ақпарат ресурстарын қорғауды қамтамасыз етудің құқықтық аспектілері

Мақалада электронды ақпарат ресурстарын қорғауды қамтамасыз етудің құқықтық аспектілері қарастырылған. Ақпарат ресурстарын қорғаудың заңды нормалары талданған. Автормен электронды ақпарат ресурстарын және ақпараттық жүйені қорғау мақсатының анықтамасы ұсынылған. Ақпараттың құпиялық, тұтастық және қол жетімділік ұғымы анықталған. Мақалада ақпаратты қорғау және оны құқықтық күзету түсінігі қарастырылған.
Түйін сөздер: ақпарат, ақпараттық қауіпсіздік, электронды ақпарат ресурстары, ақпаратты қорғау, ақпаратты қорғау шаралары.

Концепцией информационной безопасности Республики Казахстан определено, что к критическим важным объектам информатизации относятся объекты информационной и телекоммуникационной инфраструктуры, прекращение или нарушение функционирования которых приводит к чрезвычайной ситуации или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства или инфраструктуры страны [1].

Рассматривая Главу 8 «Защита электронных информационных ресурсов и информационных систем» Закона Республики Казахстан «Об информатизации», необходимо отметить, что законодатель отдает приоритет мерам по охране электронных информационных ресурсов, а не по восстановлению нарушенного права и пресечения действий, нарушающих право. Закон трактует, в первую очередь, не о правовой защите, а о правовой охране информации и, соответственно, электронных информационных ресурсов.

Следует отметить, что «охрана» ориентирует применение мер противодействия, что называется по факту посягательств, т.е. занимает некую выжидательную позицию по отно-

шению к возможным посягательствам. Например, охрана личной тайны изначально исходит из презумпции ее соблюдения всеми членами общества в рамках соответствующей правовой обязанности. Меры же реагирования срабатывают, когда этой тайне непосредственно наносится ущерб. Например, гражданин обратился за судебной защитой вследствие опубликования в СМИ отдельных аспектов его интимной жизни.

Напротив, «защита» предполагает не только охранительные меры, но и активный упреждающий поиск противоправных устремлений к соответствующим сведениям. Само слово «защита» констатирует, что такие устремления имеют не эпизодический, а постоянный направленный характер, государство заранее знает об их существовании как явлении объективной действительности.

В статье 41 Закона Республики Казахстан «Об информатизации» закреплены цели защиты электронных информационных ресурсов, в частности указано:

1. Защита электронных информационных ресурсов и информационных систем заключается в принятии правовых, организационных и технических (программно-технических) мер в целях:

1) обеспечения целостности и сохранности электронных информационных ресурсов, недопущения их несанкционированного изменения или уничтожения;

2) соблюдения конфиденциальности электронных информационных ресурсов ограниченного доступа;

3) реализации права на доступ к электронным информационным ресурсам;

4) недопущения несанкционированного воздействия на средства обработки и передачи электронных информационных ресурсов [2].

В теории информационной безопасности определяют три вида опасностей для информационной системы: нарушения конфиденциальности, целостности и доступности информации.

Конфиденциальности информации – свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса [3].

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменения осуществляются только преднамеренно субъектами, имеющими на это право.

Доступность информации – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать ее беспрепятственно [4].

Таким образом, конфиденциальность, целостность и доступность являются определяющими свойствами информации.

С учетом определенных свойств информации, автором предлагается изложить цель защиты информации в следующей формулировке: «целью защиты электронных информационных ресурсов и информационных систем является обеспечение правовыми, организационными и техническими (программно-технических) мерами конфиденциальности, целостности и доступности информации».

В рамках защиты государственных электронных информационных ресурсов защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Понятие «подлежит защите», имеет двойное значение. С одной стороны, правовые нормы предусматривают общее основание для установления режима доступа к электронным информационным ресурсам. Способность информации быть обращенной во вред субъекту отношений также дает субъекту право на защиту своих законных интересов. С другой стороны, неправомерное обращение с документированной информацией может нанести ущерб собственнику, владельцу, пользователю, иному лицу, что приводит к необходимости установления мер, препятствующих ее общеизвестности.

Право на информацию предполагает, что ее владелец может принимать превентивные меры по ограничению доступа к ней, а также требовать от других лиц не нарушать установленный режим доступа [5].

Как предусмотрено статьей 43 Закона Республики Казахстан «Об информатизации», к мерам защиты электронных информационных ресурсов и информационных систем относятся следующие:

– к правовым мерам защиты электронных информационных ресурсов относятся заключаемые собственником или владельцем электронных информационных ресурсов с пользовате-

лями информации договоры, в которых устанавливаются условия доступа к определенным электронным информационным ресурсам и ответственность за нарушение условий доступа и использования электронных информационных ресурсов;

– к организационным мерам защиты электронных информационных ресурсов и информационных систем относятся обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (к материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации;

– к техническим (программно-техническим) мерам зашиты электронных информационных ресурсов и информационных систем относятся меры по физической защите информационных систем, использование средств защиты информации, в том числе криптографических, а также систем контроля доступа и регистрации фактов доступа к информации.

Государственное регулирование отношений в сфере зашиты электронных информационных ресурсов осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Республики Казахстан о защите информации.

Меры, принимаемые собственником электронных информационных ресурсов или уполномоченными лицами, должны быть направлены, прежде всего, на ограничение доступа к конфиденциальной информации. Такие меры могут носить юридический, организационный; экономический или технический характер. Они должны быть адекватны ценности информации и соответствовать законодательству.

Закон Республики Казахстан «Об информатизации» в п. 2 ст. 42 закрепил, что собственник, владелец или национальный оператор информационной системы обязаны принимать меры, обеспечивающие:

– предотвращение несанкционированного доступа к электронным информационным ресурсам;

– своевременное обнаружение фактов несанкционированного доступа к электронным информационным ресурсам, если такой несанкционированный доступ не удалось предотвратить;

– минимизацию неблагоприятных последствий нарушения порядков доступа к информации;

– недопущение воздействия на средства обработки и передачи электронных информационных ресурсов:

– возможность скорейшего восстановления электронных информационных ресурсов, измененных либо уничтоженных вследствие несанкционированного доступа к ним.

Контроль эксплуатации государственных электронных информационных ресурсов реализуется путем осуществления процедуры обязательной сертификации. Статья 20 Закона Республики Казахстан «Об информатизации» устанавливает, что для обеспечения надежности и безопасности функционирования государственных информационных систем технические средства, которые используются для хранения, обработки и передачи электронных информационных ресурсов, должны соответствовать требованиям в области технического регулирования.

Как установлено ст. 45 Закона Республики Казахстан «Об информатизации», нарушение законодательства Республики Казахстан об информатизации влечет ответственность в соответствии с законами Республики Казахстан. Однако в Законе не указан конкретный вид ответственности за нарушение законодательства об информатизации.

На законодательном уровне защита электронных информационных ресурсов обеспечивается уголовно-правовыми, административно-правовыми мерами.

При этом остаются нерешенными проблемы, связанные с непроработанностью правовых механизмов, регулирующих информационные правоотношения при создании и применении информационных систем, их сетей, средств обеспечения, телекоммуникационной инфраструктуры.

Указанные проблемы являются следствием несогласованности единой политики обеспечения противодействия информационным преступлениям и противоречивости правовых норм.

Литература

1. Указ Президента Республики Казахстан от 14 ноября 2011 года № 174 «О Концепции информационной безопасности Республики Казахстан до 2016 года», http://www.ru.government.kz/docs/u110000017420111114.htm.
2. Закон Республики Казахстан от 11 января 2007 года «№217-III «Об информатизации», http://online.zakon.kz.
3. ГОСТ РИСО/МЭК 1335-1-2006 Информационные технологии. Методы и средства обеспечения безопасности.
4. Международный стандарт ИСО/МЭК 27001-2005 Информационные технологии. Методы защиты. Системы менеджмента защиты информации.
5. Зенин И.А. Интеллектуальная собственность и ноу-хау: учебное практическое пособие. – М.: МЭСИ, 2001.

References

1. Ukaz Prezidenta Respubliki Kazakhstan ot 14 noyabrya 2011 goda № 174 « O Kontseptsii informatsionnoy bezopasnosti Respubliki Kazakhstan do 2016 goda», http://www.ru.government.kz/docs/u110000017420111114.htm
2. Zakon Respubliki Kazkhstan ot 11 yanvarya 2007 goda №217-III « Ob informatizatsii», http://online.zakon.kz
3. GOST R ISO/MEK 1335-1-2006 Informatsionnye tekhnologii. Metody I sredstva jbespecheniya bezopasnosti.
4. Mezhdunarodnyy standart ISO/MEK 27001-2005 Informatsionnye tekhnologii. Metody i sredva zashchity. Sistemy menedzhmenta zashchity informatsii. Trebovaniya.
5. Zenin I.A. Intellektufknaya sobstvennost I nou-hau: Uchebnoe prakticheskoe posobie. – M.: MESI, 2001.