Кожуркина Олеся Алексеевна
студентка
Михнев Илья Павлович
канд. техн. наук, доцент
Волгоградский институт управления (филиал)
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте РФ»
г. Волгоград, Волгоградская область

DOI 10.21661/r-467735

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ЮРИДИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Аннотация: *в статье рассмотрена проблема обеспечения защиты информации с точки зрения юридической деятельности. В работе также представлен перечень нормативно-правовых документов, позволяющих детально проанализировать тему безопасности информационных данных.*

Ключевые слова: *информационная безопасность, нормативно-правовой документ, информация, информационные сведения.*

Для того чтобы всесторонне раскрыть тему информационной безопасности в первую очередь необходимо определить в чем суть понятия «информация». Информация по своей сущности является продуктом человеческой деятельности, который не подвержен физическому старению, но обладает свойством быстрого распространения. В данном контексте понимают уровень актуальности какого-либо знания, его ценность на данный момент времени. Информация определяет уровень прогресса всех сфер человеческой деятельности, является основой для накопления и расширения опыта предыдущих поколений. Именно поэтому в настоящее время ее определяют как один из приоритетных факторов производства. Однако, произвольное распространение информации, ее использование посторонними субъектами может быть чревато попаданием в руки

злоумышленников. В данном случае необходимо предупреждение любого несанкционированного доступа к информационным сведениям [1; 2].

Информационная безопасность предполагает обеспечение защиты информации от похищения умышленного или случайного характера. Для обеспечения информационной безопасности необходимо эффективно организовать защиту интересов собственников информации. Но для того, чтобы должное осуществление защиты наладить в полной мере, необходимо ознакомиться с понятием информационной безопасности, ее целях и методах обеспечения.

Понятие безопасности информации подразумевает условия, при которых, изменение, удаление, модерация любого рода сведений является невозможной для не обладающих конкретными правами субъектов. Соответственно, целью защиты информации является снижение возможных потерь по причине нарушения требований к свойствам информации. Под свойствами понимается целостность информации – определяет качество данных сведений, их системность; конфиденциальность – предполагает негласность конкретного источника данных; доступность информационных сведений – быстрое нахождение пользователями нужной им информации [2].

Сущность термина «информационная безопасность» подразумевает ситуацию, исключающую возможность пользования информацией посторонними субъектами. Поэтому для формирования режима информационной безопасности как комплексной проблемы выделяют следующие меры по ее решению. Их подразделяют на пять уровней [1, 2]:

– законодательный: издание законов, нормативно-правовых актов и т. д.;

– морально-этический: регулирование нормами поведения, несоблюдение которых вызывает порицание со стороны общества как регулятора деятельности определенного индивида;

– административный: действия, предпринимаемые руководителями в случае нарушения;

– физический: механические и электронные препятствия на пути проникновения потенциального нарушителя;

– аппаратно-программный: использование специальных программ для защиты информации.

Информация может быть подвержена неправомерным действиям, находясь в распоряжении, как частных лиц, организаций, предприятий, так и в государственных учреждениях. Необходимость сохранения государственной и частной информации заставила многие страны принять ряд мер, направленных на защиту информационных сетей.

Так, в Конституции РФ содержатся нормы (гл. 23, 29, 41, 42), которые затрагивают отношения в сфере информационной безопасности. Например, статья 23 пункт 2 регламентирует право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. В статье 29 закреплено право свободно осуществлять поиск, получать, передавать, производить и распространять информацию любым законным способом. Главы 41 и 42 гарантируют право на знание достоверных фактов, обязательств, создающих угрозу, как людям, так и окружающей среде [5].

В случае нарушения конфиденциальности информации предусматриваются наказания, закрепленные в Уголовном кодексе РФ. Глава 28 «Преступление в сфере компьютерной информации» содержит статьи (272–274), которые описывают преступления, связанные с неправомерным доступом к цифровой информации (ст. 272); созданием, использованием и распространением вредоносных скриптов и компьютерных программ (ст. 273), и нарушением правил эксплуатации устройств и средств хранения, обработки или передачи информации и информационно – телекоммуникационных сетей (ст. 274) [3].

В законе также предусматриваются интересы государства. В вышеупомянутой статье 29 Конституции РФ пункт 4 закреплен перечень сведений, который является государственной тайной и определяется федеральным законом. Гарантом обеспечения конфиденциальности сведений, принадлежащих государству, выступает Закон РФ от 21 июля 1993 г. «О государственной тайне». В нем определяется понятие «государственной тайны» как защищаемые государством сведения в области его военной, внешнеполитической, экономической,

разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Также содержится перечень сведений, составляющих основу государственной тайны; определяется порядок отнесения сведений к государственной тайне и дается описание средств защиты информации данного вида. Он включает в себя технические, криптографические, программные средства защиты информации, не подлежащей огласке [4; 6].

При разглашении государственной тайны в силу вступает статья 283 Уголовного кодекса РФ. Она определяет условия совершения преступления, назначает срок наказания посредством разграничения преступления на умышленное и по неосторожности.

Наблюдение за исполнением требований, а также обеспечение правовой защиты системы информации возложены на органы государственной власти. Тем не менее, подобный контроль может осуществлять и сам владелец информации. Закон не может ограничивать какой-либо реестр информационных данных. Исключением является только сведения, носящие характер государственной тайны. Согласно Доктрине РФ, утвержденной указом Президента Российской Федерации от 5 декабря 2016 г., информационные сведения и их защита являются основополагающими элементами безопасности государства и общественности.

Список литературы

1. Михнев И.П. Информационная безопасность в современном экономическом образовании // Международный журнал прикладных и фундаментальных исследований. – 2013. – №4. – С. 111–113.

2. Основы информационной безопасности хозяйственной деятельности: учебное пособие / И.П. Михнев; ВФ ФГБОУ ВПО «Российская академия народного хозяйства и государственной службы». – Волгоград: Изд-во ВФ ФГБОУ ВПО РАНХиГС, 2013. – 144 с.

3. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 26.08.2017). // Собрание законодательства Российской Федерации. – 17 июня 1996 г. – №25.

4. Федеральный закон от 21 июля 1993 г. №5485-1 «О государственной тайне» // Собрание законодательства Российской Федерации.

5. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 №6-ФКЗ, от 30.12.2008 №7-ФКЗ, от 05.02.2014 №2-ФКЗ, от 21.07.2014 №11-ФКЗ) // Собрание законодательства РФ. – 2014. – №15.

6. Бабаш А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2013. – 136 с.