СУЩНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д. Устинов, *магистрант*
Сибирского института управления, филиал Российской академии народного хозяйства и государственной службы
(Россия, г. Новосибирск)

Аннотация. *В статье рассмотрены вопросы сущности информационной безопасности. Проведен анализ легального определения данной категории. Исследованы основные аспекты защищенности, как цели информационной безопасности. Предложено понимание содержания информационной безопасности исходя из формирования активной защиты критических интересов и пассивной защиты, как создания условий для развития общества и экономики. Показаны различия в методах обеспечения информационной безопасности по данным направлениям.*

Ключевые слова: *информационная безопасность, состояние защищенности, критическая инфраструктура, критические интересы, активная защита, пассивная защита, общественное и экономическое развитие.*

Развитие современного общества во многом основывается на использовании информационных ресурсов. Информация перестала быть только одним из факторов производства, а управление информацией не является более прерогативой только корпоративных структур. Информация выступает также особого рода общественным активом, причем его особенностью следует считать формирование одновременных позиций представителей общества как потребителей информации и как участников ее создания. Развитию роли информации в обществе способствует не только создание новых средств связи и алгоритмов обработки информации, воплощенных в программные продукты. Основной движущей силой роста значимости информации для общества и экономики следует считать изменение отношения к информации. Сегодня информация становится продуктом, одновременно определяет условия общественного развития. Поэтому безусловную значимость приобретает последовательная реализация концепции информационной безопасности.

В настоящее время концепции информационной безопасности созданы на государственном уровне во многих странах мира. Причина достаточно очевидна, связана с практическими потребностями в предупреждении отрицательных последствий воздействия на экономическую и общественную инфраструктуру вредоносного программного обеспечения (ПО), а также других факторов, создающих угрозы для развития информационной сферы общества. Тем не менее, на сегодняшний день границы понятия информационной безопасности в полной мере не определены, хотя данное понятие и представлено, в том числе, на уровне российского законодательства.

Вполне очевидно, что, в отсутствие четкого понимания информационной безопасности, в частности, обозначения границ, в которых политика информационной безопасности должна проводиться, невозможно и выработать по-настоящему эффективные меры, обеспечивающие отсутствие угроз критического воздействия на объекты информационной инфраструктуры, а также жизнь общества. По меньшей мере, в отсутствие однозначного понимания сущности информационной безопасности, в том числе, ее границ, не могут быть при разумных затратах созданы системы защиты информации (СЗИ – структуры, технические средства и ПО для обеспечения информационной безопасности), а также распределены элементы по уровням ответственности.

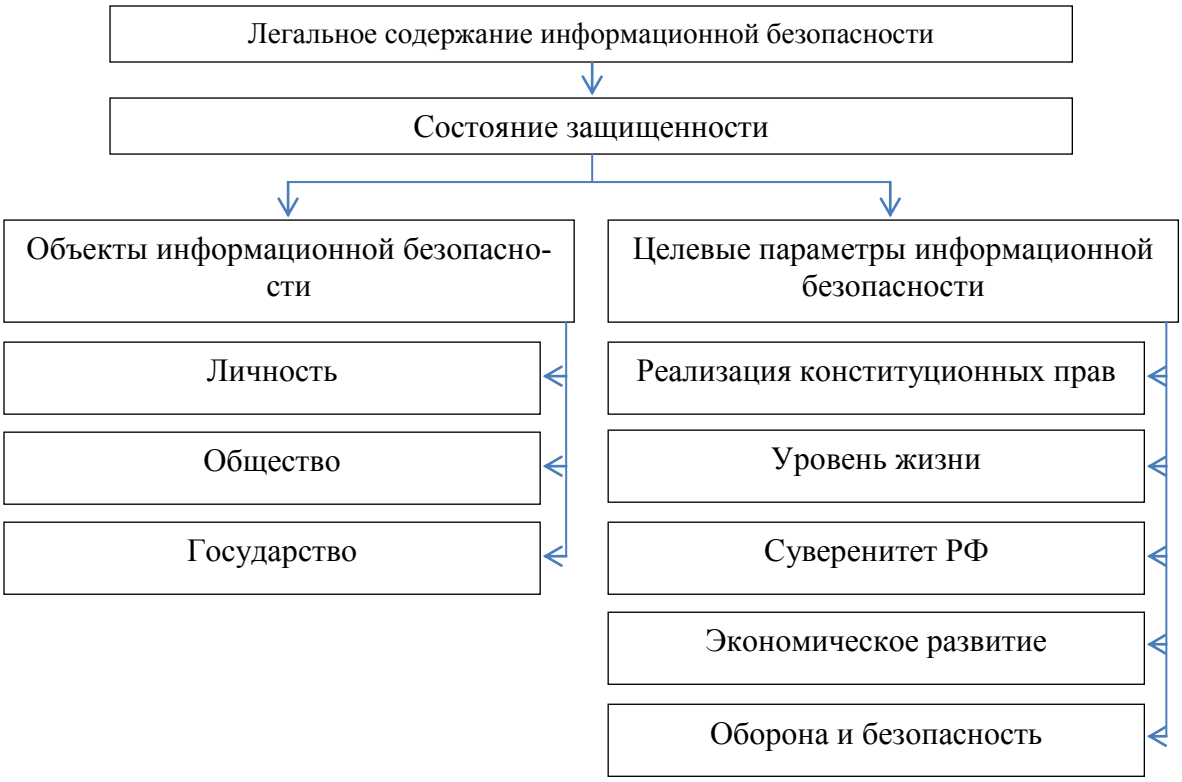

Рис. 1. Элементы легального определения информационной безопасности

В частности, легальное определение информационной безопасности сформировано в п. 2 Доктрины информационной безопасности [5]. Для наглядности элементы легального определения информационной безопасности представлены на рисунке 1. Информация, представленная на нём, показывает, что элементы легального определения содержат указания на перечень объектов, в отношении которых должно быть реализовано «состояние защищенности», а также на целевые параметры этих объектов. По существу, сформирован концептуальный перечень объектов и условий, которым следует руководствоваться при выстраивании информационной безопасности государства. Тем не менее, в легальном определении следует, прежде всего, отметить отсутствие четко обозначенного понятия защищенности. Защищенность может толковаться с точки зрения отсутствия угроз, способности СЗИ активно противодействовать угрозам, либо способности не допускать воздействия угроз на объекты защиты.

Характеристики защищенности, пригодные для локальных СЗИ, создаваемых, как правило, в крупных компаниях, либо в органах власти, не в полной мере подходят для глобального понимания информационной безопасности, поскольку, с учетом п. 8 Доктрины [5], информационная безопасность должна означать, по существу, защищенность всех наиболее значимых сторон общественной жизни и государственного управления. В подобных масштабах меняется сама суть информационной безопасности, поскольку речь идет уже о выстраивании общественных отношений, более того, о формировании принципиально иного, по сравнению с существующим подхода к пониманию защищенности.

Свойство защищенности как ключевая характеристика сущности информационной безопасности не может пониматься как контроль в отношении каждого байта информации, которой обмениваются пользователи, и каждого гаджета, который потенциально может стать объектом хакерской атаки. Это практически невозможно обеспечить при разумных экономических затратах. Не менее важен фактор общественной эффективности поскольку обеспечения защищенности в любом случае означает определенные затраты общества, ограничения, с которыми оно может столкнуться при реализации мер информационной безопасности. Поэтому обще-

ственные затраты на обеспечения информационной безопасности должны быть, по меньшей мере, приемлемы. Отсюда, очевидно, может быть сформулировано и расширенное понимание информационной безопасности как наличия активной защиты, направленной на предупреждение ущерба критической инфраструктуре, наравне с созданием условий для нормальной деятельности общества, включая развитие экономики.

Составляющая создания нормальных условий общественного развития определяется особой значимостью функционирования информации на уровне общества, ее ролью в экономическом развитии, особенно когда речь идет о производственных отношениях. Как правило, использование концепции информационной безопасности на основе СЗИ ведет к ограничениям в плане свободного обращения информации, что соответствует активному уровню защиты в обеспечении информационной безопасности. Напротив, создание условий для общественного развития означает отсутствие пассивных угроз информационной сфере развития общества. В частности, очевидно, что активное развитие платформ для смартфонов определяется общественными интересами, но возможность ограничения функционала этих платформ сторонними пользователями либо третьими государствами составляет, безусловно, угрозу информационной безопасности. В то же время, это угроза пассивного характера. Поэтому, вероятно, более предпочтительно не блокировать угрозы (в случае с платформами для смартфонов это сделать нереально), а развивать на национальном уровне индустрию ПО, способную обслуживать общественные потребности в области обмена информацией.

Тогда, с учетом характеристик национальных интересов в области информационной безопасности, ее содержание может быть представлено в виде рисунка 2. Из рисунка 2 видно, что способы реализации защищенности в рамках информационной безопасности различаются в зависимости от приоритетов. При этом понятие критической инфраструктуры, очевидно, может быть включено в более широкое понятие критических интересов. В частности, с учетом безопасности персональных данных, сюда же относится безопасность личной информации. При этом данное понятие шире только понятия персональных данных, установленного ст. 7 Закона «О персональных данных» [2], и включает в себя, вопросы безопасности персональной финансовой и инфой личной информации. Поэтому более обоснованным было бы понимать личные данные как социальные ценности, указанные в ч. 1 ст. 24 Конституции РФ [1] и иную конфиденциальную информацию. В этом смысле информационная безопасность в порядке активной защиты должна быть направлена на предупреждение несанкционированного доступа к данной информации. Кроме того, следует включить в перечень объектов активной защиты нормальные условия эксплуатации средств информационной безопасности и критической инфраструктуры. В отличие от защиты критической инфраструктуры, имеется ввиду создание таких механизмов, которые в комплексе предупреждают воздействие на данные объекты, причем в их взаимосвязи (рис. 2.).

Рис. 2. Содержание информационной безопасности

Вопрос отнесения международных интересов к критическим интересам выступает в достаточной мере дискуссионным, тем не менее, создание условий для общественного и экономического развития, кроме международного сотрудничества, относится к области информационной безопасности внутри страны.

В то же время, на международном уровне используется понятие «мягкой силы», что на практике, не исключает возможности давления на российские интересы со стороны международного сообщества. Более того, поскольку подобный опыт существует, очевидно, что в этом отношении должна существовать определенная активная защита.

Область пассивной защиты может быть определена как все интересы, не включенные в перечень критических, в первую очередь, это свобода обращения информации и условия для развития экономики, в том числе, отдельных отраслей. Одной из составляющих условий общественного развития следует считать формирование реальных возможностей для участия общества в делах государства и создания институтов взаимодействия государства с обществом, в частности, в рамках общественного контроля [3] и общественных инициатив [4]. Развитие общества означает развитие культуры, причем в широком понимании, в том числе, это возможность для приобщения к культурной жизни, особенно в тех случаях, когда иным способом такое приобщение невозможно. Наиболее характерным примером выступают районы Крайнего Севера, где доступ в Интернет является порой единственным способом контакта с цивилизацией, в том числе, знакомства с культурными новинками. Очевидно, что подобный аспект информационной безопасности не менее важен, чем другие. Реализация данных составляющих информационной безопасности различается методами и средствами. В от-

ношении критических интересов преобладают административные методы, связанные с запретами. С организационной точки зрения преобладают технические методы достижения защищенности. В отношении общественного развития должны использоваться методы дозволения, при этом преобладать должны средства экономического поощрения общественного развития. Прежде всего, это должно быть финансирование развития данных областей в сочетании с другими экономическими стимулами. При этом, с учетом представленных границ информационной безопасности, можно более обоснованно говорить и о распределении обязанностей в области ее обеспечения между различными уровнями власти. В частности, вполне очевидна роль региональных властей в обеспечении информационной безопасности с точки зрения развития общества и экономики на уровне отдельных регионов. Региональные власти в пределах полномочий должны формировать механизмы пассивной защиты в отношении общественного и экономического развития.

Таким образом, сущность информационной безопасности предлагается определить как создание активной защиты в отношении критических интересов, направленной, в первую очередь, на предупреждение ущерба критической инфраструктуре, а также формирование условий для нормального развития экономики и общества. Защищенность в данных областях реализуется различными способами. В отношении критических интересов преобладают административные методы, используются средства технической защиты данных. В отношении общественного и экономического развития преобладает метод дозволения, преимущественно используются средства экономического поощрения развития общества и экономики с точки зрения их информационной безопасности.

Библиографический список

1. *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) // СЗ РФ. – 04.08.2014. – № 31. – ст. 4398.

2. *О персональных данных*: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 29.07.2017) // СЗ РФ. – 31.07.2006. – № 31 (1 ч.). – ст. 3451.

3. *Об основах общественного* контроля в Российской Федерации: Федеральный закон от 21.07.2014 № 212-ФЗ (ред. от 03.07.2016) // СЗ РФ. – 28.07.2014. – № 30 (Часть I). – ст. 4213.

4. *О рассмотрении общественных* инициатив, направленных гражданами Российской Федерации с использованием интернет-ресурса «Российская общественная инициатива»: Указ Президента РФ от 04.03.2013 № 183 (ред. от 23.06.2014) // СЗ РФ. – 11.03.2013. – № 10. – ст. 1019.

5. *Об утверждении Доктрины* информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // СЗ РФ. – 12.12.2016. – № 50. – ст. 7074.

THE ESSENCE OF INFORMATION SECURITY

D. Ustinov, *graduate student*
Siberian institution of administration, branch of Russian presidential academy of national economy and public administration
(Russia, Novosibirsk)

Abstract. *The article covers the questions of the information security's substance. It contains the legal analysis of the one as well as the survey of different aspects concerning the information security. It is suggested to understand information security regarding to the active protection concerning the critical interests, and the passive protection which is the establishment of circumstances for social and economic development. Also the differences of these elements with respect to the methods of information security's establishment are stipulated in the article*

Keywords: *Information security, protection condition, critical infrastructure, critical interests, active protection, passive protection, social and economic development.*