УДК 38.04.04

Шахсуварова И.З.
Студент
2 курс, факультет «Государственное управление и национальная безопасность»
Института права и национальной безопасности
Российской Академии государственной службы и народного хозяйства
при Президенте Российской Федерации
Россия, г. Москва

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОНЯТИЯ

Аннотация. *В статье ставится задача раскрытия теоретического содержания понятия «информационная безопасность». Раскрывая сущностные аспекты информационной безопасности, исследуется уровень ее обеспечения в Российской Федерации.*

Ключевые слова. *Информационная безопасность, объект и субъект информационной безопасности, функция информационной безопасности.*

Keywords: *Information security, the object and subject of information security, the function of information security*

Annotation: *The article sets the task of revealing the theoretical content of the concept of "information security". It reveals and explores the essential aspects of information security and the level of its provision in the Russian Federation, as per investigation.*

Последствия четвертой промышленной революции привели к росту информатизации и цифровизации разных процессов и сфер жизнедеятельности. С другой стороны, это способствовало возникновению

возможностей нарушения целостности, конфиденциальности и доступности информации по отношению к разным субъектам – государству, экономическим агентам, отдельным индивидам. Для обеспечения предупреждения подобных инцидентов и возникла необходимость в формировании и внедрении системы информационной безопасности на разных уровнях функционирования общества, для разных сфер жизнедеятельности и субъектов.

На современном этапе развития общества информация выступает как форма собственности, и следовательно, имеет определенную ценность. Информационная безопасность постоянно развивается т.к. в связи с развитием технологий обработки и передачи информации постоянно возникают новые задачи по обеспечению информационной безопасности.

На законодательном уровне можно встретить определение информационной безопасности. Так, в Доктрине информационной безопасности Российской Федерации, где указывается, что информационная безопасность характеризует состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В соответствии со Стратегией национальной безопасности Российской Федерации под информационной безопасностью понимается состояние защищенности национальных интересов страны (личности, общества и государства) в информационной сфере от внутренних и внешних угроз.

Следовательно, можно сделать вывод, что информационная безопасность называется неотъемлемой частью политической, экономической, оборонной и других составляющих национальной безопасности.

Поскольку только в последнее время возросла активность в проведении научных исследований по проблемам информационной безопасности, то зачастую в научной литературе наблюдается существование различных подходов и направлений ее трактовки.

К.Н. Фадеева трактует информационную безопасность как совокупность средств обеспечения информационного суверенитета страны, защиту информационной сферы от внешних и внутренних информационных угроз. Эта безопасность должна включать в себя эффективное противодействие совокупности информационных угроз [Фадеева, 2019. С. 36].

А.В. Бабаш и Е.К. Баранова определили, что информационная безопасность – это составляющая национальной безопасности, процесс управления угрозами и опасностями, государственными и негосударственными институтами, отдельными гражданами, при котором обеспечивается информационный суверенитет Российской Федерации [Бабаш, 2017. С. 47].

Е.С. Зиновьева под информационной безопасностью понимает единство трех составляющих: обеспечение защиты информации; обеспечение защиты и контроля национального информационного пространства; обеспечение должного уровня информационной достаточности [Зиновьева, 2013. С.29].

Можно также встретить некоторые другие концептуальные подходы к пониманию информационной безопасности, а именно:

1) статический (безопасность как состояние защищенности информационной среды/информации, система гарантий и т.п.);

2) деятельностный (безопасность как процесс его обеспечения, способность государства эффективно защитить национальные интересы и ценности);

3) комплексный (безопасность как состояние и процесс).

В.В. Бордюже обосновал авторскую позицию, что наиболее приемлемым ввиду современной практики обеспечения информационной безопасности государства является последний. При таком подходе представляется целесообразным информационную безопасность государства рассматривать как перманентный процесс деятельности компетентных органов, направленный на предотвращение и противодействие угрозам в

информационной сфере, применение активных мер информационного воздействия, а также совокупность реализуемых условий и способных контролироваться длительное время. Этот подход основан на принципе, согласно которому основной целью обеспечения информационной безопасности является создание безопасной информационной среды [Бордюже, 2015. С.13].

Анализ существующих подходов к определению информационной безопасности позволил нам выделить два направления.

Первое направление касается подходов, определяющих информационную безопасность, исходя из ее свойств функционирования, как состояния, процесса и сферы деятельности.

Первый подход связывает информационную сохранность с состоянием защищенности, что не совсем, верно, так как она обеспечивает его, используя разные средства. То есть подобные определения делают упор на цель функционирования информационной безопасности.

Второй подход предполагает то, что информационная безопасность является процессом, включающим применение разного рода программных, технических, правовых, информационных и организационных инструментов для обеспечения функционирования ее основной цели. Также некорректно будет считать информационную безопасность только процессом, то есть последовательностью выполнения действий по защите, поскольку она может предусматривать реализацию ряда взаимосвязанных процессов, направленных на выявление и предупреждение угроз.

Третий подход достаточно широк, поскольку подчеркивает, что информационная безопасность является мультидисциплинарной сферой. Хотя можно согласиться с тем, что она является сферой деятельности, но такой подход делает ее только определенной разновидностью услуг. То есть представленные понятия только отражают один аспект информационной безопасности, связанный с ее функционированием, и не раскрывают другие,

которые достаточно важны для понимания ее сущности Поскольку последствия информационных угроз, предупреждение которых является главной задачей информационной безопасности, существенны для общества, то мы не согласны с такими трактовками в полной мере, поскольку они снижают ценность информационной безопасности для общества.

Второе направление отражает подходы, которые акцентируют внимание на обеспечивающих ее субъектах информационной безопасности, а именно государства, экономических агентов, личности.

В данном случае упор делается только на том, кто внедряет ее, регулирует и использует. Также данные понятия не учитывают общие черты безопасности для разных субъектов, позволяющих использовать общие подходы и инструменты в процессе организации защиты информации. Все это ограничивает понимание данного понятия на уровне отдельного субъекта или отдельной сферы.

Как мы видим, распространение получили структурный подход к пониманию понятия «информационная безопасность», по которому оно рассматривается в контексте национальной безопасности как ее составляющая; деятельностный подход, позволяющий рассматривать информационную безопасность как процесс, функцию государства, деятельность органов государственной власти; подход, согласно которому информационная безопасность рассматривается в статическом состоянии как определенное состояние защищенности или состояние правовых норм; подход, позволяющий рассматривать информационную безопасность как общественные отношения.

На наш взгляд, в теоретико-правовых исследованиях информационной безопасности целесообразно рассматривать ее сквозь призму правоотношений, возникающих при обеспечении состояния защищенности информационного пространства. Следовательно, информационную безопасность по нашему мнению, можно определить, как правоотношения,

возникающие при осуществлении превентивных и защитных мер в информационной среде человека, общества и государства. Таким образом информационная безопасность – это комплексная система, цель функционирования которой – защита объектов (информация, знания, информационные системы), принадлежащих финансово-хозяйственной, политической, военной, технологической сфер деятельности, от разного рода угроз (несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения) с применением программных, технических, методических, информационных и правовых средств, использующих отдельные лица или специализированные подразделения и специалисты государственных органов.

Главной функцией информационной безопасности является защита информации от случайного или преднамеренного воздействия, исключающая ее уничтожение, раскрытие или искажение.

В Российской Федерации известными центрами информационной безопасности являются такие учреждения, как Федеральная служба технического и экспортного контроля (ФСТЭК), Институт криптографии, связи и информатики Академии федеральной службы безопасности (ИКСИ) и Академия криптографии Российской Федерации (АК РФ) [Вострецова, 2019. С.15].

В теории информационной безопасности под субъектами информационной безопасности понимают владельцев и пользователей информации, причем пользователей не только на постоянной основе (сотрудники), но и пользователей, которые обращаются к базам данных в единичных случаях, например, государственные органы, запрашивающие информацию. В ряде случаев, например, в банковских информационной безопасности-стандартах к владельцам информации причисляют акционеров – юридических лиц, которым принадлежат определенные данные.

Объектами информационной безопасности следует считать: сознание, психику людей; информационно-технические системы различного масштаба и назначения. Если же говорить о социальных объектах информационной безопасности, то к ним можно отнести личность, коллектив, общество, государство, мировое сообщество.

Предметной областью информационной безопасности являются:

· информация и ее свойства;

· угрозы безопасности информации и ее собственникам;

· политика безопасности и модели безопасности;

· способы, методы и средства защиты информации;

· классификация систем защиты;

· требования к защищенности информационных систем;

· методология оценки защищенности информационных систем и проектирования защиты.

· конкретные системы защиты информации, применяемые в различных органах управления, учреждениях и на предприятиях различных форм собственности [Марков, 2019. С.77].

Информационная безопасность является сложным, системным, многоуровневым явлением, на состоянии перспективы развития которого оказывают непосредственное влияние внешние и внутренние факторы, важнейшими из которых являются:

1) политическая обстановка в мире;

2) наличие потенциальных внешних и внутренних угроз;

3) состояние и уровень информационно-коммуникационного развития страны;

4) внутриполитическая обстановка в государстве. В то же время, информационная безопасность представляет собой сложную, динамичную, целостную социальную систему, компонентами которой являются подсистемы безопасности личности, государства и общества [Зиновьева, 2017.

С.94]. Именно взаимосвязанное, системное информационное единство последних составляет качественную определенность, призванную осуществить защиту жизненно важных интересов человека, общества и государства, обеспечить их конкурентоспособное, прогрессивное развитие.

Таким образом, проблематика информационной безопасности стала весьма актуальна в наше время, что связано с ростом рисков потерь информации для экономических агентов, государства, личностей, а также увеличением киберпреступлений и атак хакеров в различных системах. Проведенный анализ научных подходов позволил определить два направления формулирования определения информационной безопасности – с позиции свойств функционирования и с позиции субъекта. В рамках определенных направлений были выделены различные подходы, главным недостатком которых является акцентирование внимания только на отдельной характеристике информационной безопасности, что говорит об узком ее понимании и ограниченности использования для других субъектов и видов деятельности. Во избежание определенных недостатков было предложено собственное определение информационной безопасности.

Список литературы:

1. Фадеева К.Н. Информационная безопасность: учебное пособие. – Чебоксары: Чувашский государственный педагогический университет им. И.Я. Яковлева, 2019. – 164 с.
2. Бабаш А.В., Баранова Е.К. Актуальные вопросы защиты информации: монография. – М.: РИОР: ИНФРА-М, 2017. – 111 с.
3. Зиновьева Е.С. Международное сотрудничество по обеспечению информационной безопасности: проблемы, субъекты, перспективы: дисс. ... канд. юрид. наук. М., 2017. 332 с.
4. Бордюже В.В. Информационная безопасность: монография. – Пермь: Урал. компьютер. форум: ГУП НИИУМС, 2015. – 82 с.

5. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. – Екатеринбург: Изд-во Урал. ун-та, 2019. – 204 с.

6. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) [электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/71456224/ (дата обращения 03.03.2022).

7. Марков А.А. Информационное общество. Информационная безопасность. Информационные войны: монография. – Санкт-Петербург: Изд-во Санкт-Петербургского гос. экономического ун-та, 2019. – 123 с.

8. Международная информационная безопасность: монография / Е.С. Зиновьева. – М.: МГИМО-Университет, 2013. – 194 с.

9. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 2 июля 2021 г. № 400) [электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/401325792/ (дата обращения 03.03.2022).