СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ ОПРЕДЕЛЕНИЯ ТЕРМИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Калинина Е.А.

Калинина Екатерина Алексеевна – магистрант,
Высшая школа бизнес-инжиниринга,
Санкт-Петербургский политехнический университет Петра Великого,
г. Санкт-Петербург

Аннотация: *в статье анализируются принципы к определению термина информационной безопасности. В рамках проведенного исследования автором были разработаны и предложены различные варианты интерпретации данного термина согласно различным подходам.*
Ключевые слова: *информационная безопасность, анализ, сравнение.*

Информация является «новой нефтью» XXI века. С этим сложно поспорить, ведь каждый день информацией оперируют во всех сферах нашей жизни, в каждой области. Так как информация является основой для принятия решений, коммуницирования и взаимодействия всех экономических субъектов – ценность данного актива становится очевидным фактом [1; 2]. Однако с тем, насколько информация становится все более значимой, необходимость ее защищать становится первостепенным фактором.

Безопасность информации заключается в предотвращении любого несанкционированного доступа к ней, непредвиденного и/или целенаправленного изменения данных, что заключается в сохранении конфиденциальности, целостности и доступности информации. Эти подходы формируют концепцию информационной безопасности [1], которая направлена на защиту данных.

Рассмотрим подробнее определения термина информационная безопасность, так как трактовка термина варьируется в зависимости от разных целей. Данные определения можно разбить на три основные подгруппы, а именно: источником является федеральный государственный документ, книга или учебное пособие, которые представляют собой более широкие и полные определения, англоязычные форумы и статьи, которые фокусируются на условиях и элементах информационных систем.

Российский государственный стандарт: ГОСТ 13335-1:2006 предлагает следующее определение: «Информационная безопасность – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки» и подчеркивает предъявляемые требования к информации и способам ее обработки [1]. Доктрина информационной безопасности РФ определяет информационную безопасность, как: «Состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [2], что подчеркивает совокупность сбалансированных интересов личности, общества и государства. ФЗ от 30.06.2003 N 86 определяет сущность информационной безопасности наиболее емко и коротко, как состояние среды, используемое всеми ее субъектами [3].

Предложенные определения В. Шаньгинем и В. Галатенко рассматривают информационную безопасность, как конкретный случай использования информации с различными целями [4, 5]. Они утверждают, что могут происходить случаи, когда информационная защищенность может быть нарушена благодаря какому-либо воздействию извне. Это может быть, как полная, безвозвратная потеря, так и незаконное распространение. Таким образом, оба случая подчеркивают важность обеспечения безопасности информационных систем и данных, которые в последствие обеспечат защиту интересов владельцев и пользователей информации. Однако стоит отметить, что в первом определении акцент смещен на незаконность при распространении и использовании информации, которая в последствии может быть полностью уничтожена. В то время как второе говорит про защищенность информационных ресурсов от воздействий любого характера, как искусственного, так и естественного.

Г. Магдэниэл в своей работе определяет информационную безопасность как некий комплекс мер направленных на защиту информационных активов от любого несанкционированного доступа, уничтожения, манипулирования и потери. Акцент делается на предотвращении различных видов угроз [6]. В. Галатенко перечисляет элементы информационных систем, которые могут быть подвержены угрозам безопасности. Упоминается, что при рассмотрении информационной безопасности иногда упускают из виду пользователей и процессы [7].

Адамс указывает, что: «Информационная безопасность определяется как способность авторизованных пользователей получать доступ к учебным ресурсам без риска быть скомпрометированными при онлайн-обучении» [8]. Определение связывает информационную безопасность с доступом авторизованных

пользователей к учебным ресурсам без риска компрометации при онлайн-обучении. Это более узкое понимание информационной безопасности, которое фокусируется на защите данных в контексте образовательного процесса.

Е. Вейппл определяет только три равнозначных, невзаимозаменяемых, самостоятельных термина для обеспечения безопасности это: Конфиденциальность, целостность и доступность [9].

Было проведено сравнение терминов из различных источников. Также определения термина информационная безопасность можно сравнить по определяющим их подходам. Сравнительный анализ подходов представлен в таблице 1.

Таблица 1. Сравнительный анализ подходов к определению термина «информационная безопасность» (составлено автором).

Аспект	Юридический	Технический	Этический
Цель	Соблюдение законодательства	Защита данных	Защита прав и свобод человека
Методика, подход	Законы, нормативные акты, регламенты	Технологии антивируса, шифрования	Моральные нормы
Фокус	Право	Технологии	Этика
Пример применения на практике	Соблюдение №152-ФЗ	Использование шифрования данных	Приватность клиента

Рассмотрим эти подходы подробнее.

1. Юридический подход. В правовой области информационная безопасность непосредственно связана с защитой прав на информацию. Таким образом, в федеральном законе 15 «О персональных данных» от 27 июля 2006 года №152-ФЗ. Определяются требования по работе с персональными данными (ПДн) российских граждан, обеспечивает защиту их интересов и надлежащий уровень защиты.
2. Технический подход. Подразумевает совокупность средств, принципов и методов, направленных на сохранение неизменности, конфиденциальности и сохранении данных. ГОСТ Р 50922-96 трактует информационную безопасность как состояние защищенности информации от угроз. В данном подходе больший фокус направлен на техническую сторону, а именно: использование или разработка антивирусов, технологии шифрования и т.п. Например, компаниям, разрабатывающим технологии по защите данных для получения официального статуса сертифицированной разработки [10] (например, ФСТЭК, ФСБ, МинПромТорг) необходимо выполнить все требования регулятора.
3. Этический подход. В данном случае главной определяющей является моральная ответственность перед заказчиком. Предполагается, что, следуя этическому подходу, должны выполняться и соблюдаться права потребителя, например право на личную и частную жизнь или безопасность и открытость процессов, связанных с обработкой данных.

Таким образом, термин информационная безопасность может быть рассмотрен с разных сторон и одновременно отвечать нескольким подходам. В современном мире необходимо найти баланс между всеми подходами, чтобы сформировать целостную концепцию к определению термина. Для эффективного обеспечения информационной безопасности важно учитывать все эти аспекты, адаптируя их к специфике отрасли.

Список литературы

1. *Федоренко И.В.* Информационная безопасность системы дистанционной коммуникации с медицинской информационной системой для отделения лучевой диагностики / И. В. Федоренко, О. С. Чемерис // Интернаука. – 2023. – № 3-1(273). – С. 11-14. – DOI 10.32743/26870142.2023.3.273.351517. – EDN QCZAEV.
2. *Погарская О.С.* Сущность знаниевого подхода к процессу эффективного функционирования экономических систем / О.С. Погарская // Социально-экономические проблемы развития территориальных систем и механизмы повышения их конкурентоспособности: Труды XII Международной конференции молодых ученых, Екатеринбург, 05–06 сентября 2014 года. – Екатеринбург: Институт экономики Уральского отделения РАН, 2014. – С. 184-189. – EDN ULCXXP.
3. Российский государственный стандарт: ГОСТ 13335-1:2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
4. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. N 646)

5. Федеральный закон «Об участии в международном информационном обмене» (в ред. Федеральных законов от 30.06.2003 N 86-ФЗ, от 29.06.2004 N 58-ФЗ)
6. *Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях. // М.: ДМК Пресс, 2012. С. 592.
7. *Галатенко В.А.* Основы информационной безопасности. // М., 2004. С. 264.
8. *McDaniel G., & McDaniel, G.* IBM dictionary of computing, 1994.
9. *Dlamini M.T., Eloff J.H., Eloff M.M.* Information security: The moving target // Computers & security, 2009. № 28 (3-4). С. 189–198.
10. *Чемерис О.С.* Опыт внедрения цифровых технологий в железнодорожной логистике / О.С. Чемерис // Экономико-управленческий конгресс: Сборник статей по материалам Международного научно-практического мероприятия НИУ "БелГУ", Белгород, 10–11 ноября 2022 года / Отв. редактор: В.М. Захаров. – Белгород: Белгородский государственный национальный исследовательский университет, 2022. – С. 454-459. – EDN YEHQPC.