Тип работы: Курсовая работа

Предмет: Информационные технологии в юриспруденции

Глава 1. Понятие информационной безопасности и органы, осуществляющие её

1.1 Понятие информационной безопасности

Эволюцию средств передачи информации можно разделить на отдельные этапы, каждый из которых знаменует собой значительный прогресс в области информационной безопасности.

Рис.1. Этапы эволюции средств передачи информации

Давайте рассмотрим эти этапы:

I этап (до 1816 г.) характеризуется использованием естественных средств для информационных коммуникаций. В этот период основное внимание в области информационной безопасности уделялось защите важных данных, включая события, факты, собственность, а также информацию, относящуюся к отдельным лицам или сообществам.

II этап (с 1816 г.) ознаменовался внедрением искусственно созданных технических средств, таких как электрическая и радиосвязь. Обеспечение скрытности и помехозащищенности в радиосвязи требовало использования знаний, полученных на предыдущем этапе. Это включало внедрение устойчивых методов кодирования сообщений (сигналов) и последующее декодирование полученных передач.

III этап (с 1935 г.) соответствовал появлению радиолокационных и гидроакустических технологий. Информационная безопасность на этом этапе основывалась на комплексе организационных и технических мероприятий, направленных на повышение защищенности объектов радиолокации. Цель состояла в том, чтобы противодействовать активной маскировке и пассивной имитации электронных помех, направленных на их приемные устройства.

IV этап (с 1946 г.) возник с изобретением и практическим использованием электронно-вычислительных машин, широко известных как ЭВМ. Проблемы информационной безопасности в основном связаны с ограничением физического доступа к оборудованию, используемому для сбора, обработки и передачи информации.

V этап (с 1965 г.) характеризовался созданием и развитием локальных информационно-коммуникационных сетей. Для решения задач информационной безопасности акцент был сделан на методы физической защиты ресурсов, задействованных в сборе, обработке и передаче информации в локальной сети.

Администрирование сетевых ресурсов и управление доступом сыграли решающую роль.
VI этап (с 1973 г.) ознаменовался появлением ультрамобильных средств связи с разнообразными функциональными возможностями. В этот период обострились угрозы информационной безопасности. Защита компьютерных систем с помощью беспроводных сетей передачи данных потребовала разработки новых критериев безопасности. Возникли сообщества хакеров, создающие риски для отдельных пользователей, организаций и целых стран. Важность защиты информационного ресурса стала первостепенной, сделав ее неотъемлемым и обязательным аспектом национальной безопасности. Следовательно, область информационного права начала формироваться как новая отрасль в рамках международной правовой системы.
VII этап (с 1985 г.) предусматривал создание и развитие глобальных информационных и коммуникационных сетей с использованием космических технологий. Забегая вперед, следующий этап развития информационной безопасности, вероятно, будет включать широкое использование ультрамобильных устройств связи с широкими возможностями, наряду с глобальным охватом, обеспечиваемым космическими информационно-коммуникационными системами. Решение задач информационной безопасности на данном этапе потребует создания комплексной макросистемы глобальной информационной безопасности под эгидой ведущих международных форумов.
Информационная безопасность охватывает различные уровни, в том числе индивидуальный, организационный и государственный .
Индивидуальная информационная безопасность: это относится к защите права человека на информацию, обеспечению ее безопасности и сохранению конфиденциальности.
Организационная информационная безопасность: включает в себя обеспечение безопасности информационной среды организации для обеспечения ее формирования, использования и развития. Как правило, организации создают специальные отделы или службы для защиты своей информации.
Государственная информационная безопасность: это самая широкая область, охватывающая сохранение информационных ресурсов государства и защиту законных прав человека и общества в информационной сфере.
При изучении структурных концепций, связанных с информационной безопасностью, уместны следующие определения:
Конфиденциальность: обеспечение того, чтобы только авторизованные пользователи имели доступ к информации.
Целостность: гарантия достоверности и полноты информации и методов, используемых для ее обработки.
Доступность: Предоставление авторизованным пользователям доступа к информации и связанным активам по мере необходимости.
Информационная безопасность охватывает все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и надежности информации или методов ее обработки.
Под информационной безопасностью (данными) понимается состояние, при котором обеспечивается конфиденциальность, доступность и целостность информации (данных). Безопасность информации (данных) зависит от минимизации неприемлемых рисков, связанных с утечкой информации по техническим каналам, несанкционированным доступом и непреднамеренным воздействием на данные или другие ресурсы автоматизированной информационной системы, используемые в приложениях информационных технологий .
Информационная безопасность (в контексте информационных технологий), также известная как ИТ-безопасность, направлена на обеспечение безопасности самих информационных технологий. Она защищает информацию, обрабатываемую технологией, и информационную безопасность автоматизированной информационной системы, в которой она работает.
Безопасность автоматизированной информационной системы включает в себя конфиденциальность, доступность, целостность, подотчетность и подлинность ее ресурсов.
В более широком смысле информационная безопасность предполагает защиту информации и поддерживающей инфраструктуры от естественных или искусственных событий, которые могут нанести значительный ущерб сторонам, участвующим в деятельности, связанной с информацией. Поддерживающая инфраструктура включает в себя системы электроснабжения, отопления, водоснабжения, газоснабжения, кондиционирования воздуха, а также обслуживающий персонал. Неприемлемый ущерб относится к ущербу, который нельзя игнорировать.

Рис.2. Стандартная модель безопасности

Стандартная модель безопасности включает три основные категории, на которые часто ссылаются:
Конфиденциальность: это относится к состоянию информации, при котором доступ ограничен только уполномоченными физическими или юридическими лицами.
Целостность: это включает в себя предотвращение несанкционированных модификаций или изменений информации, обеспечение ее точности и надежности.
Доступность. Эта категория ориентирована на предотвращение временного или постоянного отказа в доступе к информации для пользователей, обладающих необходимыми правами доступа.
В дополнение к этим основным категориям в модели безопасности есть и другие необязательные компоненты:
Подотчетность: она включает в себя идентификацию и регистрацию действий лиц, получающих доступ к информации, что обеспечивает отслеживание и установление авторства.
Надежность: этот аспект относится к последовательному соответствию информации или ресурсов их предполагаемому поведению или ожидаемым результатам.
Аутентичность: гарантирует, что предметы или ресурсы являются подлинными и соответствуют их заявленной идентичности.

Нормативные правовые акты
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) // Собрание законодательства РФ. № 31. Ст. 4398.
2. Федеральный закон от 03.04.1995 № 40-ФЗ «О Федеральной службе безопасности» // Собрание законодательства РФ. 1995. № 15. Ст. 1269
3. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 21. Ст. 436.
4. Федеральный закон от 04.05.2011 N 99-ФЗ «О лицензировании отдельных видов деятельности» // Собрание законодательства РФ. 2011. № 13. Ст. 1126.
5. Указ Президента РФ от 11.08.2003 № 960 «Вопросы Федеральной службы безопасности Российской Федерации» // Собрание законодательства РФ. 2003. № 33. Ст. 3254

Специальная литература
6. Булыгина И.А. Правовое регулирование реализации права на обращение граждан в органах федеральной службы безопасности Российской Федерации // Военное право. 2018. № 2 (48). С. 11-16.
7. Вербин А.С., Применко Д.В. История развития законодательства и совершенствование правового регулирования деятельности органов ФСБ России // Энигма. 2019. Т. 1. № 9-1. С. 332-341.
8. Газизов, А. Р. Организационное и правовое обеспечение информационной безопасности / А. Р. Газизов. – Ростов-на-Дону : Донской государственный технический университет, 2017. – 156 с.
9. Кошелева, О. В. Правовые основы деятельности органов ФСБ России в сфере лицензирования оборота специальных технических средств, предназначенных для негласного получения информации / О. В. Кошелева // Полицейское право. – 2006. – № 4(8). – С. 51-55.
10. Таибова О.Ю. Управление в сфере государственной безопасности в Российской Федерации // Северо-Кавказский юридический вестник. 2019. № 2. С. 90-96.
11. Черепанова, Ю. Е. К вопросу о новеллах нормотворчества в лицензионной сфере / Ю. Е. Черепанова // Актуальные проблемы административного и административно-процессуального права (Сорокинские чтения) : Международная научно-практическая конференция, Санкт-Петербург, 26 марта 2021 года / Под общей редакцией А.И. Каплунова. – Санкт-Петербург: Санкт-Петербургский университет Министерства внутренних дел Российской Федерации, 2021. – С. 218-222.
12. Шарыпова Т.Н., Настенко А.В. ФСБ в системе национальной безопасности // Colloquium-journal. 2020. № 3-4 (55). С. 9-10.