1. Основные понятия информационной безопасности

Понятие «информационная безопасность» исторически возникло очень давно, практически с того момента, когда человек стал выделяться из животного мира. Уже тогда необходимо было хранить в тайне от других (то есть предотвратить утечку) такую, например, информацию как: где расположены запасы продуктов (утечка по видовым и речевым каналам), сохранить тайну изготовления орудий труда (предотвратить похищение, или утечку по материально-вещественному каналу).

1.1 Периоды развития средств и методов защиты информации

Анализ процесса развития средств и методов защиты информации позволяет разделить его на три относительно самостоятельных периода. В основе такого деления лежит эволюция видов носителей информации.

Первый период (с древнейших времён до 20-х годов XIX века) определяется началом создания осмысленных и самостоятельных средств и методов защиты информации и связан с появлением возможности фиксации информационных сообщений на твердых носителях, то есть с изобретением письменности.

Этот период характеризуется использованием естественно возникавших средств информационных коммуникаций. В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение.

Вместе с неоспоримым преимуществом сохранения и перемещения данных возникла проблема сохранения в тайне,

существующей уже отдельно от источника конфиденциальной информации, поэтому практически одновременно с рождением письменности возникли такие методы защиты информации, как шифрование и скрытие.

Второй период (с двадцатых годов XIX века до тридцатых годов XX века) характеризуется появлением технических средств обработки информации и передачи сообщений с помощью электрических сигналов и электромагнитных полей (например, телефон, телеграф, радио). В связи с этим возникли проблемы защиты от так называемых радиоэлектронных технических каналов утечки (побочных излучений, наводок и др.).

Для обеспечения скрытности и помехозащищенности радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне, а именно применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).

Также в этот период активно развиваются технические средства разведки, многократно увеличивающие возможности промышленного и государственного шпионажа.

Огромные, все возрастающие убытки предприятий и фирм способствовали научно-техническому прогрессу в создании новых и совершенствовании старых средств и методов защиты информации.

Третий период (с тридцатых годов XX века по настоящее время) связан с внедрением автоматизированных систем обработки информации. При этом, продолжают активно развиваться способы и методы защиты от утечки по техническим каналам.

Учитывая влияние на трансформацию идей информационной безопасности, в развитии средств информационных коммуникаций можно выделить несколько этапов:

I этап – начиная с 1935 года по 1945 год – связан с появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства помех.

II этап – начиная с 1946 года по 1965 год – связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи информационной безопасности решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.

III этап – начиная с 1965 года по 1973 год – обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединённых в локальную сеть путём администрирования и управления доступом к сетевым ресурсам.

IV этап – начиная с 1973 года по 1985 год – связан с использованием мобильных средств связи с широким спектром задач. Угрозы информационной безопасности стали гораздо серьёзнее. Образовались сообщества людей – хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей и организаций. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности – важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право – новая отрасль международной правовой системы.

V этап – начиная с 1985 года по настоящее время – связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

В 60-х гг. на Западе стало появляться большое количество открытых публикаций по различным аспектам защиты информации. Такое внимание к этой проблеме в первую очередь было вызвано возрастающими финансовыми потерями фирм и государственных организаций от преступлений в компьютерной сфере.

В России давно и небезуспешно стали также заниматься проблемами защиты информации. И не зря советская криптографическая школа до сих пор считается лучшей в мире.

В данное время есть все основания утверждать, что в России сложилась отечественная школа защиты информации. Ее отличительной особенностью является то, что в ней наряду с решением сугубо прикладных проблем защиты большое внимание уделяется формированию развитого научно-методологического базиса, создающего объективные предпосылки для решения всей совокупности соответствующих задач на регулярной основе [1].

1.2 Актуальность проблем информационной безопасности

В настоящее время, в эпоху развитого информационного общества, практически любая информация имеет цену.

Разведывательная деятельность иностранных государств в настоящее время отличается большим разнообразием используемых сил и средств. Многофункциональные

разведывательные космические системы, наземные центры радиотехнической и радиолокационной разведки, стратегические самолеты-разведчики, морские системы и комплексы технической разведки действуют в настоящее время против России непрерывно. При этом расходы на разведывательную деятельность иностранных государств не сокращаются (например, в США они составляют ежегодно свыше 30 млрд. долларов). В сферу интересов технических разведок попадают даже союзники.

Рассматривая социальный аспект информационной безопасности, следует вспомнить, как публичная информация, обработанная спецслужбами, воздействует на граждан отдельных государств. Нередко это приводило к «цветным революциям» и смене власти в стране.

С точки зрения экономического аспекта необходимо констатировать, что в информационном пространстве крутится огромное количество недостоверной информации, которая циркулирует сегодня даже по официальным государственным информационным каналам. Достаточно вспомнить те же финансовые пирамиды, когда при помощи средств массовой информации, принадлежащих государству, тиражировалась заведомо ложная, недостоверная информация.

Преступные посягательства в финансово-кредитной и банковской сферах за последние годы стали разнообразнее и изощреннее. Ущерб от различных видов преступных посягательств, связанных с нарушением информационной безопасности в автоматизированных платежных системах, может быть не меньше чем при прямом хищении денег и ценностей. Актуальность этой проблемы возрастает по мере расширения внедрения новых автоматизированных платежных систем. При охвате автоматизированной платежной системой всех регионов страны любая дестабилизация в ее функционировании может нарушить безопасность финансово-платежной системы

страны и, как следствие, проявится в сбое всего хозяйственного механизма государства.

Военный аспект. По мнению отечественных и зарубежных специалистов, боевые действия в современных (и будущих) войнах прежде всего ведутся не для разгрома сухопутных войсковых группировок противника. Они имеют целью дезорганизацию политического, экономического и военного управления соответствующими структурами противоборствующей стороны. О том, что изменились цель и характер боевых действий, свидетельствует опыт локальных войн последнего времени (после Вьетнама). Сейчас наступает новый этап. Наметилась тенденция перехода от оружия массового уничтожения к высокоточному «информационному оружию».

В США и некоторых других странах созданы центры по реализации концепции «Информационная война». Новый орган разрабатывает положения по организации и ведению борьбы в новой сфере военного противоборства, решает задачи по подготовке специалистов в данной области, а также определяет приоритеты в НИОКР и закупках, предназначенных для этих целей вооружений и аппаратуры.

Опыт военных действий последних лет (на Ближнем Востоке, в Югославии, Ираке) показал, что резко возросшие технические возможности средств разведки сделали неэффективными многие традиционные методы и средства защиты информации. Например, данные космических средств разведки оперативно использовались непосредственно на поле боя, для управления высокоточным оружием, даже для борьбы с иракскими оперативно-тактическими ракетами СКАД. Это значит, что такие традиционные методы скрытия информации о дислокации ракетных комплексов, как пространственное маневрирование в позиционном районе, уже неэффективны.

Обосновывая актуальность информационной безопасности, а именно причины, побуждающие заниматься защитой информации, представлены на рис. 1.1.

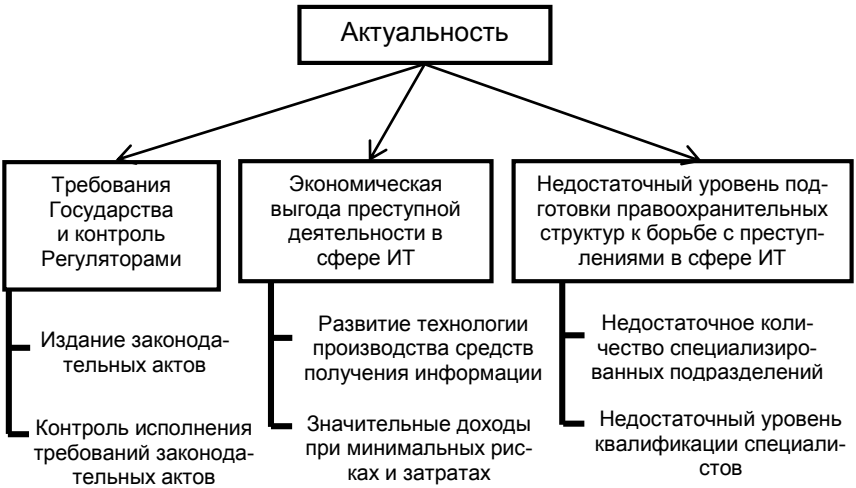

Рис. 1.1. Актуальность информационной безопасности

Чтобы оценить изобретательность злоумышленников и разнообразие форм проявления компьютерных преступлений, ниже представлено несколько вскрытых случаев по информации из общедоступных источников.

Похищение личных данных

В мае 2014 года в СМИ прошла информация о том, что ФБР арестовано 97 человек, подозреваемых в распространении и использовании вредоносного программного продукта «Блэк Шиитс», позволяющего похищать личные данные с компьютеров. Возможна даже активация видеокамеры, чтобы шпионить за хозяином.

Аппаратные закладки на бытовом уровне

Изобретению китайских специалистов могут позавидовать и хакеры, и даже американская разведка. Инженеры из

Поднебесной встраивают в бытовую технику специальные чипы, которые автоматически подсоединяются к сетям и рассылают вирусы и спам. Партию таких «шпионов» – утюгов, чайников и телефонов – случайно обнаружили в Санкт-Петербурге.

Как спецслужбы США подглядывают за иностранными гражданами

23-25 января в Брюсселе прошла конференция «Компьютеры, приватность и защита данных», на которой Каспар Боуден (Caspar Bowden), бывший советник по вопросам приватности в Microsoft Europe, поведал о том, что в США действует закон Foreign Intelligence Surveillance Act Amendments Act 2008 (FISA), который предусматривает беспрепятственный доступ американских разведывательных агентств к информации иностранных граждан на облачных хостингах, если активность этих пользователей имеет отношение к внешней политике США.

По документам Сноудена спецслужбы США «хакнули» протокол SSL

Агентство национальной безопасности (АНБ) США и его британский аналог нашли способы обходить криптографическую защиту в интернете. Спецслужбы разработали специальные методы, которые позволяют им взламывать практически все используемые в настоящее время в интернете стандарты шифрования. Эту информацию опубликовала газета New York Times со ссылкой на документы, предоставленные Эдвардом Сноуденом.

Пойман школьник движения Anonymous

Школьник из Монреаля признался в причастности к взлому правительственных сайтов по заданию активистов движения Anonymous. Ущерб от действий 12-летнего подростка составил около 60 тысяч канадских долларов.

По словам малолетнего преступника, он с ранних лет интересовался компьютерами, а задания Anonymous выполнял не из политических соображений, а в обмен на видеоигры.

1.3 Основные термины и определения в области информационной безопасности

Прежде чем говорить о защите информации, важно определить понятие информации, которое само по себе является первичным в данной области. Существует множество определений информации, которые варьируются в зависимости от контекста. В данном курсе под ***информацией*** мы будем подразумевать любые сведения (данные) независимо от формы их представления.

Информация существует в различных формах. Ее можно хранить на компьютерах, передавать по вычислительным сетям, распечатывать или записывать на бумаге, а также озвучивать в разговорах. С точки зрения безопасности все виды информации, включая бумажную документацию, базы данных, пленки, микрофильмы, модели, магнитные ленты, дискеты, разговоры и другие способы, используемые для передачи знаний и идей, требуют надлежащей защиты.

Согласно [2, 3] информацию классифицируют, как показано на рисунке 2.

В общем случае информация – это знания в самом широком понимании этого слова. То есть это не только образовательные или научные знания, а любые сведения и данные, которые присутствуют повсеместно. Защите подлежит не только конфиденциальная информация и сведения, отнесённые к государственной тайне.

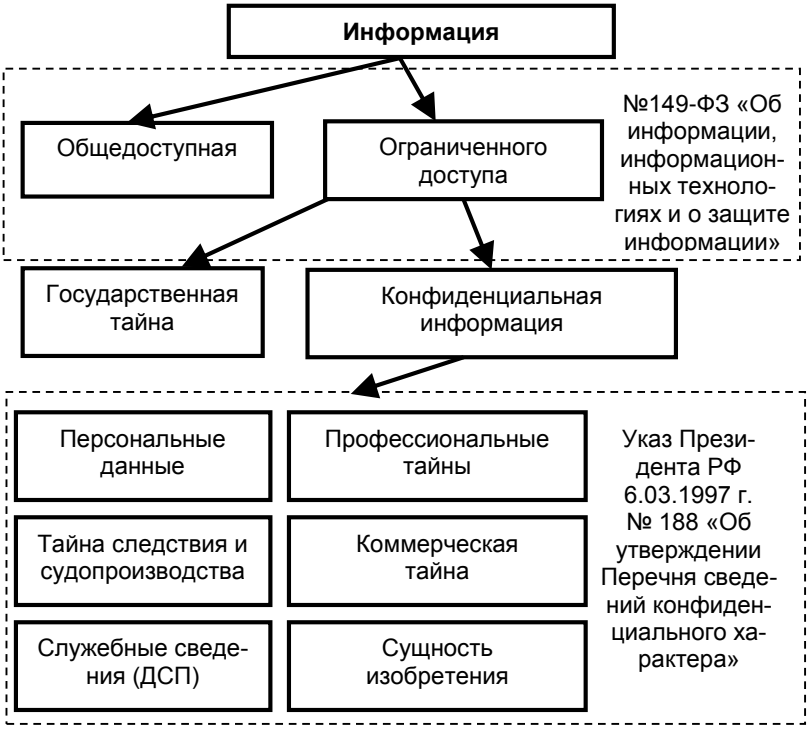

Рис. 2. Классификация информации

Под ***конфиденциальной информацией*** подразумевается информация ограниченного доступа, не содержащая государственную тайну.

Очень часто необходимо защищать и общедоступную информацию, не требующую обеспечения конфиденциальности. Но если не обеспечить целостность и доступность любой информации, если разместить фейковые новости на официальных государственных сайтах или не обеспечить своевременный доступ к данным сайтам, то можно ожидать социальных взрывов в обществе.

Конфиденциальность, целостность и доступность представляют собой три наиболее важных свойства информации в рамках обеспечения ее безопасности. Нередко данные свойства называют основными аспектами информационной безопасности и в них вкладывается следующий смысл:

конфиденциальность информации – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

доступность информации – состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Процессы, сопровождающие существование и развитие современного общества, принято объединять под общим названием «информатизация». Информатизация предполагает широкое использование информационных систем, которые обеспечивают доступ к источникам информации (в нетехнических приложениях эти источники часто называют информационными ресурсами), накопление и хранение информации (образование новых информационных ресурсов).

Существует много вариантов определений понятию «информационная система». Например, в широком смысле информационная система есть совокупность технического, программного и организационного обеспечения, а также персонала, предназначенная для того,

чтобы своевременно обеспечивать надлежащих людей надлежащей информацией.

Другой вариант, не менее популярный: под информационной системой понимается комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации

Федеральный закон РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» трактует понятие следующим образом: «***информационная система*** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств».

Понятие ИС очень широкое и оно охватывает следующие системы:

– ЭВМ всех классов и назначений;

– вычислительные комплексы и системы;

– вычислительные сети (локальные, региональные и глобальные).

Таким образом, ***объектом защиты информации*** является информационная система (предприятия, коммерческой организации) или автоматизированная система обработки данных.

В состав объектов защиты информации могут быть отнесены: охраняемая территория, здание (сооружение), выделенное помещение, информация и (или) информационные ресурсы объекта информатизации.

Предметом же защиты – информация.

В процессе защиты информации необходимо обеспечить состояние информационной безопасности (ИБ). Согласно [4], ***информационная безопасность Российской Федерации – 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.*

В более узком смысле будем считать: ***информационная безопасность – это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера****, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.*

Защитой информации называется деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию [5].

Все ***меры защиты информации*** по способам осуществления подразделяются на:

1. Правовые (законодательные);
2. Морально-этические;
3. Организационные;
4. Инженерно-технические:
   – физические;

– технические (программно-аппаратные);
– криптографические.

Два последних могут быть реализованы как в программном, так и в программно-аппаратном исполнении.

Среди перечисленных видов защиты базовыми являются правовая, организационная и инженерно-техническая защита информации.

Правовая защита информации или защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением [5].

К ***морально-этическим мерам*** относятся устоявшиеся в обществе нормы поведения. В отдельных случаях они могут быть оформлены в письменном виде, например, уставом или кодексом чести организации. Соблюдение морально-этических норм не является обязательным и носит скорее профилактический характер.

Организационные (административные) меры защиты – меры организационного характера, предназначенные для регламентации функционирования информационных систем, работы персонала, взаимодействия пользователей с системой. Среди базовых организационных мер по защите информации можно выделить следующее:

– формирование политики безопасности;
– регламентация доступа в помещения;
– регламентация допуска сотрудников к использованию ресурсов информационной системы.

– определение ответственности в случае несоблюдения требований информационной безопасности и др.

Инженерно-техническая защита (ИТЗ) – это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации. Она решает следующие задачи:

– предотвращение проникновения злоумышленника к источникам информации с целью ее уничтожения, хищения или уничтожения;

– защита носителей информации от уничтожения в результате воздействия стихийных сил;

– предотвращение утечки информации по различным техническим каналам.

Физическая защита информации – защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты [5].

Техническая защита информации **(*ТЗИ*)** – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств [5].

Технические (аппаратно-программные) меры защиты основаны на использовании различных электрон-

ных устройств и специальных программ, которые самостоятельно или в комплексе с другими средствами, реализуют следующие способы защиты:

- идентификацию (распознавание) и аутентификацию (проверку подлинности) субъектов (пользователей, процессов);
- разграничение доступа к ресурсам;
- регистрацию и анализ событий;
- криптографическое закрытие информации;
- резервирование ресурсов и компонентов систем обработки информации и др.

Криптографическая защита информации – защита информации с помощью ее криптографического преобразования [5].

Дадим определение еще некоторым понятиям в области ИБ.

Защита информации от утечки – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами [5].

Защита информации от разглашения – защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации [5].

Защита информации от несанкционированного доступа (ЗИ от НСД) – защита информации,

направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации [5].

***Защита информации от несанкционированного воздействия* (*ЗИ от НСВ*) –** защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации [5].

Система защиты информации – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации [5].

Политика безопасности (информации в организации) – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности [5].

Безопасность информации (данных) – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность [5].

Вопросы для самопроверки по Лекции 1 тема 1

1. Периоды развития средств и методов защиты информации.
2. Этапы развития средств и методов защиты информации в рамках 3 периода.
3. В чем состоит актуальность информационной безопасности?
4. Причины, побуждающие заниматься защитой информации.
5. Что такое информация?
6. Определение конфиденциальной информации.
7. Дать классификацию информации.
8. Перечислить основные аспекты ИБ.
9. Дать определение конфиденциальности информации.
10. Дать определение целостности информации.
11. Дать определение доступности информации.
12. Что такое информационная система?
13. Что является объектом защиты информации?
14. Дать определение ИБ РФ.
15. Дать определение ИБ в узком смысле.
16. Что такое защита информации?
17. Как классифицируют меры защиты информации?
18. Дать понятие правовой защите информации.
19. Дать понятие организационным мерам ЗИ.
20. Дать определение физической ЗИ.
21. Дать определение ТЗИ.

22. Дать определение криптографической ЗИ.
23. Дать понятие ЗИ от утечки.
24. Дать понятие ЗИ от разглашения.
25. Дать определение ЗИ от НСД.
26. Дать определение ЗИ от НСВ.
27. Что такое система защиты информации?
28. Дать определение политике безопасности информации.

Литература

1. https://studfile.net/preview/6211048/page:9/
2. №149-ФЗ «Об информации, информационных технологиях и о защите информации»
3. Указ Президента РФ 6.03.1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера»
4. Доктрина информационной безопасности
5. Национальный стандарт Российской Федерации ГОСТ Р 50922 – 2006 Защита информации. Основные термины и определения.
6. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации: учебное пособие. – СПб: НИУ ИТМО, 2011. – 112 с.