Федеральная служба исполнения наказаний
Вологодский институт права и экономики

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Учебное пособие
для направления подготовки 40.03.01 – Юриспруденция,
специальности 40.05.02 – Правоохранительная деятельность,
специальности 37.05.02 – Психология служебной
деятельности очной и заочной форм обучения

Вологда
2018

УДК 004.056(075)
ББК 32.97.1
И74

Рецензенты:
О. Б. Голубев – зав. каф. информ. технологий и методики преподавания информатики Вологод. гос. ун-та, канд. пед. наук, доц.;
О. А. Шахов – начальник инженер.-эконом. фак., канд. техн. наук, доц.

Авторский коллектив:
О. А. Панфилова – канд. техн. наук; Д. Ю. Крюкова – канд. техн. наук; А. Н. Наимов – д-р физ.-мат. наук, проф.; В. В. Мухин – д-р физ.-мат. наук, проф.

И74 **Информационная безопасность и защита информации** : учеб. пособие для направления подготовки 40.03.01 – Юриспруденция, специальности 40.05.02 – Правоохранительная деятельность, специальности 37.05.02 – Психология служебной деятельности, очной и заочной форм обучения / О. А. Панфилова и др. ; Федер. служба исполн. наказаний; Вологод. ин-т права и экономики. – Вологда : ВИПЭ ФСИН России, 2018. – 59 с. : табл.

ISBN 978-5-94991-428-1 Работа частично поддержана грантом РФФИ 18-47-350001 р_а

В учебном пособии рассматриваются основные понятия по информационной безопасности и защите информации, особенности компьютерных преступлений и методы их предотвращения.

УДК 004.056(075)
ББК 32.97.1

ISBN 978-5-94991-428-1

ВВЕДЕНИЕ

В повседневной и служебной деятельности каждый человек имеет дело с информацией, доступ к которой и обработка зачастую осуществляются в электронном виде и с применением информационных технологий. В связи с широким распространением и повсеместным использованием персональных компьютеров, гаджетов, средств телекоммуникации, сетей актуальными становятся проблемы обеспечения информационной безопасности, знание и владение методами защиты информации. Такое свойство, как компьютерная грамотность является обязательным и само собой разумеющимся для современного пользователя.

Изучение дисциплин «Информационная безопасность» и «Защита информации» является важным аспектом при подготовке специалистов и бакалавров в области юриспруденции, психологии и в других отраслях. В федеральных государственных образовательных стандартах по многим специальностям и направлениям подготовки заложено формирование следующих компетенций:

– способность работать с различными информационными ресурсами и технологиями, с компьютером как средством управления информацией, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации;

– способность работать с информацией в глобальных компьютерных сетях;

– способность соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;

– готовность к выполнению должностных обязанностей по обеспечению безопасности личности, общества, государства.

Учебный курс предполагает приобретение обучающимися профессиональных знаний, необходимых для грамотного при-

менения и эксплуатации компьютера, информационных ресурсов и технологий, компьютерных сетей.

Данное учебное пособие предназначено для работы по дисциплинам «Информационная безопасность» и «Защита информации» для курсантов, слушателей и студентов очной и заочной форм обучения по направлению подготовки 40.03.01 Юриспруденция, специальности 40.05.02 Правоохранительная деятельность, специальности 37.05.02 Психология служебной деятельности. Он рассчитан на групповую или индивидуальную работу на лекционных и практических занятиях, самостоятельную работу обучающихся, подготовку к зачету.

Учебное пособие включает теоретический материал, направленный на изучение основных понятий по информационной безопасности и защите информации, мероприятий по обеспечению информационной безопасности, вредоносных программ и методов защиты от них, компьютерных преступлений и методов их предотвращения. Отдельный интерес представляют современные криптографическими методы защиты информации, такие как электронная подпись.

Цель учебного пособия – формирование системы знаний по информационной безопасности и защите информации личности, организации, общества, государства и основных мерах по их обеспечению.

Материал имеет четкую структуру. Пособие разбито на четыре раздела: основные понятия информационной безопасности, мероприятия по обеспечению информационной безопасности, методы защиты от компьютерных вирусов, компьютерная преступность. Учебное пособие при обучении предполагается использовать совместно с практикумом и методическими материалами.

ТЕМА 1
ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Актуальность защиты информации

Сколько на Земле существует человечество, столько времени люди имеют дело с информацией и сталкиваются с необходимостью ее защиты. На протяжении многих веков человеческие судьбы и судьбы государств зависели и зависят от сохранности и надежности защиты важной информации. В истории можно привести много ярких примеров, когда судьбы людей и государств ломались и наоборот были спасены с помощью информации.

Например, согласно сведениям древнегреческого историка Геродота искусство тайнописи (сокрытие информации) спасло Древнюю Грецию от порабощения персидским царем Ксерксом. Живший в Персии грек увидел наращивание военной мощи и подготовку к войне Персии и вовремя предупредил своих бывших соотечественников, передав деревянную дощечку с сообщением, покрытую воском (метод стеганографии, сокрытие информации). Греческие города-государства успели объединиться, построить военные корабли. Элемент внезапности был утерян, персидский флот был разбит при Саламине (480 г. до н. э.).

Мария Стюарт, королева Шотландии, была казнена по причине того, что ее письма сообщникам были перехвачены, расшифрованы, вскрылся заговор (использован ненадежный шифр) против английской королевы Елизаветы I (XVII в.).

Расшифровка немецкого кода шифровальной машины «Энигма», поставленной на вооружение немецким военно-морским флотом, совместными усилиями польских, французских и английских ученых и криптографов повлияло на ход Второй мировой войны.

Этим был внесен неоценимый вклад в победу над немецкими подводными лодками, высадку союзников в Нормандии в июне 1944 г.

В настоящее время проблема защиты информации по-прежнему важна и актуальна, хотя изменились технологии хранения, обработки и передачи информации. Например, политики ряда стран говорят о кибератаках хакеров на правительственные базы данных, влиянии на результаты предвыборных кампаний и выборов. Защита информации важна не только на государственном уровне – мы оберегаем и свои личные данные, кроме того, для безопасности компаний и организаций важны соблюдение коммерческой и служебной тайны.

Широкое применение информационных технологий в практической деятельности в сочетании с растущим объемом сетевых операций привело к необходимости усиления защиты информации на компьютерах и в сетях.

Задача защиты именно «компьютерной» информации в настоящее время вышла на первое место среди всех других задач, связанных с внедрением информационных технологий, потому что современные компьютеры контролируют и управляют работой ядерных боеголовок, химическим производством, заводами, самолетами в воздухе, промышленными ядерными реакторами, спутниками. В странах с развитыми информационными технологиями ущерб от компьютерных преступлений ежегодно оценивается десятками миллиардов.

Увеличение возможностей по передаче информации:

– высокоскоростные потоки;

– совершенствование структур передачи данных;

– развитие методов передачи информации;

– создание новых видов передачи информации (спутники).

Предпосылки увеличения роли информации:

– развитие средств КТ;

– развитие методов автоматизации обработки данных.

Негативные последствия:

– зависимость людей от эффективности и надежности средств информационных технологий;

– возможность информационного влияния на поведенческие характеристики социальных групп;

– политические интересы;

– коммерческие интересы;

– военные интересы.

1.2. Основные понятия

Информация – одно из базовых понятий в науке (как материя, энергия), которое невозможно выразить через более простые понятия, поэтому используется метод объяснения на примерах или в сравнении с другими понятиями.

Различные подходы к понятию информации

Информация (от лат. informatio) – разъяснение, сведения.

Информация – сведения (сообщения, данные) независимо от формы их представления (Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Информация – это любые сведения об окружающем мире, которые человек получает с помощью органов чувств.

Информация (в широком смысле) – это общенаучное понятие, включающее в себя обмен сведениями между людьми, обмен сигналами между живой и неживой природой, людьми и устройствами, между устройствами без участия человека.

Информация есть информация, а не материя и не энергия (Н. Винер «Кибернетика, или Управление и связь в животном и машине»).

Информацией является то, что в результате ответа (сообщения) превращает неопределенность в определенность; это нематериальный смысл, извлекаемый человеком из сообщения (с точки зрения информатики как технической науки).

Данные – фиксируемые в виде определенных сигналов воспринимаемые факты окружающего мира.

Знание – форма существования и систематизации результатов человека.

Виды информации

Символ (знак, жест), текст (состоит из символов, важен их порядок), числовая информация, графическая информация (рисунки, картины, чертежи, фото, схемы, карты), звук, тактильная информация (осязание), вкус, запах.

Информационные процессы

Сбор; хранение (мозг, бумага, камень, береста, память ПК, дискеты, винчестеры, CD, DVD, магнитная лента); обработка (создание новой информации, кодирование, поиск, сортировка); передача.

Свойства информации

Информация должна быть объективной, понятной, полезной, достоверной, актуальной, полной.

Свойства информации с точки зрения информационной безопасности: защищенность, конфиденциальность, целостность и доступность информации.

Свойство целостности данных – это гарантия их сохранности при случайных и преднамеренных действиях. Целостность данных означает, что данные (и общедоступные, и конфиденциальные) не были изменены, подменены или уничтожены.

Конфиденциальность информации – требование не передавать информацию третьим лицам без согласия ее обладателя.

Доступность информации – свойство информации, состоящее в том, что субъекты, имеющие право доступа, могут реализовать его беспрепятственно.

Федеральный закон «Об информации, информационных технологиях и о защите информации»

Информация в зависимости от порядка ее предоставления или распространения подразделяется:

1) на информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Вся информация делится на общедоступную и ограниченного доступа. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. В законе определяется информация, к которой нельзя ограничить доступ, например информация об окружающей среде или деятельности государственных органов. Оговаривается также, что ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Перечень нормативных актов, относящих сведения к категории ограниченного доступа

Сведения, отнесенные к категории ограниченного доступа	Основания отнесения сведений к категории ограниченного доступа
Государственная тайна	Ст. 5 Закона РФ от 21.07.1993 № 5485-1 «О государственной тайне»
Коммерческая тайна	Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
Персональные данные	Ст. 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
Банковская тайна	Ст. 857 ГК РФ (часть вторая)
	Ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности»
Врачебная тайна	Ст. 13, 92 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»

Информационная безопасность

Информационная безопасность – это состояние защищенности информационной среды общества, обеспечивающее ее формирование и развитие в интересах граждан, организаций и государства.

Информационная безопасность – защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам или пользователям информации и поддерживающей инфраструктуры.

Информационная безопасность:

1) комплекс организационно-технических мероприятий, обеспечивающих целостность данных и конфиденциальность информации в сочетании с ее доступностью для всех авторизованных пользователей;

2) показатель, отражающий статус защищенности информационной системы;

3) состояние защищенности информационной системы;

4) состояние, обеспечивающее защищенность информационных ресурсов и каналов, а также доступа к источникам информации.

ГОСТ «Защита информации. Основные термины и определения» вводит понятие информационной безопасности как состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния.

Меры по обеспечению информационной безопасности должны осуществляться в различных сферах – политике, экономике, обороне, и на различных уровнях – государственном, региональном, организационном и личностном. Задачи информационной безопасности на уровне государства отличаются от задач информационной безопасности на уровне организации.

Информационная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры (системы электро-, водо-, теплоснабжения, кондиционеры, средства коммуникации, обслуживающий персонал).

Международный день защиты информации отмечается 30 ноября 1988 г. В этот год произошла первая массовая компьютерная эпидемия – эпидемия червя Морриса.

Объект информационной безопасности – информация, которая затрагивает государственные, служебные, коммерческие, интеллектуальные и личностные интересы, а также средства и инфраструктура ее обработки и передачи.

Объект информационного воздействия – общественное и индивидуальное сознание (совокупность идей, взгляд в обществе).

Субъекты информационной безопасности – органы законодательной, исполнительной и судебной власти (уровень государства), граждане и общественные объединения (уровень личности), СМИ, предприятия и организации (уровень организаций).

Цель мероприятий в области информационной безопасности – защита интересов субъектов информационной безопасности.

1.3. Нормативные правовые акты в сфере информационной безопасности

– Об информации, информационных технологиях и о защите информации : федер. закон от 27.07.2006 № 149-ФЗ.

– О государственной тайне : закон Рос. Федерации от 21.07.1993 № 5485-1.

– О безопасности : федер. закон от 28.12.2010 № 390-ФЗ.

– О персональных данных : федер. закон от 27.07.2006 № 152-ФЗ.

– Об электронной подписи : федер. закон от 06.04.2011 № 63-ФЗ.

– О коммерческой тайне : федер. закон от 29.07.2004 № 98-ФЗ.

– О средствах массовой информации : закон Рос. Федерации от 27.12.1991 № 2124-1.

– О рекламе : федер. закон от 13.03.2006 № 38-ФЗ.

– О связи : федер. закон от 07.07.2003 № 126-ФЗ.

– О лицензировании отдельных видов деятельности : федер. закон от 04.05.2011 № 99-ФЗ.

– О техническом регулировании : федер. закон от 27.12.2002 № 184-ФЗ.

– Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Рос. Федерации от 05.12.2016 № 646.

– О Концепции правовой информатизации России : указ Президента Рос. Федерации от 28.06.1993 № 966.

– Об основах государственной политики в сфере информатизации : указ Президента Рос. Федерации от 20.01.1994 № 170.

– О президентских программах по правовой информатизации : указ Президента Рос. Федерации от 04.08.1995 № 808.

– О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента Рос. Федерации от 09.05.2017 № 203.

– Об утверждении государственной программы Российской Федерации «Информационное общество (2011–2020 годы)» : постановление Правительства Рос. Федерации от 15.04.2014 № 313.

– О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена : указ Президента Рос. Федерации от 17.03.2008 № 351.

1.4. Информационные опасности и угрозы информационной безопасности

Для создания системы информационной безопасности необходимо выявить источники опасности, угрозы.

Существует четыре действия, которые могут содержать в себе угрозу: сбор, модификация (искажение), утечка и уничтожение информации.

Угрозы информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Атакой называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, – злоумышленником. Потенциальные злоумышленники называются источниками угрозы.

Угроза является следствием наличия уязвимых мест или уязвимостей в информационной системе. Уязвимости могут возникать по разным причинам, например в результате непреднамеренных ошибок программистов при написании программ.

Угрозы можно классифицировать по нескольким критериям:

– по свойствам информации (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;

– компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);

– способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);

– расположению источника угроз (внутри/вне рассматриваемой информационной системы);

– в зависимости от способа воздействия на объекты информационной безопасности (информационные, программные, физические, радиоэлектронные и организационно-правовые угрозы).

К *внутренним угрозам* относятся: ошибки пользователей и системных администраторов; нарушения сотрудниками фирмы установленных правил сбора, обработки, передачи и уничтожения информации; ошибки в работе программного обеспечения; отказы и сбои в работе компьютерного оборудования.

Внешние угрозы проявляются в форме заражения компьютерными вирусами (вредоносными программами); несанкционированного доступа к корпоративным системам; информационного мониторинга (отслеживания) со стороны конкурирующих структур, разведывательных и специальных служб; действия государственных структур и служб (сбор, модификация, изъятие, уничтожение информации); аварии, пожары, техногенные катастрофы, стихийные бедствия.

К с*лучайным угрозам* можно отнести, например, случайные ошибки пользователей и системных администраторов, компьютерную неграмотность или ошибки в работе программного обеспечения. К преднамеренным – создание и распространение вредоносных программ.

Информационные угрозы: несанкционированный доступ к информационным ресурсам; незаконное копирование данных в информационных системах; хищение информации из библиотек, архивов, банков и баз данных; нарушение технологии обработки информации; противозаконный сбор и использование информации; использование информационного оружия.

К *программным угрозам* относятся использование ошибок и «дыр» в программном обеспечении; компьютерные вирусы и вредоносные программы; установка «закладных» устройств (шпионы, жучки в клавиатуру, сервер, телекоммуникационную аппаратуру).

В качестве *физических опасностей* можно рассматривать уничтожение или разрушение средств обработки информации и связи; хищение носителей информации; хищение программных и аппаратных ключей и средств криптографической защиты данных; воздействие на персонал.

Радиоэлектронные угрозы: внедрение электронных устройств перехвата информации в технические средства и помещения; перехват, расшифровка, подмена и уничтожение информации в каналах связи.

К *организационно-правовым опасностям* относят нарушение требований законодательства и задержку в принятии необходимых нормативно-правовых решений в информационной

сфере, закупки несовершенных и устаревших информационных технологий и средств информатизации.

1.5. Информация как объект права

В процессе создания, распространения, преобразования и потребления информации возникают общественные отношения, которые требуют правового регулирования.

Правовое обеспечение защиты информации представляет собой совокупность законов и других нормативно-правовых актов, организационных решений, которые регламентируют, упорядочивают общие вопросы обеспечения защиты информации, организацию и функционирование защиты конкретных объектов и систем.

В результате образовалась самостоятельная область законодательства, которая регулирует информационные отношения:

– законодательство об интеллектуальной собственности;

– законодательство о СМИ;

– законодательство о формировании информационных ресурсов и предоставлении информации из них;

– законодательство о реализации права на поиск, получение и использование информации;

– законодательство о создании и применении информационных технологий и средств их обеспечения.

Информационные отношения возникают при формировании и использовании информационных ресурсов, создании и использовании информационных технологий, средств их обеспечения, защите информации, прав субъектов.

Отрасли права, которые содержат информационно-правовые нормы:

– конституционное право;

– административное право;

– гражданское право;

– уголовное право;

– предпринимательское право.

Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации: дисциплинарная, гражданско-правовая, административная, уголовная.

1.6. Государственные органы, регулирующие вопросы защиты информации

Регулирующие органы

1. ФСТЭК России – Федеральная служба по техническому и экспортному контролю.

Государственные функции:

– осуществление контроля за соблюдением лицензионных требований при осуществлении деятельности по технической защите конфиденциальной информации и по разработке и производству средств защиты конфиденциальной информации;

– осуществление в пределах своей компетенции контроля за экспортом и (или) импортом товаров (работ, услуг), информации, результатов интеллектуальной деятельности, в отношении которых установлен экспортный контроль;

– осуществление контроля за проведением независимой идентификационной экспертизы товаров и технологий в целях экспортного контроля.

2. ФСБ России – Федеральная служба безопасности Российской Федерации.

Государственные услуги:

1) осуществление лицензирования деятельности:

– по выявлению электронных устройств, предназначенных для негласного получения информации;

– разработке и производству средств защиты конфиденциальной информации;

– разработке, производству, распространению шифровальных средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных средств, выполнению работ, оказанию услуг в области шифро-

вания информации, техническому обслуживанию шифровальных средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных средств;

2) осуществление и организация сертификации средств защиты информации, систем и комплексов телекоммуникаций, технических средств, используемых для выявления электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах, специальных технических средств, предназначенных для негласного получения информации, технических средств обеспечения безопасности и (или) защиты информации;

3) регулирование в области ввоза в Российскую Федерацию и вывоза из Российской Федерации специальных технических средств, предназначенных для негласного получения информации.

3. Минкомсвязь России – Министерство связи и массовых коммуникаций Российской Федерации.

Занимается выработкой и реализацией государственной политики и нормативно-правовым регулированием в следующих сферах:

– информационных технологий (включая использование информационных технологий при формировании государственных информационных ресурсов и обеспечение доступа к ним),

– электросвязи (включая использование и конверсию радиочастотного спектра) и почтовой связи,

– массовых коммуникаций и СМИ, в том числе электронных (включая развитие сети Интернет, систем телевизионного (в том числе цифрового) вещания и радиовещания и новых технологий в этих областях),

– печати, издательской и полиграфической деятельности,

– обработки персональных данных.

Среди приоритетных направлений деятельности Минкомсвязь России выделяет такие, как информатизация госорганов, электронные услуги для граждан и бизнеса, инфраструктура электронного правительства, стратегия и «дорожная карта» раз-

вития ИТ-отрасли, реестр отечественного ПО, цифровая экономика, государственная информационная система ЖКХ (ГИС ЖКХ), безопасный Интернет и др.

4. Роскомнадзор – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Сферы деятельности:

– массовые коммуникации (регистрация СМИ, лицензирование, контрольная и надзорная деятельность в сфере СМИ),

– связь (разрешительная деятельность в сфере связи, лицензирование, контроль и надзор),

– персональные данные (защита прав субъектов персональных данных, портал персональных данных, реестр операторов персональных данных).

5. Технический комитет ТК 26 по стандартизации «Криптографическая защита информации».

За техническим комитетом закреплены объекты стандартизации, относящиеся к методам шифрования информации, способам их реализации, а также методам обеспечения безопасности информационных технологий с использованием криптографического преобразования информации, включая аутентификацию, имитозащиту и электронную цифровую подпись.

6. Росстандарт – Федеральное агентство по техническому регулированию и метрологии.

Государственные функции: оказание государственных услуг, управление государственным имуществом в сфере технического регулирования и метрологии; контроль и надзор за соблюдением обязательных требований государственных стандартов и технических регламентов.

7. Совет безопасности Российской Федерации.

Государственные функции: обеспечение реализации функций Президента Российской Федерации по управлению государством, формированию внутренней, внешней и военной политики в области безопасности, сохранению государственного суверенитета России, поддержанию социально-политической стабильности в обществе, защите прав и свобод граждан, в том числе по информационной безопасности.

8. Комитет Государственной Думы по безопасности и противодействию коррупции.

Контрольные вопросы и задания

1. Приведите исторические примеры влияния надежности защиты информации на человеческие судьбы и судьбы государств.

2. В чем состоит актуальность защиты информации сегодня?

3. В чем состоит цель изучения дисциплины «Информационная безопасность», каковы задачи изучения, содержание дисциплины?

4. Перечислите основные нормативные правовые акты, связанные с защитой информации.

5. Назовите различные точки зрения понимания информации. Перечислите ее виды и свойства.

6. Как связаны с понятием информации понятия «данные», «знания»?

7. Назовите информационные процессы.

8. Что понимают под термином «информационная безопасность»? Есть ли отличие от понятия «защита информации»?

9. Что такое конфиденциальность, целостность и доступность информации?

10. Что является источником опасностей и угроз информации? Классифицируйте информационные опасности и угрозы.

11. В чем состоит понимание информации как объекта права? Когда возникают информационные отношения? Какие отрасли права они затрагивают?

12. Какие виды информации выделяются в соответствии с федеральным законом «Об информации, информационных технологиях и о защите информации»?

Литература по теме: 1–17, 19–21, 23, 25–28, 31, 33–34.

ТЕМА 2
МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется комплексный подход. Выделяют следующие уровни защиты информации:

– законодательный – законы, нормативные акты и прочие документы Российской Федерации и международного сообщества;

– административный – комплекс мер, предпринимаемых локально руководством организации;

– процедурный уровень – меры безопасности, реализуемые людьми;

– программно-технический уровень – непосредственно средства защиты информации.

В соответствии со ст. 16 п. 1 федерального закона «Об информации, информационных технологиях и о защите информации» защита информации представляет собой принятие правовых, организационных и технических мер. При такой трактовке защита информации включает и физические меры.

2.1. Законодательные мероприятия по обеспечению информационной безопасности

Законодательные (правовые) меры – это меры по разработке и практическому применению законов, постановлений, инструкций и правил эксплуатации, контроля как аппаратного обеспечения, так и программного обеспечения компьютеров и информационных систем, включая линии связи, а также все объекты инфраструктуры, обеспечивающие доступ к этим системам.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые по-

нятия предметной области и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) отношение к людям, нарушающим информационную безопасность.

В России деятельность в информационной сфере регулируют более 1000 нормативных документов. Уголовное преследование за преступления в этой сфере осуществляется в соответствии с Уголовным кодексом Российской Федерации (Раздел IX. Преступления против общественной безопасности и общественного порядка. Глава 28. Преступления в сфере компьютерной информации, статьи 272, 273, 274).

Ст. 272. Неправомерный доступ к компьютерной информации

Неправомерный доступ к компьютерной информации – это незаконное или неразрешенное собственником или иным законным владельцем использование возможности получения компьютерной информации.

Доступ – проникновение в ее источник с использованием средств (вещественных и интеллектуальных) компьютерной техники, позволяющее использовать компьютерную информацию (копировать, модифицировать, блокировать, уничтожать).

Предусмотрено наказание в зависимости от тяжести последствий, ущерба, количества участников преступления: штраф (до 200–500 тысяч рублей), исправительные работы (в срок до 1–2 лет), ограничение свободы (на срок до 2–5 лет), принудительные работы (до 2–5 лет), лишение свободы (до 2–7 лет).

Ст. 273. Создание, использование и распространение вредоносных компьютерных программ

Вредоносные компьютерные программы – это компьютерные программы или компьютерная информация, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Предусмотрено наказание в зависимости от тяжести последствий, ущерба, количества участников преступления: ограничение свободы (на срок до 4 лет), принудительные работы (до 4–5 лет) и лишение права занимать определенные должности (на срок до 3 лет), лишение свободы (до 4–7 лет) и штраф (до 200 тысяч рублей) и лишение права занимать определенные должности (на срок до 3 лет).

Ст. 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Предусмотрено наказание в зависимости от тяжести последствий, ущерба: штраф (до 500 тысяч рублей), исправительные работы (в срок до 1 года), ограничение свободы (на срок до 2 лет), принудительные работы (до 2–5 лет), лишение свободы (до 2–5 лет).

Законодательный уровень является важнейшим для обеспечения информационной безопасности (регламентация законом и нормативными актами действий с информацией и оборудованием, наступление ответственности за нарушение правильности таких действий).

Большинство людей не совершают противоправные действия не потому, что это технически невозможно, а потому, что это осуждается и (или) наказывается обществом, потому, что так поступать не принято.

На законодательном уровне различаю две группы мер:

1) меры, направленные на созидание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности – меры ограничительной направленности (их большинство в Российской Федерации);

2) направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

Самое важное и самое трудное на законодательном уровне – это создать механизм, позволяющий согласовывать процесс разработки законов с реалиями и прогрессом информационных технологий.

Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих негативных моментов, это ведет к снижению информационной безопасности.

Подводя итог, можно отметить основные направления деятельности на законодательном уровне: разработка новых законов с учетом интересов всех категорий субъектов информационных отношений; обеспечение баланса созидательных и ограничительных законов; интеграция в мировое пространство; учет современного состояния информационных технологий.

2.2. Административные мероприятия по обеспечению информационной безопасности

Административный (организационный) уровень информационной безопасности – это действия общего характера, предпринимаемые руководством организации.

Главная идея мер административного уровня – сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел. Основа программы – политика безопасности, которая отражает подход организации к защите своих информационных активов.

Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

Политика безопасности – совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и информационных ресурсов. Политика безопасности определяет структуру системы защиты и реализуется через административно-организационные

меры и физические и программно-технические средства. После того как сформулирована политика безопасности, можно приступать к составлению программы ее реализации.

Два уровня программы работ в области информационной безопасности:

1) верхний, центральный, затрагивает всю организацию. Возглавляет лицо, отвечающее за информационную безопасность организации. На этом уровне принимаются стратегические решения по обеспечению безопасности, оцениваются технологические новинки;

2) нижний уровень обеспечивает надежную и экономичную защиту конкретного сервиса или группы сервисов. На этом уровне решается, какие следует использовать механизмы защиты, закупаются и устанавливаются технические средства, выполняется повседневное администрирование, отслеживание состояния слабых мест. за этот уровень отвечают администраторы сервисов.

Политика безопасности:

– что нужно защищать в первую очередь?

– какие угрозы наиболее опасны?

– как организуется защита информации?

– кто имеет право доступа к информации (чтение, изменение)?

– кто отвечает за информационную безопасность?

– что запрещено и как наказывают за эти нарушения?

Организационные (административные) меры:

– разработка политики безопасности для информационных систем (определение профилей, паролей, атрибутов, прав доступа);

– разработка средств управления безопасностью (кто, когда и в каком порядке изменяет политику безопасности);

– распределение ответственности за безопасность (кто и за что отвечает при нарушении политики безопасности);

– обучение персонала безопасной работе и периодический контроль за деятельностью сотрудников;

– контроль за соблюдением установленной политики безопасности;

– разработка мер безопасности на случай природных, техногенных катастроф и террористических актов (отвечают руководители, начальники службы безопасности, системные администраторы).

2.3. Процедурные мероприятия по обеспечению информационной безопасности

Процедурный (физический) уровень информационной безопасности – меры безопасности, ориентированные на людей, а не на технические средства. Именно люди формируют режим информационной безопасности, и они же оказываются главной угрозой, поэтому «человеческий фактор» заслуживает особого внимания.

Осознавая степень зависимости от компьютерной обработки данных в современном обществе, следует сделать акцент на вопросах доступности и целостности данных.

Классы мер на процедурном уровне: управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушение режима безопасности, планирование восстановительных работ.

1. Управление персонала начинается с приема нового сотрудника на работу и даже раньше – с составления описания должности. Уже на данном этапе желательно подключить к работе специалиста по информационной безопасности для определения компьютерных привилегий для должности.

Существует два принципа при управлении персоналом для уменьшения ущерба от случайных или умышленных некорректных действий:

– принцип разделения обязанностей (распределять роли и ответственность так, чтобы один человек не мог нарушить критически важный для организации процесс);

– принцип минимизации привилегий (выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей).

Далее кандидат на должность проходит обучение, знакомится со служебными обязанностями, нормами и процедурами информационной безопасности.

При возникновении конфликта между сотрудником и организацией производится физическое ограничение доступа к рабочему месту (в случае увольнения), у него принимают все компьютерное хозяйство, в частности криптографические ключи, если использовались средства шифрования.

2. Физическая защита. Безопасность информационной системы зависит от окружения, в котором она функционирует. Необходимо принять меры для защиты зданий и прилегающей территории, поддерживающей инфраструктуры (сети), вычислительной техники, носителей данных. Основной принцип – непрерывность защиты во времени и пространстве.

Основные направления физической защиты:

– физическое управление доступом,

– противопожарные меры,

– защита поддерживающей инфраструктуры,

– защита от перехвата данных,

– защита мобильных систем.

3. Поддержание работоспособности. В данном случае следует учитывать фактор безопасности в повседневной работе. Дорогие средства безопасности теряют смысл, если они конфликтуют с другим программным обеспечением. Нужно выснить, менялся ли пароль администратора с момента установки. Кроме того, нечаянные ошибки администратора и пользователей грозят повреждением аппаратуры, разрушением программ и данных.

Направления повседневной деятельности, направленные на поддержание работоспособности: поддержка пользователей, поддержка программного обеспечения, конфигурационное управление, резервное копирование, управление носителями, документирование, регламентные работы.

4. Реагирование на нарушение режима безопасности. Программа безопасности, принятая организацией, должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима безопасности.

Последовательность действий должна быть спланирована заранее. Необходимо локализовать инцидент, уменьшить наносимый вред, выявить нарушителей, предупредить повторные нарушения.

В организации должен быть человек, доступный 24 часа в сутки (лично, по телефону, через электронную почту), который отвечает за реакцию на нарушения. Чтобы найти нарушителя, нужно заранее выяснить контактные координаты поставщика сетевых услуг. Позаботиться заранее об уменьшении ущерба.

5. Планирование восстановительных работ. Ни одна организация не застрахована от серьезных аварий, вызванных естественными причинами, действиями злоумышленника, халатностью или некомпетентностью.

Планирование восстановительных работ позволяет подготовиться к авариям, уменьшить ущерб от них и сохранить способность функционировать хотя бы в минимальном объеме.

Меры информационной безопасности делятся на три группы: предупреждение атак, обнаружение атак, ликвидация последствий атак.

Процесс планирования восстановительных работ делится на этапы:

– выявить важные функции организации,

– выявить ресурсы для обеспечения этих функций, определить перечень возможных атак,

– разработать стратегию восстановительных работ,

– подготовиться к реализации стратегии, проверить стратегию.

При определении перечня аварий нужно попытаться разработать их сценарии. Как будут развиваться события? Каковы могут быть масштабы ущерба? Что произойдет с ресурсами?

Например, смогут ли сотрудники попасть на работу, будут ли выведены из строя компьютеры? Возможны ли случаи сабо-

тажа? Будет ли работать связь? Пострадает ли здание организации? Можно ли будет найти и прочитать необходимые бумаги?

Должна быть предусмотрена работа по временной схеме, затем возврат к нормальному функционированию.

Использовать меры резервного копирования, хранения копий в нескольких местах, возможность предоставление информации на бумаге и в файлах.

Меры процедурного уровня:

– мероприятия, осуществляемые при проектировании, строительстве и оборудовании вычислительных центров и других объектов систем обработки данных;

– мероприятия по разработке правил доступа пользователей к ресурсам системы (политика безопасности);

– мероприятия при подборе и подготовке персонала, обслуживающего систему;

– организация охраны и режима доступа к системе;

– организация учета, хранения, использования и уничтожения документов и носителей информации;

– организация явного и скрытого контроля за работой пользователей;

– распределение реквизитов разграничения доступа;

– мероприятия при проектировании, разработке, ремонте и модифицировании оборудования и программного обеспечения.

Физические меры:

– обеспечивают ограничение доступа к компьютерам, линии связи, телекоммуникационному оборудованию и контроль доступа;

– направлены на управление доступом физических лиц, автомобилей, грузов в охраняемую зону, на противодействие средствам агентурной и технической разведки.

Функции:

– внешняя защита (нейтрализация электромагнитных излучений, разграничение физического доступа, охрана периметра, территории, помещений, визуальное и видеонаблюдение);

– опознавание (людей и грузов, идентификация технических средств, техники);

– внутренняя защита (идентификация, разграничение доступа, подавление электромагнитных излучений, сигнализация, блокировка, ограничение физического доступа в помещение).

2.4. Программно-технические мероприятия по обеспечению информационной безопасности

Программно-технические (технические, технологические, программно-аппаратные) меры направленны на контроль оборудования, программ, данных (использование специальных программ и аппаратуры с функцией защиты информации).

Основной ущерб наносят действия легальных пользователей, по отношению к которым процедурные меры малоэффективны. Главные враги – некомпетентность и неактивность при выполнении служебных обязанностей. Им могут противостоять только программно-технические меры.

Быстрое развитие информационных технологий затрудняет обеспечение надежной защиты информации.

Причины:

1) повышение быстродействия микросхем позволяет преодолевать методом грубой силы криптографические и другие барьеры в защите информации;

2) развитие сетей и сетевых технологий, увеличение числа связей между информационными системами, рост пропускной способности каналов расширяют круг злоумышленников, имеющих технические возможности организовать атаки;

3) появление новых информационных сервисов ведет к образованию новых уязвимых мест как внутри сервисов, так и на месте их стыков;

4) конкуренция среди производителей программного обеспечения заставляет сокращать сроки разработки, что приводит к снижению качества тестирования, выпуску продуктов с дефектами защиты;

5) навязываемая потребителям идея постоянного наращивания мощности аппаратного и программного обеспечения не

позволяет долго оставаться в рамках надежных и апробированных конфигураций, что приводит к увеличению финансирования и сокращению доли финансирования на безопасность.

Сервис обеспечения безопасности:

– идентификация и аутентификация пользователей;

– управление (разграничение) доступом, к ресурсам;

– протоколирование и аудит (регистрация событий);

– шифрование (криптографическая защита);

– контроль целостности систем;

– экранирование (создание физических препятствий на путях проникновения нарушителей);

– анализ защищенности;

– проверка отсутствия вредоносных программ;

– создание резервных копий ценной информации;

– мониторинг и сигнализация соблюдения правильности работы системы;

– защита системы от наличия и появления нежелательной информации,

– виртуальные частные сети;

– средства контентной фильтрации.

Межсетевые экраны (система – барьер между двумя сетями, проверяет пакеты данных на соответствие входящего и исходящего IP-адреса в базе разрешенных адресов). Брандмауэр, файерволл, сетевой экран является необходимый элемент сетевой защиты и безопасности, в том числе без пользователя, подключенного к сети Интернет. Блокирует нежелательное проникновение внутрь компьютера через компьютерную сеть: контролирует сетевой трафик – пропускать (фильтровать) в Интернет или запускать из Интернета только те программы, которые разрешены (все остальные блокируются на вход и выход).

Приемы защиты, которые реализуются непосредственно с использованием защищаемых объектов (компьютеров, средств телекоммуникации):

– антивирусная защита;

– создание защищенных сетевых соединений;

– разграничение прав доступа;

– резервирование (резервное копирование);

– создание защитных атрибутов;

– парольная защита;

– хеширование (преобразование исходного файла в файл меньшей длины);

– преобразование информации к нечитаемому виду (перекодирование, шифрование, стеганография);

– архивирование (сжатие) информации;

– электронная подпись.

2.5. Криптографические методы защиты информации

Криптография – наука о принципах, средствах и методах преобразования информации для защиты ее от несанкционированного доступа и искажения для обеспечения надежности и быстродействия.

Цель – разработка шифров и соответствующего программного обеспечения.

Помимо криптографии (преобразования информации) для защиты информации применяется стеганография (сокрытие информации).

Криптографические методы позволяют: шифровать информацию, реализовать электронную подпись, распределять ключи шифрования, защищать от случайного и умышленного изменения информации.

В криптографии используют методы замены, подстановки (один символ меняют на другой) и перестановки (текст разбивается на группы, внутри каждой группы буквы меняются местами, переставляются).

Метод замены получил толчок в развитии: кодирование – целое слово заменяется одним символом, кодом (неэффективно, так как слов много); шифрование – одна буква заменяется другой (позволяет зашифровать текст любого размера).

Готовое к передаче сообщение (документ) называется открытым, исходным, незащищенным текстом. В процессе передач по незащищенным каналам связи оно может быть легко перехвачено, отслежено. Для предотвращения несанкционированного доступа сообщение шифруется, преобразуется в шифрограмму, закрытый текст. Получатель сообщения дешифрует его посредством обратного преобразования криптограммы, получается исходный открытый текст.

Метод преобразования в криптографической системе определяется специальным алгоритмом (правилом, по которому происходит преобразование информации), работа которого определяется уникальным ключом – шифрующим ключом (условие, которое необходимо знать, чтобы зашифровать текст). Один алгоритм может иметь множество ключей.

В современной криптографии предполагается, что вся секретность сосредоточена в ключе, а не в деталях алгоритма. Степень секретности ключа определяет стойкость (криптоустойчивость, то есть время, необходимое для расшифровки текста; способность шифра противостоять криптоанализу) любой системы закрытой связи. Ключ должен быть известен другим пользователям сети для свободного обмена зашифрованными сообщениями.

Новый алгоритм шифрования изобрести достаточно трудно и вряд ли возможно каждый раз, когда необходимо отправить послание. К одному алгоритму создается множество ключей, по одному для каждого корреспондента.

Количество возможных ключей зависит от числа бит в ключе. Восьмибитный ключ дает 256 числовых комбинаций или ключей. Чем больше возможных ключей, тем труднее вскрыть послание. Таким образом, степень надежности алгоритма зависит от длины ключа. Для передачи наиболее важной информации генерируют ключи в 100 и более бит.

Шифры могут шифровать сразу весь текст (блочный шифр) или по мере поступления (поточный шифр).

В криптографии действуют два противоборствующих направления – криптозащита (отвечает за разработку методов и

средств защиты информации, шифрования) и криптоанализ (разрабатывает методы дешифровки текстов без знания шифра). Примером метода криптоанализа является частотный анализ, который позволяет по частоте появления символа в тексте предположить букву, замененную символом.

Криптографическая система позволяет решить проблему аутентификации принятой информации.

Аутентификация абонента – проверка принадлежности абонента предъявляемому им идентификатору, подтверждение подлинности в сетях.

Типы шифрования: симметричное (использование одного секретного ключа для шифрования и дешифрования); асимметричное (для шифрования используется один ключ – общедоступный, для дешифрования другой – секретный).

Распределение ключей – одна из фундаментальных задач криптографии. Физическое распределение – с помощью доверенных курьеров, вооруженной охраны ключи рассылаются (до 1970-х гг. единственный безопасный путь). Недостатки: криптостойкость зависит в основном не от ключа, а от курьера. С помощью протоколов с открытым ключом: партнеры не доверяют посредникам и лишены возможности встретиться могут договориться об общем секретном ключе в режиме реального времени.

Современная криптография включает в себя асимметричные криптографические системы, системы электронной цифровой подписи, хеш-функции, управление ключами, получение скрытой информации, квантовой криптографии.

Электронная цифровая подпись (ЭЦП).

ЭЦП функционально аналогична обычной рукописной подписи и обладает следующими достоинствами:

– удостоверяет, что подписанный текст исходит от лица, поставившего подпись;

– не дает самому этому лицу (владельцу подписи) возможность отказаться от обязательств, связанных с подписанным текстом;

– гарантирует целостность подписанного текста.

ЭЦП – небольшое количество дополнительной цифровой информации, передаваемой вместе с подписанным текстом.

Производятся две процедуры при установке ЭЦП: формирование ЭЦП (используется секретный ключ отправителя сообщения), проверка ЭЦП (открытый ключ отправителя).

Процедура формирования ЭЦП:

Абонент генерирует пару ключей – секретный и открытый. Открытый ключ вычисляется из парного к нему секретного ключа. Открытый ключ рассылается или публикуется в сети для остальных абонентов (доступен в общем ресурсе).

1. Вычисляется хеш-функция текста (сжимает текст в хеш-код, который характеризует весь текст в целом).

2. Шифруется хеш-код секретным ключом, то есть создается цифровая подпись для текста.

3. Сообщение (текст, файл) и ЭЦП отправляются получателю.

4. Процедура проверки ЭЦП. Получатель расшифровывает хеш-код открытым ключом отправителя и вычисляет хеш-код сообщения самостоятельно, сравнивая их.

5. При совпадении хеш-кодов (полученного и сформированного) делается вывод о подлинности ЭЦП. Иначе либо подпись подделана, либо сообщение изменено в процессе пересылки.

ЭЦП – уникальное число, зависящее от документа и секретного ключа абонента и содержит дополнительную информацию, однозначно идентифицирующую автора подписанного документа. Эта информация и обеспечивает целостность. Содержит дату подписания, номер секретного ключа, срок окончания, информацию о лице, подписавшем файл, имя открытого ключа.

Преимущества: невозможно подделать ЭЦП пользователя без знания его секретного ключа. Следовательно, необходима защита закрытого (секретного) ключа от несанкционированного доступа.

Механизм цифровой электронной подписи основан на алгоритмах асимметричного шифровании, формирует подпись отправителя и позволяет опознать ее получателю.

Механизмы контроля доступа осуществляют проверку полномочий объектов ИТ (программ и пользователей) на доступ к ресурсам сети.

Система регистрации и учета информации отвечает за ведение регистрационного журнала, перекрывает каналы утечки информации, фиксирует все осуществленные и неосуществленные попытки доступа к данным и программам.

Механизмы обеспечения целостности информации устанавливают соответствие между передаваемой информацией и принятой.

Механизмы аутентификации проверка правильности введенной пользователем регистрационной информации для входа в систему.

Механизмы подстановки трафика или подстановки текста реализуют засекречивание потока данных.

Механизмы управления маршрутизацией обеспечивают выбор маршрутов движения информации по сети таким образом, чтобы исключить передачу секретных сведений по небезопасным, физически ненадежным каналам.

Механизмы арбитража обеспечивают подтверждение характеристик данных, передаваемых между объектами ИТ третьей стороной (арбитром).

Контрольные вопросы и задания

1. Какие уровни защиты информации выделяют?
2. Что понимают под комплексным подходом защиты информации?
3. Какие группы мероприятий по защите информации (ЗИ) выделяют?
4. Что понимают под законодательными мерами ЗИ?
5. Что такое меры ограничительной и созидательной направленности?
6. Перечислите акты, затрагивающие вопросы информационной безопасности.
7. Что понимают под административным уровнем ЗИ? Какие мероприятия сюда входят?

8. Что понимается под политикой безопасности предприятия?

9. Раскройте содержание процедурного уровня ЗИ, перечислите его мероприятия, раскройте их суть.

10. Из каких мероприятий состоит программно-технический уровень ЗИ?

11. Назовите причины, затрудняющие обеспечение надежной ЗИ.

12. Укажите сервис обеспечения безопасности.

13. Дайте понятия идентификации и аутентификации.

14. Назовите виды криптографической защиты информации.

Литература по теме: 1 – 34.

ТЕМА 3
МЕТОДЫ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

3.1. Классификация вредоносных программ. Компьютерные вирусы

Вредоносной является программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы. В свою очередь, несанкционированное воздействие на информацию представляет собой воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», утвержденный приказом Ростехрегулирования от 27.12.2006 № 373-ст.

Классификация вредоносных программ

Черви – вредоносные программы, которые несанкционированно (то есть без ведома или без уведомления пользователя) создают свои копии на доступных носителях информации, включая сетевые диски, постепенно занимая все свободное место.

Этим способом они снижают скорость работы компьютера, приводят к полной неработоспособности операционной системы, могут блокировать работу отдельной программы или компьютера в целом. Однако они не совершают деструктивных разрушительных действий и не проводят изменения хранимой

на носителе информации. Лечение: поиск червей или их частей на носителях информации, их удаление.

Вирусы – вредоносные программы, которые несанкционированно создают свои копии (либо их модификации), размещаемые, как правило, в объектах файловой системы. Это небольшие исполняемые или интерпретируемые программы, обладающие свойством распространения и самовоспроизведения в компьютерной системе.

Вирусы заражают эти файлы, внедряя свой машинный код внутрь этих объектов, причем таким образом, чтобы код вируса исполнялся до начала работы зараженного объекта. В процессе распространения вирусы могут себя модифицировать.

Большинство вирусов обладают деструктивными действиями: нарушение работы операционной системы, прикладного программного обеспечения, разрушение файлов, разрушение каталогов, уничтожение папок и файлов, форматирование или шифрование носителей.

В настоящее время в мире насчитывается несколько десятков тысяч зарегистрированных компьютерных вирусов.

Все компьютерные вирусы классифицируются по среде обитания, способу заражения среды обитания, степени опасности воздействия, алгоритму функционирования.

По среде обитания компьютерные вирусы делятся:

– на сетевые (среда обитания – элементы компьютерных сетей);

– файловые (размещаются в исполняемых файлах, поражают все виды двоичных исполняемых файлов, драйверы, объектные модули и системные библиотеки, записывая свое тело внутрь исполняемой программы таким образом, чтобы при запуске зараженной программы первоначально вирус начинал работать);

– загрузочные (находятся в загрузочных секторах, областях внешних запоминающих устройств). Записывают в загрузочные секторы носителей информации головку вируса, размещая тело (большую часть кода) внутри отдельных файлов или программ, почти как файловые вирусы. Загрузочные секторы носителей читаются всегда при обращении к носителю. Это позволяет ак-

тивизировать вирус без открытия файла при вызове окна диска, выводе списка файлов, просмотре структуры дерева каталогов;

– комбинированные (например, загрузочно-файловые – могут размещаться как в загрузочных секторах накопителей на магнитных дисках, так и в теле загрузочных файлов).

Также выделяют:

– вирусы-спутники (размещаются в исполняемых файлах с расширением *.exe). Создается одноименная копия *.com вируса, которая из-за особенностей операционной системы всегда запускается раньше, чем основной файл *.exe;

– Dir-вирусы (от слова директория – каталог). Размещают свою «головку» таким образом, чтобы активизироваться при просмотре зараженного каталога или структуры дерева каталогов;

– макровирусы – написаны на языке высокого уровня, способны проникать и заражать неисполняемые файла, например файлы с документами и шаблонами, подготовленные в MS Word, MS Excel. Переносятся и копируются вместе с зараженными документами;

– полиморфные вирусы – каждая новая копия имеет иную цепочку кода, что затрудняет его обнаружение.

По способу заражения среды обитания компьютерные вирусы делятся:

– на резидентные (после активации полностью или частично перемещаются из среды обитания (сети, загрузочного сектора, файла) в оперативную память ПК);

– нерезидентные (попадают в оперативную память только на время их активности, затем покидают оперативную память полностью, оставаясь в среде обитания).

Жизненный цикл вируса: внедрение, инкубационный период (для скрытия источника происхождения), репродуцирование (саморазмножение), деструкция (искажение, уничтожение).

Способы проявления компьютерного вируса:

– замедление работы ПК, зависание, прекращение работы;

– изменение данных в файлах;

– невозможность загрузки операционной системы;

– прекращение, неправильная работа программы;

– увеличение количества файлов на диске;

– изменение размеров файлов;

– нарушение работоспособности ОС, периодическая перезагрузка;

– появление звуковых эффектов;

– уменьшение объема свободной оперативной памяти;

– возрастание времени доступа к винчестеру;

– изменение времени и даты создания файлов;

– разрушение файловой структуры (исчезновение файлов, искажение каталогов);

– загораются сигнальные лампочки дисковода, когда к нему нет обращения пользователя;

– форматирование диска без команды пользователя.

Резидентная программа – программа, постоянно находящаяся в оперативной памяти ПК.

Несанкционированный доступ – это нарушение установленных правил разграничения доступа, последовавшее в результате стихийных или преднамеренных действий пользователя (овладение информацией лицом, не имеющим права доступа к охраняемым сведением – подслушивание, перехват, копирование, вывод из строя, хищение, наблюдение).

Лечение: поиск и удаление заранее известного кода вируса внутри объектов файловой системы; процедура восстановления работоспособности объекта, файла с документом или программного файла; удаление кода вируса, который способен шифровать код заражаемого объекта, может приводить к невозможности расшифровывания, к потере работоспособности «вылеченного» объекта.

Трояны – вредоносные программы, не несут деструктивных, разрушающих действий, как правило, маскируются под доверенные приложения, проводят шпионскую работу по сбору информации ограниченного доступа. В отличие от вирусов не занимаются несанкционированным копированием.

Стараются выполнять резидентно, то есть постоянно, во время каждого сеанса работы прописаться в оперативной памяти, отслеживать оттуда операции по вводу паролей.

При наличии подключения компьютера к локальной или глобальной сети трояны пытаются несанкционированно и незаметно для пользователя переслать перехваченные пароли хозяину, внедрившему его на компьютер.

Лечение: поиск и удаление троянов.

Программы Adware / Spyware – интересуются «простым» слежением за работой компьютера (слежение не наказуемо по российскому законодательству). Adware осуществляет демонстрацию нежелательной рекламы, Spyware не проявляет свою активность, скрывается.

Вред: сильно замедляет работу компьютера, занимает оперативную и дисковую память, увеличивает интернет-трафик, собирают персональные данные, данные о конфигурации компьютера, введенные с клавиатуры пароли к аккаунтам платежных систем, тексту.

Лечение: поиск и удаление. Лечение осложняется скрытностью присутствия программ данного типа и их активным противодействием лечению и удалению.

Сетевой трафик – «движение, грузооборот», объем информации, передаваемой через сеть за определенный период времени.

Программы-обманщики (Hoax) – не наказуемы по российскому законодательству, изображают, симулируют работу легальных программ, сообщая о наличии ошибок в их работе и требуя платы деньгами за якобы лицензионный ключ для устранения ошибок и лечения.

Например, Hoax.Renos подделывает работу антивирусной программы, сообщает о наличии десятков вирусов даже в лицензионных версиях Windows. За лечение от псевдовирусов Hoax необходимо заплатить.

Root Kit – программы, позволяющие прятать, скрывать другие программы или процессы от операционных систем, файловых менеджеров, антивирусных программ.

Лечение: поиск и удаление, но эти программы изначально предназначены для сокрытия своих действий и действий других вредоносных программ от операционных систем и антивирусных программ.

Ряд фирм работает над созданием Root Kit программ, подключающих защиту до загрузки операционной системы (эти программы используются для благих целей – скрытному установлению и включению защитных механизмов на конкретном компьютере). Антивирусные программы работают только под управлением операционной системы и лечить «до нее» не могут.

Боты/зомби – комплекс программ, организуют удаленное управление различными вредоносными программами. Бот-системы, бот-сети компьютеров для рассылки спама, кибератак.

Эксплойт – программа или ее часть, использует уязвимые места в ПО компьютера для захвата контроля над ним, нарушения функционирования.

Логическая бомба – фрагмент программного кода, программа, осуществляет вредоносные действия при наступлении определенных условий (например, по прошествии некоторого времени).

Пример: программа начисления зарплаты, которая при отсутствии денежных выплат ее разработчику разрушает бухгалтерскую базу данных.

Логическая бомба может быть внедрена внутрь другой вредоносной или обычной программы. Автоматически ликвидируется при окончании исполнения заданного алгоритма.

«Люк» – модуль, вставленный в программу на этапе отладки для облегчения работы (отражается на системе защиты).

Backdoor – программы, которые обеспечивают скрытное управление работой компьютера, позволяют производить манипуляции с компьютером (ввод с клавиатуры, управление курсором, просмотр содержимого окон и экрана, доступ к периферийному оборудованию), опасна для управляющей и администрирующей деятельности, электронных платежных систем.

Killer – программы (убийцы), активно противодействуют работе антивирусных программ, другим защитным механизмам до их полного уничтожения.

Спам и фишинг

Спам-сторожа – не выявляют вредоносные программы и не проводят лечение; контролируют выполнение некоторых операций на диске, которые часто используют вредоносные программы, и сообщают об этих операциях пользователю. Перечень операций, какая программа и когда их «заставила» выполняться, записывается в журнал. Проанализировав записи в журнале, пользователь может сделать вывод о несанкционированности некоторых операций, возможном воздействии вредоносных программ.

Детекторы (сканеры) – программы, содержащие внутри себя или в отдельных подключаемых библиотеках базы данных с цепочками кодов (сигнатур), присущими ранее выявленным вирусам (ищут «известные» версии вредоносных программ). Проверяя файлы на наличие таких цепочек, детекторы находят и, вырезая вредоносный код, убивают вирусы.

Недостаток детекторов: невозможность обнаружения и лечения новых, незнакомых вирусов, вирусов-невидимок (стелс) и самомодифицирующихся (полиморфных) вирусов. Сканеры, реализующие детектирующие функции, встроены во все современные антивирусные программы.

Полиморфные детекторы – программы, создающие на основе одной сигнатуры полиморфного вируса базу данных, содержащую до 1 миллиона его модификаций, что позволяет обнаружить практически все полиморфные вирусы (например, NOD 32).

Программы-мониторы (модули многофункциональных программ) позволяют постоянно за счет размещения в оперативной памяти компьютера контролировать все процессы в реальном времени, в точение всего сеанса работы пользователя. Мониторы входят в состав программ всех современных антивирусных программ.

Эвристические доктора – программы, способные находить группу вирусов по общим признакам, даже если вирусы имеют разное внутреннее строение (разные сигнатуры). Типичный общий признак для большинства вирусов – несанкционирован-

ное копирование, которое доктора и фиксируют. В сочетании с поиском и удалением известных сигнатур можно найти ранее выявленные вирусы либо заподозрить новый неизвестный вирус. Эвристические подходы используют большинство современных антивирусных программ (например, DOCTOR WEB, AVP Касперского).

Карантинные доктора («виртуальные песочницы») используются на особо опасных участках заражения, позволяют вновь прибывшим на компьютер программам работать, но только в отдельной изолированной области памяти. За ними в это время наблюдают программы-доктора. Если в течение определенного времени «гости» не заявят о себе плохо, то карантин заканчивается и они пропускаются в «общую компанию». В противном случае при подозрении «гости» удаляются с компьютера. Пример: программы семейства eSafeProtect, AVZ.

Проактивная защита – программы, которые кроме эвристического анализа проводят мониторинг системного реестра, работы приложений с оперативной памятью, контроль целостности наиболее важных системных файлов. Пример: антивирусный пакет AVP Касперского.

Перечень актуальных антивирусных программных средств: Антивирус Касперского, ESET NOD 32, DOCTOR WEB, F-Secure Anti-Virus, Avast!Professional Edition, AVG Anti-Virus Free Edition, Avira AntiVir Personal Edition, Norton AntiVirus, Panda Antivirus, Sophos Norton Virus Control, McAffee VirusScan.

Однако нужно отметить, что нет лучшей антивирусной программы, нет единого лекарства, у каждой свой принцип работы, свои типы вредоносных программ. Также антивирусные средства несовместимы для одновременной установки на один компьютер, не могут работать одновременно.

В качестве лучшего и самого быстрого сканера можно назвать NOD 32, лучший эвристик – Avira AntiVir Personal Edition, DOCTOR WEB, лучший проактив – Антивирус Касперского.

При подозрении, что компьютер заражен, следует:

– провести архивирование наиболее существенной информации (на случай, если в процессе лечения она будет повреждена);

– затем выключить компьютер (перезагружать нежелательно, некоторые вирусы активизируются именно после загрузки);

– по возможности необходимо загрузить ОС с внешнего защищенного от записи носителя информации (CD-ROM, DVD или вновь подключенного проверенного винчестера);

– запустить с защищенного от записи диска, CD-ROM, DVD самую свежую версию антивирусной программы;

– проверить работоспособность ОС или приложений после работы антивирусной программы;

– после завершения работы антивирусной программы, если лечение прошло успешно (не осталось вирусов), желательно запустить программу ScanDisk для проверки каждого из логических дисков винчестера);

– если работоспособность системы, программ не удалось восстановить после работы антивирусной программы, провести установку этих программ заново.

Microsoft ScanDisk – утилита, исправляет ошибки в структуре жесткого диска, ищет и помечает «испорченные» части, удаляет «потерянные» кластеры.

Все «приносимые извне» на компьютер материалы должны подвергаться немедленной, до размещения на компьютере, антивирусной проверке или помещению в карантин.

Выполнить это требования при работе в Интернете непросто. Следует сохранять все, что получено в текущем сеансе работы в Интернете, в отдельную папку. Сразу после завершения работы в Интернете проверить эту папку и папку Temporary Internet Files на наличие вирусов. Только после этого можно работать с подозрительными материалами, включая почтовые вложения.

Контрольные вопросы и задания

1. Чем определяется вредоносность программ?
2. Назовите классификацию вредоносных программ (ВП).

3. В чем выражается гибридность современных ВП?

4. Что такое дерево классификации ВП?

5. Какой ущерб информации могут нанести ВП?

6. Назовите пути заражения ВП.

7. Какие вы знаете правила профилактики и лечения от ВП?

8. Кто создает ВП?

9. Что такое спам? фишинг?

10. Что понимается под антивирусом?

11. Перечислите методы поиска ВП.

12. Как классифицируются антивирусные программы по типу действия?

13. Назовите критерии выбора оптимальной защиты от ВП.

14. Укажите перспективные средства защиты от ВП.

Литература по теме: 1–17, 19–21, 23–28, 31–34.

ТЕМА 4
КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ

Стремительное развитие процесса информатизации общества и его распространение практически во все сферы жизни и деятельности людей создает объективные условия для появления нового вида правонарушений – информационной преступности. Информационная преступность имеет те же корни, что и преступность в целом, но обладает рядом особенностей, которые позволяют отнести ее проявления к особому типу «преступлений высоких технологий». Большая часть преступлений данного разряда формально может оцениваться как мошенничество, незаконные финансовые операции, обман потребителя и т. д.

Основные виды информационных преступлений:

– информационные преступления в интеллектуальной сфере;

– информационные преступления против личности;

– компьютерные преступления.

Широкое применение информационных технологий принесло и негативные явления. Самыми общественно опасными из них явились компьютерные преступления:

– несанкционированный доступ с целью овладения закрытой информацией;

– несанкционированный доступ с целью изменения данных, их модификации;

– создание и распространение вредоносных программ и т. д.

Такие действия вместе с достижением преступных целей часто приводят к нарушению работоспособности отдельных программ и систем, наносят существенный материальный ущерб.

Следует отметить использование компьютерных технологий как средства достижения преступных целей, например фальсификация документов, изготовление фальшивых денежных знаков и т. д.

Экономические:
– обогащение путем взлома информационных систем;
– компьютерный шпионаж;
– кража программ («пиратство»).
Против личных прав:
– ложная информация;
– незаконный сбор информации;
– разглашение банковской и врачебной тайны.
Против общественных и государственных интересов:
– разглашение государственной тайны;
– утечка информации;
– искажение информации (подсчет голосов);
– вывод из строя информационных систем (диверсии).

Информационные преступления в интеллектуальной сфере

Нарушение прав граждан и организаций на интеллектуальную собственность. Например, распространение на информационном рынке «пиратской» информационной продукции – компьютерных программ, баз данных, аудио- и видеопродукции.

Рынки «пиратской» информационной продукции сегодня существуют практически во всех странах. Особенно сильно они развиты там, где процесс информатизации общества находится в начальной стадии и информационное законодательство практически отсутствует. Некоторые производители рассматривают «пиратство» как способ рекламы продукции.

Информационные преступления против личности

Объектами авторского права:

1) являются:

– программы для компьютеров (включая подготовительные материалы, а также звук, графику и видео, которые получаются с помощью программы);

– базы данных (данные, специально организованные для поиска и обработки с помощью компьютеров);

2) не являются:

– алгоритмы и языки программирования;

– идеи и принципы, лежащие в основе программ, баз данных, интерфейса;

– официальные документы.

Использование программ и баз данных

Основания:

– договор в письменной форме;

– при массовом распространении – лицензионное соглашение на экземпляре.

Можно без разрешения автора:

– хранить в памяти одного компьютера (или по договору);

– вносить изменения, необходимые для работы на компьютере пользователя (но не распространять!);

– исправлять явные ошибки;

– изготовить копию для архивных целей.

Компьютерные преступления

Компьютерные преступления – преступления, совершенные с помощью вычислительной техники и вычислительных сетей, направленные на незаконное похищение информации или приводящие к ее модификации или разрушению.

К числу наиболее уязвимых объектов с точки зрения компьютерных преступлений относятся:

– АИС органов государственной власти;

– системы управления объектами жизнеобеспечения и критическими технологиями;

– системы управления войсками, вооружением и военной техникой;

– учетные АИС правоохранительных органов;

– кредитно-финансовая система;

– государственные и муниципальные регистрационные системы;

– биржи;

– ИС подразделений таможни;

– учетные АИС налоговых служб.

Особенности компьютерных преступлений

Правонарушения в киберпространстве включают в себя все, что происходит в физическом мире: воровство, рэкет, вандализм, шпионаж и слежку, подслушивание, вымогательство, мошенничество и обман.

Хотя компьютерные преступления имеют те же цели, что и нападения в физическом мире, все же они будут существенно различаться: будут проще, шире распространены и более разрушительны.

У Интернета есть три свойства, которые помогают осуществлять преступную атаку:

1) автоматизация – решение повторяющихся задач, даже если возможное число успешных попыток мизерно;

2) действие на расстоянии – если раньше человек защищал склад в конкретном месте, то ему приходилось думать о преступниках в этом месте. Теперь благодаря Интернету все компьютеры равноудалены от любого другого компьютера, и человеку надлежит принимать во внимание преступность всего мира. Также Интернет затрудняет поиск преступников и их обвинение;

3) легкость передачи опыта, удачных атак по Интернету – только первому нападающему приходится быть изобретательным, все остальные могут просто использовать его программы.

В качестве орудия преступления может выступать машинная информация, компьютер, компьютерная сеть, компьютерная система.

Преступления, имеющие своим предметом лишь аппаратно-технические средства вычислительных машин (хищение, уничтожение), подпадают под другой тип уголовных правонарушений – гл. 21 «Преступления против собственности».

Последствия неправомерного использования информации могут быть разнообразными: нарушение неприкосновенности интеллектуальной собственности, разглашение сведений о частной жизни граждан. Имущественный ущерб, потеря репутации организации. Различные виды нарушений нормальной

деятельности предприятий, отрасли. Поэтому преступления данного вида помещены в раздел «Преступления против общественной безопасности и общественного порядка».

Криминальная характеристика компьютерных преступлений

Цели компьютерных преступлений: хищение средств из автоматизированных денежных фондов, кража информации из баз данных и компьютерных программ, преднамеренное искажение информации, нарушение нормального функционирования систем, повреждение, уничтожение. Основная часть угроз исходит от персонала организации.

Предотвращение и раскрытие компьютерных преступлений

1. Уголовный кодекс Российской Федерации.

Раздел IX. Преступления против общественной безопасности и общественного порядка.

Глава 28. Преступления в сфере компьютерной информации.

Статья 272. Неправомерный доступ к компьютерной информации.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Действия компьютерных преступников тщательно готовятся, маскируются и обнаруживаются спустя продолжительное время. Шансов быть пойманным у компьютерных преступников гораздо меньше, а при поимке меньше шансов попасть в тюрьму. Обнаруживается в среднем 1 % компьютерных преступлений.

Существует много косвенных признаков того, что в организации готовится или осуществляется компьютерное преступление, например: производится перезапись данных без серьезных причин; данные изменяются, стираются, заменяются; данные не обновляются; на ключевых документах появляются подделанные подписи; жалобы клиентов становится хроническими.

Выявление этих признаков не требует специальных знаний, следовательно можно предусмотреть дополнительные меры по совершенствованию компьютерной безопасности.

Организации – жертвы компьютерных преступлений с неохотой сообщают об этом в правоохранительные органы. Латентность компьютерных преступлений чрезвычайно высока. Часто виновные лица увольняются, переводятся в другие структурные подразделения.

Особый интерес приобретают характеристики личности преступников. С криминалистической точки зрения можно выделить несколько самостоятельных обособленных групп компьютерных преступников:

– лица, сочетающие черты профессионализма с изобретательностью и развлечением, озорством. Набирают опыт, пытаются совместить свои занятия с получением материальной выгоды. Путь большинства хакеров;

– лица, страдающие особого рода информационными болезнями, развившимися на почве взаимодействия с компьютерной техникой. Неадекватное поведение, компьютерный вандализм. Месть уволенных сотрудников, люди, страдающие компьютерными неврозами;

– специалисты или профессиональные компьютерные преступники. Действуют расчетливо, маскируют свои действия, стараются не оставлять следы. Корыстные цели.

Интернет-преступления (Интернет выступает средством коммуникации): распространение через Интернет порнографии, реклама запрещенных услуг, распространение сведений об изготовлении наркотиков, оружия,

2. Управление «К» МВД России.

В 1997 г. в Российской Федерации была введена уголовная ответственность за преступления в сфере компьютерной информации. В 1998 г. в МВД России создано специальное подразделение по борьбе с преступлениями в сфере информационных технологий. В настоящее время задачи по выявлению и пресечению данных преступлений решаются управлением «К» ГУСТМ МВД России и подразделениями «К» в субъектах Рос-

сийской Федерации. На настоящий момент данные специализированные подразделения работают в 81 регионе России.

Основные направления работы управления «К» МВД России:

1) Борьба с преступлениями в сфере компьютерной информации:

– выявление и пресечение фактов неправомерного доступа к компьютерной информации;

– борьба с изготовлением, распространением и использованием вредоносных программ для ЭВМ;

– противодействие мошенническим действиям с использованием возможностей электронных платежных систем;

– борьба с распространением порнографических материалов с участием несовершеннолетних через сеть Интернет;

2) Пресечение противоправных действий в информационно-телекоммуникационных сетях, включая сеть Интернет:

– выявление и пресечение преступлений, связанных с незаконным использованием ресурсов сетей сотовой и проводной связи;

– противодействие мошенническим действиям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть Интернет;

– противодействие и пресечение попыток неправомерного доступа к коммерческим каналам спутникового и кабельного телевидения;

3) Борьба с незаконным оборотом радиоэлектронных и специальных технических средств;

4) Выявление и пресечение фактов нарушения авторских и смежных прав в сфере информационных технологий;

5) Борьба с международными преступлениями в сфере информационных технологий:

– противодействие преступлениям в сфере информационных технологий, носящим международный характер;

– взаимодействие с национальными контактными пунктами зарубежных государств;

6) Международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных технологий.

Контрольные вопросы и задания

1. Назовите основные виды и различные классификации информационных преступлений.

2. Что является объектом авторского права? Что не является?

3. Перечислите виды информационных преступлений в интеллектуальной сфере, приведите примеры.

4. Назовите различные точки зрения на «пиратство».

5. Назовите виды информационных преступлений, связанных с нарушением прав личности на информационную безопасность.

6. Перечислите криминальные характеристики компьютерных преступлений.

7. Дайте характеристику личности компьютерного преступника, классификацию хакеров.

8. Что такое интернет-преступления?

9. Что понимают под компьютерным преступлением?

10. Перечислит наиболее уязвимые объекты.

11. Какие особенности выделяют в компьютерных преступлениях?

12. Дайте уголовно-правовую характеристику компьютерных преступлений.

13. Дайте понятие киберпространства, киберпреступления, кибербезопасности, кибертерроризма. Отметьте их характерные особенности, связь и отличие от компьютерных преступлений.

14. Что такое управление «К»? Чем оно занимается?

15. Перечислите органы государственной власти, регулирующие вопросы информационной безопасности.

16. Назовите тенденции развития компьютерной преступности.

Литература по теме: 1–17, 19–28, 30, 31, 33, 34.

СПИСОК ЛИТЕРАТУРЫ

1. Об информации, информационных технологиях и о защите информации : федер. закон от 27.07.2006 № 149-ФЗ // Российская газета. – 2006. – № 165.

2. О государственной тайне : закон Рос. Федерации от 21.07.1993 № 5485-1 // Рос. газ. – 1993. – № 182.

3. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена : указ Президента Рос. Федерации от 17.03.2008 № 351 // Собр. законодательства Рос. Федерации. – 2008. – № 12. – Ст. 1110.

4. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Рос. Федерации от 05.12.2016 № 646 //Собр. законодательства Рос. Федерации. – 2016. – № 50. – Ст. 7074.

5. О безопасности : федер. закон от 28.12.2010 № 390-ФЗ // Рос. газ. – 2010. – № 295.

6. О персональных данных : федер. закон от 27.07.2006 № 152-ФЗ // Рос. газ. – 2006. – № 165.

7. Об электронной подписи : федер. закон от 06.04.2011 № 63-ФЗ // Рос. газ. – 2011. – № 75.

8. О Концепции развития уголовно-исполнительной системы Российской Федерации до 2020 года : распоряжение Правительства Рос. Федерации от 14.10.2010 № 1772-р // Собр. законодательства Рос. Федерации. – 2010. – № 43. – Ст. 5544.

9. О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государствен-

ной тайны : постановление Правительства Рос. Федерации от 15.04.1995 № 333 // Рос. газ. – 1995. – № 87.

10. О лицензировании отдельных видов деятельности : федер. закон от 04.05.2011 № 99-ФЗ // Рос. газ. – 2011. – № 97.

11. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // Рос. газ. – 2001. – № 256.

12. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собр. законодательства Рос. Федерации. – 1996. – № 25. – Ст. 2954.

13. Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги «Ведение реестра операторов, осуществляющих обработку персональных данных» : приказ Минкомсвязи России от 21.12.2011 № 346 // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2012. – № 24.

14. О вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки : разъяснения Роскомнадзора // Экономика и жизнь (Бухгалтерское приложение). – 2013. – № 36.

15. О лицензировании деятельности по технической защите конфиденциальной информации : постановление Правительства Рос. Федерации от 03.02.2012 № 79 // Собр. законодательства Рос. Федерации. – 2012 – № 7. – Ст. 863.

16. Баранова, Е. К. Информационная безопасность и защита информации : учеб. пособие / Е. К. Баранова, А. В. Бабаш. − 3-е изд., перераб. и доп. − М. : РИОР: ИНФРА-М, 2017. URL: http://znanium.com/bookread2.php?book=763644 (дата обращения: 03.02.2018).

17. Бабаш, А. В. Информационная безопасность и защита информации : учеб. / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. − М. : РИОР, 2013. – 222 с. URL: http://znanium.com/bookread2.php?book=405000 (дата обращения: 03.02.2018).

18. Бабаш, А. В. Криптографические методы защиты информации / А. В. Бабаш. − 2-е изд. − М. : РИОР; ИНФРА-М, 2014. – Т. 3. − 216 с. URL: http://znanium.com/bookread2.php?book=432654 (дата обращения: 03.02.2018).

19. Безручко, В. Т. Информатика (курс лекций) : учеб. пособие / В. Т. Безручко. − М. : Форум ; ИНФРА-М, 2014. – 432 с. URL: http://znanium.com/bookread2.php?book=429099 (дата обращения: 03.02.2018).

20. Гаврилов, М. В. Информатика и информационные технологии : учеб. для прикладного бакалавриата / М. В. Гаврилов. − 4-е изд., перераб. и доп. − М. : Юрайт, 2015. – 383 с.

21. Гафнер, В. В. Информационная безопасность : учеб. пособие / В. В. Гафнер. – Ростов н/Д : Феникс, 2010. – 324 с.

22. Ефремова, М. А. К вопросу об уголовной ответственности за создание, распространение и использование вредоносных компьютерных программ // Информационное право. – 2015. – № 3. − С. 12–16.

23. Жук, А. П. Защита информации : учеб. пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. − 2-е изд. − М. : РИОР ; ИНФРА-М, 2015. – 392 с. URL: http://znanium.com/bookread2.php?book=474838 (дата обращения: 03.02.2018).

24. Зайцев, А. П. Технические средства и методы защиты информации : учеб. пособие для вузов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков. – М. : Горячая линия – Телеком, 2009. – 616 с.

25. Информационные технологии в юридической деятельности : учеб. для бакалавров / под ред. В. Д. Элькина. – М. : Проспект, 2013. – 352 с.

26. Каратунова, Н. Г. Защита информации : курс лекций : учеб. пособие / Н. Г. Каратунова. – Краснодар : КСЭИ, 2014. − 188 с. URL: http://znanium.com/bookread2.php?book=503511 (дата обращения: 03.02.2018).

27. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков. − 4-е изд., стер. − М. : Академия, 2011. – 336 с.

28. Партыка, Т. Л. Информационная безопасность : учеб. пособие / Т. Л. Партыка, И. И. Попов. – 5-е изд., перераб. и доп. − М. : Форум ; НИЦ ИНФРА-М, 2016. − 432 с. URL: http://znanium.com/bookread2.php?book=516806 (дата обращения: 03.02.2018).

29. Рогожин, В. П. Современные технические системы охраны в следственных изоляторах в период реформирования уголовно-исполнительной системы (на примере ФКУ СИЗО-3 УФСИН России по Вологодской области) // Информационно-техническое обеспечение деятельности уголовно-исполнительной системы на современном этапе : сб. материалов науч.-практ. семинара (Вологда, 27 октября 2016 г.). – Вологда : ВИПЭ ФСИН России, 2017. − С. 89–92.

30. Степанов-Егиянц, В. Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации / В. Г. Степанов-Егиянц. − М. : Статут, 2016. – 190 с.

31. Федотова, Е. Л. Информационные технологии и системы : учеб. пособие / Е. Л. Федотова. − М. : ФОРУМ, 2012. − 352 с.

32. Хорев, П. Б. Программно-аппаратная защита информации : учеб. пособие / П. Б. Хорев. – 2-е изд., испр. и доп. − М. : Форум; НИЦ ИНФРА-М, 2015. – 352 с. URL: http://znanium.com/bookread2.php?book=489084 (дата обращения: 03.02.2018).

33. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В. Ф. Шаньгин. − М. : Форум ; НИЦ ИНФРА-М, 2016. − 416 с. URL: http://znanium.com/bookread2.php?book=549989 (дата обращения: 03.02.2018).

34. Ярочкин, В. И. Информационная безопасность : учеб. для вузов. – М. : Академ. проект, 2008. – 544 с.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....3

ТЕМА 1. Основные понятия информационной безопасности....5

1.1. Актуальность защиты информации.....5

1.2. Основные понятия.....7

1.3. Нормативно-правовые акты в сфере информационной безопасности.....11

1.4. Информационные опасности и угрозы информационной безопасности.....13

1.5. Информация как объект права.....15

1.6. Государственные органы, регулирующие вопросы защиты информации.....16

ТЕМА 2. Мероприятия по обеспечению информационной безопасности.....20

2.1. Законодательные мероприятия по обеспечению информационной безопасности.....20

2.2. Административные мероприятия по обеспечению информационной безопасности.....23

2.3. Процедурные мероприятия по обеспечению информационной безопасности.....25

2.4. Программно-технические мероприятия по обеспечению информационной безопасности.....29

2.5. Криптографические методы защиты информации.....31

ТЕМА 3. Методы защиты от компьютерных вирусов.....37

3.1. Классификация вредоносных программ. Компьютерные вирусы.....37

ТЕМА 4. Компьютерная преступность.....47

СПИСОК ЛИТЕРАТУРЫ.....55

Учебное издание

Панфилова Ольга Александровна, **Крюкова** Диана Юрьевна,
Наимов Алижон Набиджанович и др.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Учебное пособие
для направления подготовки 40.03.01 – Юриспруденция,
специальности 40.05.02 – Правоохранительная деятельность,
специальности 37.05.02 – Психология служебной
деятельности очной и заочной форм обучения

Выпускается в авторской редакции

Верстка М. Ф. Ситова
Печать Е. Н. Левичева

Подписано в печать 07.05.2018. Формат 60x84 1/16. Усл. печ. л. 3,5
Тираж 22 экз. Заказ № 6904. Дата выхода в свет 23.05.2018
ФКОУ ВО «Вологодский институт права и экономики ФСИН России»
160002, г. Вологда, ул. Щетинина, д. 2