ПИТЕР

Ю. Родичев

Информационная безопасность: нормативно-правовые аспекты

ДОПУЩЕНО
УЧЕБНО-МЕТОДИЧЕСКИМ ОБЪЕДИНЕНИЕМ

Родичев Юрий Андреевич

Информационная безопасность: нормативно-правовые аспекты Учебное пособие

Рецензенты:

Ефимов А. В. к. т. н., доцент, председатель УМС по специальности 090105, заместитель начальника факультета информационной безопасности ИКСИ

Лось В. П. д. в. н., профессор, председатель УМС по специальности 090102, начальник факультета информационной безопасности ИКСИ

Заведующий редакцией	*А. Сандрыкин*
Руководитель проекта	*А. Юрченко*
Ведущий редактор	*О. Некруткина*
Художественный редактор	*С. Маликова*
Корректоры	*И. Тимофеева, Н. Филатова*
Верстка	*Т. Соловьева*

ББК 67.629.43я7
УДК 004.3:34(075)

Родичев Ю. А.

Р60 Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. — СПб.: Питер, 2008. — 272 с.: ил.

ISBN 978-5-388-00069-9

В учебном пособии рассмотрены организационные и правовые аспекты в области информационных технологий с учетом изменений законодательства Российской Федерации на конец 2007 года. Представлен обширный справочный материал по основным нормативным правовым актам Российской Федерации в области информационной безопасности и правовых вопросов, связанных с использованием информационных технологий; описана организационная структура государственных органов.

Для студентов высших учебных заведений, обучающихся по специальностям в области информационной безопасности, слушателей курсов повышения квалификации по проблемам защиты информации. Рассмотренные вопросы могут быть полезны как техническим специалистам, так и руководителям, курирующим вопросы обеспечения информационной безопасности.

Допущено Учебно-методическим объединением по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальностям 090102 «Компьютерная безопасность», 090105 «Комплексное обеспечение информационной безопасности автоматизированных систем».

ISBN 978-5-388-00069-9

ООО «Питер Пресс», 198206, Санкт-Петербург, Петергофское шоссе, д. 73, лит. А29.
Налоговая льгота — общероссийский классификатор продукции ОК 005-93, том 2; 95 3005 — литература учебная.
Подписано в печать 25.06.08. Формат 70x100/16. Усл. п. л. 21,93. Тираж 2500. Заказ
Отпечатано по технологии CtP в ОАО «Печатный двор» им. А. М. Горького.
197110, Санкт-Петербург, Чкаловский пр., д. 15.

Содержание

Введение 7

Глава 1. Информация как объект правовой защиты 11

1.1. Необходимость защиты информации 11
1.2. Основные термины и определения 17
1.3. Структура информационных ресурсов 35
1.4. Модель информационной безопасности 40
1.5. Правовая модель отношений субъектов информационного обмена 44
1.6. Особенность отношений субъектов информационного обмена в сети Интернет 50
1.7. Структура нормативных правовых актов в области информационной безопасности. 55
1.8. Судебная практика в области компьютерных преступлений 60
Контрольные вопросы к главе 1 84

Глава 2. Государственная система обеспечения информационной безопасности Российской Федерации 86

2.1. Организационная структура государственной системы обеспечения информационной безопасности. 86
2.2. Совет Безопасности Российской Федерации 91
2.3. Комиссия Совета Федерации по информационной политике 95
2.4. Федеральные органы исполнительной власти в области информатизации . . 97
2.5. Межведомственная комиссия по защите государственной тайны 98
2.6. Правительственная комиссия по федеральной связи 98
2.7. Федеральная служба безопасности Российской Федерации 100
2.8. Федеральная служба по техническому и экспортному контролю 104
2.9. Федеральная служба охраны Российской Федерации 107
2.10. Служба внешней разведки Российской Федерации 110
2.11. Федеральное агентство по информационным технологиям 111
2.12. Федеральная служба по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия 112

2.13. Федеральная служба по интеллектуальной собственности, патентам и товарным знакам . . . 113
2.14. Федеральное агентство по техническому регулированию и метрологии . . 114
2.15. Обеспечение информационной безопасности на уровне субъектов Российской Федерации . . . 117
Контрольные вопросы к главе 2 . . . 120

Глава 3. Нормативно-правовое обеспечение информационной безопасности . . . 122

3.1. Международные стандарты в области информационной безопасности . . . 122
3.2. Основные нормативно-правовые документы Российской Федерации в области защиты информации . . . 125
3.3. Конституция Российской Федерации . . . 137
3.4. Концепция национальной безопасности Российской Федерации . . . 138
3.5. Доктрина информационной безопасности Российской Федерации . . . 139
3.6. Концепция использования информационных технологий в деятельности федеральных органов исполнительной власти . . . 149
3.7. Концепция региональной информатизации . . . 154
3.8. Концепция создания системы персонального учета населения Российской Федерации . . . 156
3.9. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации . . . 158
3.10. Концепция формирования информационного общества в России . . . 160
3.11. Стратегия развития информационного общества в России . . . 162
3.12. Закон «Об информации, информационных технологиях и о защите информации» . . . 167
3.13. Кодекс Российской Федерации об административных правонарушениях . . . 174
3.14. Уголовный кодекс Российской Федерации . . . 177
3.15. Гражданский кодекс Российской Федерации . . . 189
3.16. Налоговый кодекс Российской Федерации . . . 197
3.17. Таможенный кодекс Российской Федерации . . . 198
3.18. Трудовой кодекс Российской Федерации . . . 199
3.19. Федеральный Закон «О государственной тайне» . . . 202
3.20. Федеральный Закон «О коммерческой тайне» . . . 207
3.21. Федеральный Закон «О техническом регулировании» . . . 210
3.22. Федеральный Закон «Об электронной цифровой подписи» . . . 213
3.23. Федеральный Закон «О персональных данных» . . . 216
3.24. Федеральный Закон «О связи» . . . 221
3.25. Федеральный Закон «О государственной автоматизированной системе Российской Федерации Выборы» . . . 226
3.26. Федеральный Закон «О рекламе» . . . 232
3.27. Федеральный Закон «О средствах массовой информации» . . . 233
3.28. Федеральный Закон «О безопасности» . . . 235

3.29. Федеральный Закон «О лицензировании отдельных видов деятельности» 237
3.30. Федеральный Закон «О транспортной безопасности» 240
3.31. Федеральный Закон «Об оперативно-розыскной деятельности» 243
3.32. Федеральный Закон «Об архивном деле в Российской Федерации» 246
Контрольные вопросы к главе 3 247

Приложение. Анализ тенденций развития теории и практики компьютерной безопасности 250
Особенности современного этапа развития теории компьютерной безопасности 250
Практические аспекты применения защиты информации 256

Литература 269

Интернет-ресурсы 272

Глава 1
Информация как объект правовой защиты

1.1. Необходимость защиты информации

Реалии современного информационного общества однозначно показывают, что ни одна сфера жизни цивилизованного государства не может эффективно функционировать без развитой информационной инфраструктуры, широкого применения аппаратно-программных средств и сетевых технологий обработки информации. По мере возрастания ценности информации, развития и усложнения средств ее обработки безопасность общества все в большей степени зависит от безопасности используемых информационных технологий. Многочисленные публикации последних лет показывают, что способы злоупотреблений информацией, циркулирующей в системах, совершенствуются не менее интенсивно, чем меры защиты от них. Более того, объектами компьютерных преступлений являются не только информационные ресурсы, но и сами компьютеры, программное обеспечение, телекоммуникационное оборудование и линии связи.

Проблемы обеспечения информационной безопасности неразрывно связаны с историей развития компьютерных технологий. Первоначально проблема обеспечения безопасности данных возникла при увеличении количества ЭВМ, расширении областей их применения и круга пользователей. Проблему обеспечения безопасности данных значительно обострило появление и распространение автоматизированных информационных систем.

Центральной идеей того времени являлось намерение обеспечить безопасность данных механизмами, функционирующими по строго формальным алгоритмам. Для создания таких механизмов использовались технические и в основном программные средства. Программные средства защиты включались в состав операционных систем или систем управления базами данных. Слабым звеном разработанных механизмов защиты оказался механизм защиты доступа пользователя к данным. Поэтому следующим шагом к повышению эффективности защиты стала организация дифференцированного доступа к данным.

В 60-х и 70-х годах XX века основное внимание было сосредоточено на разработке методов защиты данных, обрабатываемых на компьютере, и повышении отказоустойчивых решений в области обработки информации в автоматизированных системах, построенных в основном на базе централизованных систем и терминального доступа.

В 80-х годах с появлением персональных компьютеров возникла необходимость в разработке средств защиты от копирования и несанкционированного использования программ, появились первые криптографические стандарты защиты данных, а также были разработаны критерии оценки безопасности операционных систем, определяющие различные системы разграничения доступа. В то время появился термин *компьютерная безопасность* и были определены ее основные цели: *конфиденциальность, целостность, доступность*.

В 90-х годах с интенсивным развитием сетевых компьютерных технологий, появлением распределенных компьютерных систем и клиент-серверных технологий основные усилия специалистов были направлены на решение задач по обеспечению безопасности сетевого и межсетевого взаимодействия, разграничению доступа к распределенным ресурсам, комплексному обеспечению безопасности информации в распределенных автоматизированных системах. Средства защиты стали встроенными в большинство создаваемых промышленных продуктов. В это же время был накоплен опыт расследования и пресечения компьютерных преступлений. Несмотря на развитие теории и реализацию в практических системах технологий обеспечения компьютерной безопасности, объем ущерба, наносимого в результате компьютерных инцидентов, возрастал. По-явилось осознание того, что информационные ресурсы организации или государства являются важным объектом экономической инфраструктуры. Стало понятно, что обеспечение безопасности объектов информатизации требует привлечения различных ресурсов (людских, организационных, программно-технических) и разработки системы мер и методов защиты. Поэтому в научной литературе, а затем и в средствах массовой информации стал использоваться термин *информационная безопасность* (*information security*).

В конце XX века формируются основы теории обеспечения информационной безопасности как направления научных исследований. Теория приобретает определенную структуру, организуются специализированные институты и международные сообщества исследователей, проводятся тематические научные конференции.

В настоящее время для обеспечения защиты информации требуется не просто разработка частных механизмов защиты, а реализация системного подхода,

включающего в себя комплекс взаимосвязанных мер с использованием специальных аппаратно-программных средств, организационных мероприятий, нормативно-правовых актов. Поэтому обеспечение информационной безопасности компьютерных систем и сетей является одним из ведущих направлений развития информационных технологий.

Актуальность и важность проблемы обеспечения информационной безопасности обусловлена следующими факторами:

- высокие темпы роста парка персональных компьютеров, применяемых в самых разных сферах деятельности, и, как следствие, резкое расширение круга пользователей, имеющих непосредственный доступ к вычислительным сетям и информационным ресурсам;
- увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;
- бурное развитие аппаратно-программных средств и технологий, не соответствующих современным требованиям безопасности;
- несоответствие бурного развития средств обработки информации и проработки теории информационной безопасности, разработки международных стандартов и правовых норм, обеспечивающих необходимый уровень защиты информации;
- повсеместное распространение сетевых технологий, создание единого информационно-коммуникационного мирового пространства на базе сети Интернет, которая по своей идеологии не обеспечивает достаточного уровня информационной безопасности.

Ежегодно в мире растет количество правонарушений в информационной сфере. Соответственно, растет и размер ущерба, нанесенного злоумышленниками. По данным Управления «К» Министерства внутренних дел России, за 2005 год зарегистрировано 6910 преступлений в сфере компьютерной информации. Успешно расследуется около 49 % компьютерных преступлений. Обвинительные приговоры выносятся только в 25,5 % случаев.

В табл. 1 представлена статистика преступлений в информационной сфере за 2003–2004 годы.

Таблица 1. Статистика преступлений в информационной сфере за 2003–2004 годы

Статья Уголовного кодекса	2003 год	2004 год
146. Нарушение авторских и смежных прав	249	528
159. Мошенничество	272	371
165. Причинение имущественного ущерба путем обмана или путем злоупотребления доверием	2321	2892
171. Незаконное предпринимательство		5

Статья Уголовного кодекса	2003 год	2004 год
183. Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну	242	480
187. Изготовление или сбыт поддельных кредитных либо расчетных карт	1740	1616
242. Незаконное распространение порнографических материалов или предметов	123	335
272. Неправомерный доступ к информации	7053	8002
273. Создание, использование и распространение вредоносных программ для ЭВМ или машинных носителей с такими программами	728	1079
274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети	1	11

В 2003 году только на сайт Президента Российской Федерации было осуществлено около 100 000 компьютерных атак (то есть приблизительно по 274 хакерские атаки в день, или 11 атак в час). Всего же число зарегистрированных атак на интернет-представительства органов государственной власти Российской Федерации в 2003 году превысило 730 000 [9].

Безопасность информации в современных условиях выдвигается на первый план и становится важнейшим элементом национальной безопасности государства. Информационная безопасность рассматривается как одна из приоритетных государственных задач.

С 29 марта по 8 апреля 2005 года в Москве прошел международный форум по обеспечению информационной безопасности, на котором присутствовали ведущие эксперты более чем из 50 стран.

Участники форума отметили следующие важные положения:

1. Системы обеспечения безопасности должны рассматриваться как неотъемлемая составная часть информационно-телекоммуникационных систем.
2. Вопросы обеспечения информационной безопасности являются комплексными. Их решение требует объединения усилий и организации согласованных мероприятий со стороны органов государственной власти, силовых структур, научных учреждений, операторских компаний.
3. Для согласованного развития нормативных, юридических, технологических и организационных элементов кибербезопасности важным фактором становится международное сотрудничество.

Участники форума выделили следующие основные направления совершенствования информационно-коммуникационных систем и информационной безопасности в России:

1. Дальнейшее совершенствование законодательства в сфере обеспечения информационной безопасности, разработка единого правового понятийного аппарата, подходов к правовому регулированию в сфере информационной безопасности, правоприменительной практики.
2. Консолидация усилий операторов связи и правоохранительных органов по оперативному реагированию на действия злоумышленников. Необходимость административного определения базового уровня обеспечения безопасности операторами связи и принятия его в качестве одного из условий операторской деятельности.
3. Обеспечение дальнейшего развития теории информационной безопасности инфокоммуникационных систем.
4. Подготовка специалистов в области современных информационных технологий и технологий обеспечения информационной безопасности.

Следует отметить, что на информационную безопасность Российской Федерации значительное влияние оказали происходящие в последние годы преобразования. Возникли новые факторы, которые необходимо учитывать при оценке состояния информационной безопасности и определении ключевых проблем в этой области. Всю совокупность факторов можно разделить на политические, экономические и организационно-технические.

К основным политическим факторам следует отнести следующие:

- становление новой российской государственности на основе принципов демократии, законности, информационной открытости;
- разрушение ранее существовавшей командно-административной системы государственного управления;
- нарушение информационных связей вследствие образования независимых государств на территории бывшего СССР;
- низкая общая правовая и информационная культура в российском обществе;
- активизация деятельности международных террористических организаций и ее направленность на дестабилизацию ситуации в стране, в том числе с использованием средств «информационной войны»;
- изменение геополитической обстановки вследствие фундаментальных перемен в различных регионах мира, эскалация конфликтов вблизи государственной границы Российской Федерации.

Важнейшими экономическими факторами являются:

- переход России на рыночные отношения в экономике, появление множества отечественных и зарубежных коммерческих структур — производителей и потребителей информации, средств информатизации и защиты информации, включение информационной продукции в систему товарных отношений;
- критическое состояние отраслей промышленности, производящих средства информатизации и защиты информации, отставание телекоммуникационной инфраструктуры от аналогичных структур развитых стран;
- расширяющаяся кооперация с зарубежными странами в развитии информационной инфраструктуры России;

- появление криминальных структур, их разрастание до угрожающих масштабов, срастание с чиновничьим аппаратом и стремление оказывать влияние на все уровни руководства государством;
- нарушение хозяйственных связей вследствие распада СССР;
- ослабление научно-технического и технологического потенциала страны, сокращение исследований на стратегически важных направлениях, в том числе в сфере информатизации, и, как следствие, — усиление внешней технологической зависимости.

В «Стратегии развития информационного общества в России», утвержденной 25 июля 2007 года Советом Безопасности Российской Федерации, явно указано, что в настоящее время «практически отсутствует производство конкурентоспособной продукции микроэлектронной промышленности, телекоммуникационного оборудования и средств вычислительной техники, в результате чего зависимость развития российской информационной инфраструктуры от поставок зарубежных информационно-коммуникационных технологий значительно превышает критический уровень».

К важнейшим организационно-техническим факторам следует отнести следующие:

- недостаточная нормативно-правовая база информационных отношений, в том числе в области обеспечения информационной безопасности;
- слабое регулирование государством процессов функционирования и развития рынка средств информатизации, информационных продуктов и услуг в России;
- широкое использование не защищенных от утечки информации и несертифицированных импортных аппаратно-программных средств и технологий для хранения, обработки и передачи информации;
- обострение криминогенной обстановки, рост числа компьютерных преступлений.

Все указанные выше факторы создают целый спектр угроз национальной безопасности государства. Средством нейтрализации значительной части угроз является эффективная нормативно-правовая база, регулирующая отношения во всех сферах информационного общества, и ведущая роль государства в построении комплексной системы информационной безопасности.

Стремительное внедрение компьютерных технологий и телекоммуникаций в общественную деятельность опережает темпы развития социальных и правовых отношений в информационном обществе. Во всем мире растет количество законодательных коллизий, связанных с информационной сферой. Человечество впервые столкнулось с ситуацией, когда широкомасштабная информатизация вызвала новые отношения в обществе, а существующая законодательная база не соответствует складывающимся реалиям. Появились новые проблемы, связанные с киберпреступностью, информационной безопасностью, цифровым неравенством. Для решения этих проблем необходима в первую очередь совершенная законодательная база в области информатизации и телекоммуникаций.

1.2. Основные термины и определения

Анализ научно-технической литературы в области информационной безопасности, в том числе законодательных актов Российской Федерации, а также отечественных и зарубежных стандартов, показывает, что в области терминологии не существует пока полного единства трактовок одних и тех же понятий. Поэтому ниже приведены основные определения в области информационной безопасности, как они трактуются в Законах Российской Федерации, руководящих документах Гостехкомиссии (ныне Федеральной службы по техническому и экспортному контролю, ФСТЭК), а также государственных стандартах России (ГОСТ Р 50922—96, ГОСТ Р 51275—99 и др.).

Понятие информационной безопасности тесно связано с процессом информатизации общества. По определению ЮНЕСКО, *информатизация* — это «развитие и широкомасштабное применение методов и средств сбора, преобразования, хранения и распространения информации, обеспечивающих систематизацию имеющихся и формирование новых знаний, и их использование обществом в целях его текущего управления и дальнейшего совершенствования и развития». Информатизация общества представляет собой целенаправленный процесс изменения социальной информационной среды. Целью информатизации является повышение эффективности эксплуатации информационных ресурсов общества путем системной компьютеризации всех этапов жизненного цикла информации.

Защита информации — это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. Собственником информации могут быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

Защита информации от утечки — деятельность по предотвращению неконтролируемого распространения защищаемой информации, по защите от ее разглашения, несанкционированного доступа к защищаемой информации и от получения защищаемой информации иностранными разведками.

Защита информации от несанкционированного воздействия — деятельность по предотвращению воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от непреднамеренного воздействия — деятельность по предотвращению воздействия на защищаемую информацию ошибок пользователя, сбоя технических и программных средств информационных систем, а также

природных явлений или иных нецеленаправленных на изменение информации воздействий, связанных с функционированием технических средств, систем или с деятельностью людей, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от разглашения — деятельность по предотвращению несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

Защита информации от несанкционированного доступа — деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Заинтересованным субъектом, осуществляющим несанкционированный доступ к защищаемой информации, может выступать государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Защита информации от [*иностранной*] *разведки* — деятельность по предотвращению получения защищаемой информации [иностранной] разведкой.

Защита информации от [*иностранной*] *технической разведки* — деятельность по предотвращению получения защищаемой информации [иностранной] разведкой с помощью технических средств.

Защита информации от агентурной разведки — деятельность по предотвращению получения защищаемой информации агентурной разведкой.

Цель защиты информации — желаемый результат защиты информации.

Целью защиты информации может быть предотвращение ущерба собственнику, владельцу, пользователю информации в результате возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию.

Эффективность защиты информации — степень соответствия результатов защиты информации поставленной цели.

Показатель эффективности защиты информации — мера или характеристика для оценки эффективности защиты информации.

Нормы эффективности защиты информации — значения показателей эффективности защиты информации, установленные нормативными документами.

Организация защиты информации — содержание и порядок действий по обеспечению защиты информации.

Система защиты информации — совокупность органов и (или) исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Мероприятие по защите информации — совокупность действий по разработке и (или) практическому применению способов и средств защиты информации.

Мероприятие по контролю эффективности защиты информации — совокупность действий по разработке и (или) практическому применению методов [способов] и средств контроля эффективности защиты информации.

Техника защиты информации — средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Объект защиты — информация, носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Способ защиты информации — порядок и правила применения определенных принципов и средств защиты информации.

Категорирование защищаемой информации [*объекта защиты*] — установление градаций важности защиты защищаемой информации [объекта защиты].

Метод [*способ*] *контроля эффективности защиты информации* — порядок и правила применения определенных принципов и средств контроля эффективности защиты информации.

Контроль состояния защиты информации — проверка соответствия организации и эффективности защиты информации установленным требованиям и (или) нормам в области защиты информации.

Средство защиты информации — техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Средство контроля эффективности защиты информации — техническое, программное средство, вещество и (или) материал, предназначенные или используемые для контроля эффективности защиты информации.

Контроль организации защиты информации — проверка соответствия состояния организации, наличия и содержания документов требованиям правовых, организационно-распорядительных и нормативных документов по защите информации.

Контроль эффективности защиты информации — проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты информации.

Организационный контроль эффективности защиты информации — проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

Технический контроль эффективности защиты информации — контроль эффективности защиты информации, проводимый с использованием средств контроля.

Фактор, воздействующий на защищаемую информацию, — явление, действие или процесс, результатом которых может быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней.

Объект информатизации — совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они

установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Информационная технология — приемы, способы и методы применения технических и программных средств при выполнении функций обработки информации.

Обработка информации — совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения информации.

Под *информационной безопасностью* понимают состояние защищенности обрабатываемых, хранимых и передаваемых данных от незаконного ознакомления, преобразования и уничтожения, а также состояние защищенности информационных ресурсов от воздействий, направленных на нарушение их работоспособности.

Под *безопасностью информационной системы* понимается ее защищенность от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, от попыток несанкционированного получения информации, модификации или физического разрушения ее компонентов.

В последние годы понятие *информационная безопасность* распространилось и на такие объекты, как сложные организационно-технические системы, имеющие информационные компоненты (информационную среду), и собственно информационные системы (ИС) и телекоммуникационные сети (ТС). В ИС и ТС основными объектами защиты выступают информационные ресурсы и информационная инфраструктура, образующие их информационную среду. Другими словами, защищенность информационной системы или корпоративной сети (КС) достигается принятием мер по обеспечению как безопасности (конфиденциальности, целостности и доступности) информации, так и доступности и целостности компонентов и ресурсов системы (сети), то есть ее информационной среды как совокупности информационных ресурсов и информационной инфраструктуры.

Достоверность информации — свойство, выражаемое в строгой принадлежности информации субъекту, который является ее источником, либо тому субъекту, от которого она принята.

Субъект — это активный компонент системы, который может стать причиной образования потока информации от объекта к субъекту или изменения состояния системы.

Объект — пассивный компонент системы, хранящий, принимающий или передающий информацию. Доступ к объекту означает доступ к содержащейся в нем информации.

Доступ к информации — ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение. Различают санкционированный и несанкционированный доступ к информации.

Санкционированный доступ к информации — доступ к информации, не нарушающий установленные правила разграничения доступа. Правила разграничения доступа служат для регламентации права доступа к компонентам системы.

Несанкционированный доступ к информации — доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Целостность ресурса или компонента системы — свойство быть неизменным в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений либо разрушающих воздействий.

Применение при межсетевом взаимодействии открытых каналов передачи данных создает потенциальную угрозу проникновения злоумышленников. Если пассивный нарушитель только просматривает доступные ему сообщения, то активный наряду с прослушиванием может перехватывать, искажать и уничтожать их. Поэтому одной из важных задач обеспечения информационной безопасности при межсетевом взаимодействии является использование методов и средств, позволяющих одной стороне убедиться в подлинности другой стороны.

С допуском к информации и ресурсам системы (сети) связана группа таких понятий, как идентификация, аутентификация, авторизация. С каждым зарегистрированным субъектом системы (сети) связывают некоторую информацию, однозначно идентифицирующую субъект. Эта информация является идентификатором субъекта системы (сети). Субъект, имеющий зарегистрированный идентификатор, считается законным (легальным).

Идентификация — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов. Эта функция выполняется, в первую очередь, когда пользователь делает попытку войти в сеть. Он сообщает системе по ее запросу свой идентификатор, и система проверяет его наличие в своей базе данных.

Аутентификация — проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности. Процедура аутентификации устанавливает, является ли субъект именно тем, кем он себя объявил. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, неизвестную другим пользователям информацию о себе (например, пароль или сертификат). Идентификация и аутентификация — взаимосвязанные процессы распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После того как субъект идентифицирован и аутентифицирован, выполняется его авторизация.

При защите каналов передачи данных выполняется *взаимная аутентификация субъектов*, то есть взаимное подтверждение подлинности субъектов, связывающихся между собой по линиям связи. Процедура подтверждения подлинности выполняется обычно в начале сеанса при установлении соединения абонентов; термин *соединение* указывает на логическую связь (потенциально двустороннюю) между двумя субъектами сети. Цель данной процедуры — обеспечить уверенность в том, что соединение установлено с законным субъектом и вся информация дойдет до места назначения.

Авторизация субъекта — это процедура предоставления законному субъекту, успешно прошедшему идентификацию и аутентификацию, соответствующих полномочий и доступных ресурсов системы (сети).

Под *угрозой безопасности* для системы (сети) понимаются возможные воздействия, которые прямо или косвенно могут нанести ущерб ее безопасности.

Ущерб безопасности подразумевает нарушение состояния защищенности информации, содержащейся и обрабатывающейся в системе (сети), или самой системы или сети.

Уязвимость системы (*сети*) — это любая характеристика компьютерной системы, использование которой может привести к реализации угрозы.

Атака на компьютерную систему (*сеть*) — это действие, предпринимаемое злоумышленником с целью поиска и использования той или иной уязвимости системы. Таким образом, атака — это реализация угрозы безопасности. Противодействие угрозам безопасности — цель, которую призваны выполнить средства защиты компьютерных систем и сетей.

Политика безопасности — это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты компьютерной системы (сети) от заданного множества угроз безопасности.

Политика безопасности регламентирует эффективную работу средств защиты корпоративной сети. Она охватывает все особенности процесса обработки информации, определяя поведение системы в различных ситуациях. Политика безопасности определяет архитектуру системы защиты и реализуется посредством комплексного применения административно-организационных мер, физических мер и программно-аппаратных средств. Для конкретной организации политика безопасности должна носить индивидуальный характер и зависеть от конкретной технологии обработки информации и используемых программных и технических средств.

Политика безопасности зависит от способа управления доступом, определяющего порядок доступа к объектам системы. Различают два основных вида политики безопасности: избирательную и полномочную.

Избирательная политика безопасности основана на избирательном способе управления доступом. Он характеризуется задаваемым администратором множеством разрешенных отношений доступа (например, в виде троек: **объект, субъект, тип доступа**). Обычно для описания свойств избирательного управления доступом применяют математическую модель на основе матрицы доступа, в которой столбец соответствует объекту системы, а строка — субъекту. На пересечении столбца и строки указывается тип разрешенного доступа субъекта к объекту. Обычно выделяют такие типы, как «доступ на чтение», «доступ на запись», «доступ на исполнение» и т. п.

Полномочная политика безопасности основана на полномочном (мандатном) способе управления доступом. Она заключается в совокупности правил предоставления доступа, базирующихся на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от метки конфиденциальности информации и уровня допуска пользователя. Полномочное управление доступом подразумевает, что:

- все субъекты и объекты системы однозначно идентифицированы;
- каждому объекту системы присвоена метка конфиденциальности, определяющая ценность содержащейся в нем информации;
- каждому субъекту системы присвоен некий уровень допуска, определяющий максимальное значение метки конфиденциальности информации объектов, к которым субъект имеет доступ.

Чем важнее объект, тем выше его метка конфиденциальности. Поэтому самыми защищенными оказываются объекты с наиболее высокими значениями метки конфиденциальности.

Основным назначением полномочной политики безопасности являются регулирование доступа субъектов системы к объектам с различными уровнями конфиденциальности, предотвращение утечки информации с верхних уровней должностной иерархии на нижние, а также блокирование возможных проникновений с нижних уровней на верхние.

Активы — информация или ресурсы, подлежащие защите.

Идентификатор — представление уполномоченного пользователя (например, строка символов), однозначно его идентифицирующее. Таким представлением может быть либо полное или сокращенное имя этого пользователя, либо его псевдоним.

Уполномоченный пользователь — пользователь, которому разрешено выполнять какую-либо операцию.

Продукт — совокупность программных, программно-аппаратных и(или) аппаратных средств информационных технологий (ИТ), предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы.

Объект оценки — подлежащий оценке продукт ИТ или система с руководствами администратора и пользователя.

Информационная технология — упорядоченная совокупность аппаратных, программных, аппаратно-программных средств, систем и информационных процессов.

Носитель информации — физическое лицо или материальный объект, в том числе физическое поле, в которых информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов.

Правило доступа к информации — совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

Субъект доступа — лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Объект доступа — единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Правила разграничения доступа — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Система разграничения доступа — совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

Администратор защиты — субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Орган защиты информации — административный орган, осуществляющий организацию защиты информации.

Политика безопасности организации — одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.

Цель безопасности — изложенное намерение противостоять установленным угрозам и (или) удовлетворять установленной политике безопасности организации.

Безопасность информации — состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних или внешних угроз.

Безопасность информационной технологии — состояние информационной технологии, обеспечивающее ее применение на объектах эксплуатации, при котором отсутствует недопустимый риск, связанный с причинением ущерба здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу.

Конфиденциальность — состояние защищенности информации ограниченного доступа от неправомочного раскрытия.

Целостность — состояние защищенности информации и активов от модификации, подмены, уничтожения неправомочным способом.

Целостность информации — способность средства вычислительной техники или автоматизированной системы обеспечить неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

Доступность — состояние информационной технологии, обеспечивающее своевременный и надежный доступ к информации и (или) функциональным возможностям информационной технологии правомочным образом.

Нарушитель правил разграничения доступа — субъект доступа, осуществляющий несанкционированный доступ к информации.

Защита от несанкционированного доступа — предотвращение или существенное затруднение несанкционированного доступа.

Средство защиты от несанкционированного доступа — программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.

Комплекс средств защиты — совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

Система защиты информации от несанкционированного доступа — комплекс организационных мер и программно-технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

Защищенное средство вычислительной техники (*защищенная автоматизированная система*) — средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты.

Класс защищенности средств вычислительной техники, автоматизированной системы — определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации.

Показатель защищенности средств вычислительной техники — характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню и глубине в зависимости от класса защищенности средств вычислительной техники.

Доверие — основание для уверенности в том, что сущность отвечает своим целям безопасности.

Верификация — процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на предмет надлежащего соответствия.

Сертификация уровня защиты — процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите.

Матрица доступа — таблица, отображающая правила разграничения доступа.

Уровень полномочий субъекта доступа — совокупность прав доступа субъекта доступа.

Пароль — идентификатор субъекта доступа, который является его (субъекта) секретом.

Модель защиты — абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа.

Дискреционное управление доступом — разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту.

Мандатное управление доступом — разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться именно к информации такого уровня конфиденциальности.

Метка конфиденциальности — элемент информации, который характеризует конфиденциальность информации, содержащейся в объекте.

Средство криптографической защиты информации — средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Сертификат защиты — документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных.

В Федеральном Законе «Об информации, информатизации и защите информации» от 20 февраля 1995 года № 24-ФЗ также введен ряд терминов (Закон утратил силу с 27 июля 2006 года в связи с принятием Закона № 149-ФЗ).

Информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информатизация — организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

Документированная информация (*документ*) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Информационные процессы — процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Информационная система — организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Информационные ресурсы — отдельные документы и отдельные массивы документов, а также документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Информация о гражданах (*персональные данные*) — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Конфиденциальная информация — документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Средства обеспечения автоматизированных информационных систем и их технологий — программные, технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию.

Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами в соответствии с актами.

Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения — субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом и (или) собственником.

Пользователь (потребитель) информации — субъект, пользующийся информацией, полученной от собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.

В Федеральном Законе 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации», пришедшем на смену Закону № 24-ФЗ, сходные понятия представлены в несколько другой трактовке, а введены определения других терминов.

Информация — сведения (сообщения, данные) независимо от формы их представления.

Информационные технологии — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть — технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Обладатель информации — лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Доступ к информации — возможность получения информации и ее использования.

Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Предоставление информации — действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Распространение информации — действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Электронное сообщение — информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Документированная информация — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Оператор информационной системы — гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

В Законе «О государственной тайне» от 21 июля 1993 года № 5485-I (с учетом последних изменений от 22 августа 2004 года № 122-ФЗ) также приведен ряд терминов.

Государственная тайна — защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Носители сведений, составляющих государственную тайну, — материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Система защиты государственной тайны — совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

Допуск к государственной тайне — процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций — на проведение работ с использованием таких сведений.

Доступ к сведениям, составляющим государственную тайну, — санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

Гриф секретности — реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.

Средства защиты информации — технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Перечень сведений, составляющих государственную тайну, — совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

В Законе «О коммерческой тайне» от 29 июля 2004 года № 98-ФЗ (с изменениями и дополнениями от 02.02.06 № 19-ФЗ, от 18.12.06 № 231-ФЗ) используются следующие основные понятия.

Коммерческая тайна — конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Информация, составляющая коммерческую тайну, — научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства (ноу-хау)), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны.

В соответствии с Федеральным Законом от 18 декабря 2006 года № 231-ФЗ с 1 января 2008 года указанные два термина изложены в следующей редакции:

«*Коммерческая тайна* — режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Информация, составляющая коммерческую тайну (*секрет производства*), — сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны».

Режим коммерческой тайны — правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности.

Обладатель информации, составляющей коммерческую тайну, — лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны.

Доступ к информации, составляющей коммерческую тайну, — ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Передача информации, составляющей коммерческую тайну, — передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Контрагент — сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию.

Предоставление информации, составляющей коммерческую тайну, — передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Разглашение информации, составляющей коммерческую тайну, — действие или бездействие, в результате которого информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

В Законе «О правовой охране программ для электронных вычислительных машин и баз данных» от 23 сентября 1992 года № 3523-1 приведен также ряд терминов. Следует отметить, что данный закон утрачивает силу с 01.01.08 г. в связи с принятием Закона от 18.12.06 № 231-ФЗ «О введении в действие части четвертой Гражданского Кодекса Российской Федерации».

Программа для ЭВМ — это объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин (ЭВМ) и других компьютерных устройств с целью получения определенного результата. Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения.

База данных — это объективная форма представления и организации совокупности данных (например статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Адаптация программы для ЭВМ или базы данных — это внесение изменений, осуществляемых исключительно в целях обеспечения функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя.

Модификация (*переработка*) *программы для ЭВМ или базы данных* — это любые их изменения, не являющиеся адаптацией.

Декомпилирование программы для ЭВМ — это технический прием, включающий преобразование объектного кода в исходный текст в целях изучения структуры и кодирования программы для ЭВМ.

Воспроизведение программы для ЭВМ или базы данных — это изготовление одного или более экземпляров программы для ЭВМ или базы данных в любой материальной форме, а также их запись в память ЭВМ.

Распространение программы для ЭВМ или базы данных — это предоставление доступа к воспроизведенной в любой материальной форме программе для ЭВМ или базе данных, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей.

Выпуск в свет (опубликование) программы для ЭВМ или базы данных — это предоставление экземпляров программы для ЭВМ или базы данных с согласия автора неопределенному кругу лиц (в том числе путем записи в память ЭВМ и выпуска печатного текста) при условии, что количество таких экземпляров должно удовлетворять потребностям этого круга лиц, принимая во внимание характер указанных произведений.

Использование программы для ЭВМ или базы данных — это выпуск в свет, воспроизведение, распространение и иные действия по их введению в хозяйственный оборот (в том числе в модифицированной форме). Не признается использованием программы для ЭВМ или базы данных передача средствами массовой информации сообщений о выпущенной в свет программе для ЭВМ или базе данных.