Вопрос 1. Понятие информации, задачи информационной безопасности.

Понятие информации.

В части 4 статьи 29 Конституции РФ устанавливается право каждого свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Согласно статье 3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на ряде принципов, в число которых входит принцип свободы поиска, получения, передачи, производства и распространения информации любым законным способом.

Согласно ч. 1 ст. 2 Закона «Об информации, информационных технологиях и защите информации» информация - это сведения (сообщения, данные) независимо от формы их представления.

В ст. 5 Закона «Об информации, информационных технологиях и защите информации» закреплено, что информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами. Основания отнесения сведений к категории ограниченного доступа закреплены в ряде нормативных актов:

- Статья 5 Закона РФ от 21.07.1993 № 5485-1 «О государственной тайне»;
- Указ Президента РФ от 30.11.1995 № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне»;
- Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Статья 1465 Гражданского кодекса РФ (часть четвертая);
- Статья 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и многие другие.

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) 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.

4. Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

В ГК РФ информация включена в число объектов гражданских прав наряду с такими традиционными объектами, как вещи, деньги, ценные бумаги, работы и услуги, результаты интеллектуального труда. Важной характеристикой информации как объекта гражданских прав является оборотоспособность ее отдельных видов, т.е. возможность отчуждаться в возмездном порядке.

Информацию как объект информационного права можно охарактеризовать следующем образом:

- информация должна существовать в момент правоотношения;

- информация предназначена для физических или юридических лиц и имеет определенное предназначение;
- информация возможна для передачи и для размножения;
- информация имеет определенную форму и единицу измерения;
- информация научно обоснована и доказана, в связи с чем может быть предметом судебного спора;
- информация юридически закреплена;
- информация имеет определенный источник и, соответственно, может иметь получателя.

Информационно-телекоммуникационная сеть определяется как технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники (п. 4 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»). Понятие «информационно-телекоммуникационная сеть» выделяется в связи с необходимостью обеспечения правового регулирования отношений по поиску, получению, передаче, производству и распространению информации, т.е. сведений (сообщений, данных) независимо от формы их представления.

Понятие «информационно-телекоммуникационная сеть» шире понятия «сеть связи» и применяется для обозначения среды, в которой находится и через которую передается информация. В то же время более узкое понятие «сеть связи» отражает технологическое состояние средств и линий связи, непосредственно предназначенных для электросвязи.

Часть 1 ст. 15 Федерального закона от 27 июля 2006 г. № 149-ФЗ устанавливает условия использования информационно-телекоммуникационных сетей на территории Российской Федерации. Такое использование должно осуществляться с соблюдением требований законодательства Российской Федерации в области связи. Иными словами, информационно-телекоммуникационные сети, используемые для оказания услуг связи, должны соответствовать требованиям к созданию и эксплуатации сетей связи.

В телекоммуникационной системе можно выделить три варианта воздействия на информацию:

Задержка в передаче информации. Телекоммуникационная система может обеспечить абсолютно достоверную передачу информации, но время ее передачи может оказаться столь длительным, что она потеряет свою актуальность для потребителя. В предельном случае задержка информации может привести к её полной потере.

Искажение или нарушение целостности информации. При этом часть информации может быть утеряна, подменена другой информацией, либо к исходной информации может быть добавлена информация, искажающая исходную (например, вирусы). В предельном случае искажение информации может привести к полной её потере.

Несанкционированный доступ к информации, т.е. нарушение конфиденциальности информации.

Задержка в передаче информации возникает, в основном, в сетях электросвязи. Усложнение применяемых технологий сетей электросвязи, процессов управления сетями и их технической эксплуатации объективно ведет к возникновению сбоев в функционировании этих сетей и, как следствие, к задержкам передачи информации.

Отметим, что примерно четверть нарушений приходится на повреждение физических линий и 2% возникли в результате злого умысла. Методы защиты здесь применяются на 3-х нижних уровнях эталонной модели открытых систем, а также на «О» уровне модели. Основными из них являются:

- устранение возможных преднамеренных или непреднамеренных ошибок при проектировании сетей электросвязи, а также при настройке оборудования;
- защита от внедрения вредоносных программ и компонентов, реализующих не

декларированные функции, на этапах создания и модернизации сетей электросвязи, а также в процессе технической эксплуатации;

- контроль за соблюдением правил технической эксплуатации сетей;
- повышение живучести сетей электросвязи;
- резервирование линий связи, каналов и трактов;
- создание системы оперативного управления сетями;
- создание препятствий для возможного вмешательства в процесс функционирования сетей электросвязи;
- обеспечение мониторинга состояния сетей электросвязи, своевременного обнаружения попыток деструктивного воздействия на сети электросвязи, локализации места воздействия и оперативной ликвидации последствий воздействия.

Понятие и задачи информационной безопасности.

Информационная безопасность - один из главных приоритетов современного бизнеса, поскольку нарушения в этой сфере приводят к гибельным последствиям для бизнеса любой компании. Применение высоких информационных технологий XXI в., с одной стороны, дает значительные преимущества в деятельности предприятий и организаций, а с другой - потенциально создает предпосылки для утечки, хищения, утраты, искажения, подделки, уничтожения, копирования и блокирования информации и, как следствие, нанесение экономического, социального или других видов ущерба, т. е. проблема информационных рисков и нахождения путей снижения ущерба становится с каждым годом все острее.

Кузнецова О.Б. Оценка информационных рисков в обеспечении экономической безопасности предприятия // Труды ИСА РАН 2007. Т. 31. С. 78-98.

В Доктрине информационной безопасности РФ защита информационных ресурсов названа в качестве четвертого элемента информационной безопасности РФ. Под информационной безопасностью РФ понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов человека, организации и страны. Информационная безопасность РФ является неотъемлемым элементом безопасности РФ в целом.

Под защитой информации подразумевается:

- деятельность, направленная на предотвращение утечки конфиденциальной информации, несанкционированных и непреднамеренных воздействий на конфиденциальную информацию;
- комплекс административных, организационных и технических мероприятий по ограничению доступа к информации и ее носителям в целях обеспечения ее сохранности и недоступности третьим сторонам, предусмотренный законодательством РФ.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Понятие «безопасность информации» распадается на две составляющие:

- безопасность содержательной части (смысла) информации - отсутствие в ней побуждения человека к негативным действиям, умышленно заложенных механизмов негативного воздействия на человеческую психику или негативного воздействия на иной блок информации (например, информация, содержащаяся в программе для ЭВМ, именуемой компьютерным вирусом);
- защищенность информации от внешних воздействий (попыток неправомерного копирования, распространения, модификации (изменения смысла) либо уничтожения.

Цель информационной безопасности - выявить возможные угрозы безопасности информации, определить их последствия и возможный ущерб, обеспечить необходимые меры и средства защиты, и оценить их эффективность.

Статьей 16 (ч. 1) Закона «Об информации, информационных технологиях и о защите информации» защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

Следует отметить, что в целом проблема информационной безопасности включает, наряду с задачами обеспечения защищенности информации и информационных систем, еще два аспекта:

- защиту от воздействия вредоносной информации,
- обеспечение принятия обоснованных решений с максимальным использованием доступной информации.

Обеспечение информационной безопасности призвано решать следующие основные задачи:

- выявление, оценка и предотвращение угроз информационным системам и информационным ресурсам;
- защита прав юридических и физических лиц на интеллектуальную собственность, а также сбор, накопление и использование информации;
- защита государственной, служебной, коммерческой, личной и других видов тайны.

Поскольку анализ всей информационной инфраструктуры далеко не всегда оправдан с экономической точки зрения, целесообразно сосредоточиться на наиболее важных, одновременно выявляя не только сами угрозы, вероятность из осуществления, размер потенциального ущерба, но и их источники.

Режим защиты информации устанавливается в отношении трех групп сведений:

1) сведения, относящиеся к государственной тайне: режим устанавливается уполномоченным государственным органом на основании закона РФ от 21 июля 1993 г. № 5485-1 «О государственной тайне»;

2) конфиденциальная информация. Режим защиты информации устанавливается собственником информационных ресурсов или уполномоченным им лицом на основании закона об информации;

3) персональные данные. Режим защиты информации устанавливается специальным Федеральным законом № 152-ФЗ от 27 июля 2006 года «О персональных данных».

Контроль за соблюдением требований к защите информации, а также обеспечение органами мер защиты информационной системы, образующих информацию с ограниченным доступом в негосударственных структурах, возложены на государственные органы. Собственник информации также имеет право осуществить аналогичный контроль. Законом устанавливается только перечни сведений, которые не могут быть отнесены к конкретному виду информации с ограниченным доступом. Исключение - перечень сведений, составляющих государственную тайну.

Защита информации осуществляется от:

- утечки (неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками);
- несанкционированного воздействия (воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к ее искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации);
- непреднамеренного воздействия (воздействия на защищаемую информацию ошибок

ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации);

- разглашения (несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации);

- несанкционированного доступа (получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации);

- разведки (получения защищаемой информации технической, агентурной разведкой).

Организационно-техническими методами обеспечения информационной безопасности РФ являются совершенствование системы обеспечения информационной безопасности РФ, сертификация и стандартизация средств и способов защиты информации, лицензирование деятельности в области защиты государственной тайны, предупреждение и пресечение правонарушений в информационной сфере, создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и др. Так, Постановление Правительства РФ от 03.03.2012 N 171 «О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации», осуществляемой юридическими лицами и индивидуальными предпринимателями. Постановление Правительства РФ от 03.02.2012 N 79 "О лицензировании деятельности по технической защите конфиденциальной информации" определяет порядок лицензирования деятельности по технической защите конфиденциальной информации (не содержащей сведения, составляющие государственную тайну, но защищаемой в соответствии с законодательством РФ), осуществляемой юридическими лицами и индивидуальными предпринимателями. Лицензирование деятельности по разработке и производству средств защиты конфиденциальной информации осуществляет Федеральная служба по техническому и экспортному контролю, а в части разработки и производства средств защиты конфиденциальной информации, устанавливаемых на объектах Администрации Президента РФ, Совета Безопасности РФ, Федерального Собрания РФ, Правительства РФ, Конституционного Суда РФ и Верховного Суда РФ, - Федеральная служба безопасности РФ. Лицензирование деятельности по технической защите конфиденциальной информации осуществляет Федеральная служба по техническому и экспортному контролю.

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 являются средствами защиты информации и подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации. Данные отношения по сертификации регулируются Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Предмет регулирования Закона о техническом регулировании составляют отношения, возникающие при:

- разработке, принятии, применении и исполнении обязательных требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации;

- разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;

- оценке соответствия.

Система защиты государственной тайны трактуется в законе как - 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.

К органам защиты государственной тайны относятся: межведомственная комиссия по защите государственной тайны; органы федеральной исполнительной власти (Федеральная служба безопасности РФ, Министерство обороны РФ), Служба внешней разведки РФ, Федеральная служба по техническому и экспортному контролю России (бывшая Государственная техническая комиссия при Президенте РФ), и их органы на местах; органы государственной власти, предприятия, учреждения и организации и их структурные подразделения по защите государственной тайны.

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

1) обеспечения безопасности (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в том числе в функционирующих в составе критически важных объектов РФ информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям;

2) противодействия иностранным техническим разведкам на территории РФ;

3) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения, и блокирования доступа к ней на территории РФ;

4) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;

5) осуществления экспортного контроля.

Концепция безопасности и выработанная политика безопасности должны отвечать требованиям специализированных нормативных документов и стандартов, в частности: международных - ISO 17799, 9001, 15408 (CCIMB-99-031), BSI; российских - распоряжения и руководящие документы Федеральной службы по техническому и экспортному контролю и ФАПСИ, ГОСТ 34.003, Р 51624, Р 51583 и др.

Требования к уровню защиты информации всегда определялись через показатель ее ценности или важности для собственника. Чем выше степень ограничения доступа к информации заявляется ее собственником, тем более дорогостоящей она становится и, как показывает практика, тем меньший круг субъектов выступает носителем такой информации. В то же время защищаемая информация должна приносить пользу ее собственнику. При этом нужно не забывать и о возмещении уже потраченных средств на ее защиту.

Контроль и надзор за выполнением требований обеспечения безопасности персональных данных при их обработке в автоматизированных информационных системах, установленных Правительством РФ, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (ФСБ России), и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации - Федеральной службой по техническому и экспортному контролю (ФСТЭК России).

Так, в соответствии с ч. 1 ст. 27 Закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе», Правительство РФ устанавливает требования к защите информации о

средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством РФ. Операторы по переводу денежных средств, банковские платежные агенты (субагенты), операторы платежных систем, операторы услуг платежной инфраструктуры обязаны обеспечивать защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством РФ. Правительство РФ устанавливает требования к защите указанной информации.

Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

Ведущее значение в деле обеспечения информационной безопасности принадлежит техническим средствам.

В России классификация систем защиты определяется руководящим документом Гостехкомиссии «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». В соответствии с этим документом устанавливается семь классов защищенности средств вычислительной техники от несанкционированного доступа к информации. Самый низкий класс - седьмой, самый высокий - первый.

Перечень показателей по классам защищенности средств вычислительной техники (СВТ) приведен в таблице 7.2.1.

Таблица 7.2.1. Перечень показателей по классам защищенности СВТ

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	-	-	+	=	=	=
Очистка памяти	-	+	+	+	=	=
Изоляция модулей	-	-	+	=	+	=
Маркировка документов	-	-	+	=	=	=
Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	=	=
Сопоставление пользователя с устройством	-	-	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	-	+	+	+	+	+
Регистрация	-	+	+	+	=	=
Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
Надежное восстановление	-	-	-	+	=	=
Целостность КСЗ	-	+	+	+	=	=
Контроль модификации	-	-	-	-	+	=
Контроль дистрибуции	-	-	-	-	+	=
Гарантии архитектуры	-	-	-	-	-	+
Тестирование	+	+	+	+	+	=
Руководство для пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Тестовая документация	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

Обозначения:

- «-» - нет требований к данному классу;
- «+» - новые или дополнительные требования,
- «=« - требования совпадают с требованиями к СВТ предыдущего класса.

Например, к показателям защищенности шестого класса применяются следующие требования:

1. Дискреционный принцип контроля доступа. Комплекс средств защиты (КСЗ) должен контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.).

Для каждой пары (субъект - объект) в СВТ должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту).

КСЗ должен содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа.

Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).

Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.

Права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности и т.д.).

2. Идентификация и аутентификация. КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ. КСЗ должен подвергать проверке подлинность идентификации - осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации. КСЗ должен препятствовать доступу к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась.

3. Тестирование. В СВТ шестого класса должны тестироваться:

- реализация дискреционных ПРД (перехват явных и скрытых запросов, правильное распознавание санкционированных и несанкционированных запросов на доступ, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);
- успешное осуществление идентификации и аутентификации, а также их средств защиты.

4. Руководство для пользователя. Документация на СВТ должна включать в себя краткое руководство для пользователя с описанием способов использования КСЗ и его интерфейса с пользователем.

5. Руководство по КСЗ. Данный документ адресован администратору защиты и должен содержать:

- описание контролируемых функций;
- руководство по генерации КСЗ;
- описание старта СВТ и процедур проверки правильности старта.

6. Тестовая документация.

Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с п. 3.) и результатов тестирования.

7. Конструкторская (проектная) документация. Должна содержать общее описание принципов работы СВТ, общую схему КСЗ, описание интерфейсов КСЗ с пользователем и интерфейсов частей КСЗ между собой, описание механизмов идентификации и аутентификации.

Дополнительно требуется, чтобы высокоуровневые спецификации КСЗ были отображены последовательно в спецификации одного или нескольких нижних уровней, вплоть до реализации высокоуровневой спецификации КСЗ на языке программирования высокого уровня. При этом методами верификации должно осуществляться доказательство соответствия каждого такого отображения спецификациям высокого (верхнего для данного отображения) уровня. Этот процесс может включать в себя как одно отображение (высокоуровневая спецификация - язык программирования), так и последовательность отображений в промежуточные спецификации с понижением уровня, вплоть до языка программирования. В результате верификации соответствия каждого уровня предыдущему должно достигаться соответствие реализации высокоуровневой спецификации КСЗ модели защиты, изображенной на чертеже (рис. 7.2.1).

Рис. 7.2.1. Схема модели защиты

Оценка класса защищенности СВТ проводится в соответствии с Положением о сертификации средств и систем вычислительной техники и связи по требованиям защиты информации, Временным положением по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники и другими документами.