Лекция 1 Основные понятия теории информационной безопасности

1. Предметная область теории информационной безопасности. Основные термины и определения правовых понятий в области информационных отношений и защиты информации.
2. Понятия предметной области защиты информации. Основные принципы построения систем защиты.
3. Концепция комплексной защиты информации. Средства реализации комплексной защиты информации.
4. Понятие об информации как объекте защиты. Уровни представления информации.
5. Основные свойства защищаемой информации. Виды и формы представления информации. Информационные ресурсы.
6. Структура и шкала ценности информации. Классификация информационных ресурсов. Правовой режим информационных ресурсов.

1 Предметная область теории информационной безопасности. Основные термины и определения правовых понятий в области информационных отношений и защиты информации

Предметная область теории информационной безопасности

Теория информационной безопасности наука сравнительно молодая. Свое развитие она получила в связи с бурным развитием информационных технологий, радиоэлектроники и связи и необходимостью сохранения информационных ресурсов. Как и любая другая наука, информационная безопасность имеет свой понятийный аппарат, который способен наиболее точно охарактеризовать все аспекты защиты информации. Многие понятия по своему содержанию соответствуют зарубежным аналогам. В то же время некоторые термины не являются устоявшимися и не всегда точно и полно характеризуют какой- либо процесс, свойство или предмет.

Предметной областью информационной безопасности являются:

· информация и ее свойства;
· угрозы безопасности информации и ее собственникам;
· политика безопасности и модели безопасности;
· способы, методы и средства защиты информации;
· классификация систем защиты;
· требования к защищенности информационных систем;
· методология оценки защищенности информационных систем и проектирования защиты.
· конкретные системы защиты информации, применяемые в различных органах управления, учреждениях и на предприятиях различных форм собственности.

Основные термины и определения правовых понятий в области информационных отношений и защиты информации

Основные термины и определения правовых понятий в изучаемой области установлены в Федеральном законе «Об информации, информационных технологиях ио защите информации». В нем сформулировано понятие информации и информационных технологий, определены субъекты информационных отношений и защиты.

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. В соответствии с ГОСТ 33707–2016 (ISO/IEC 2382:2015) Информационные технологии. Словарь, информационная система — это система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы (человеческие, технические, финансовые и т.д.), которые обеспечивают и распространяют информацию.

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.

Также к правовым понятиям следует отнести понятие прав доступа к защищаемой информации. Ограничения доступа устанавливаются к сведениям, составляющим государственную тайну и иные виды тайны. В качестве собственников информации рассматриваются государство, организации и граждане (юридические и физические лица).

Доступ к информации — возможность получения информации и ее использования.

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.

2 Понятия предметной области защиты информации. Основные принципы построения систем защиты

Понятия предметной области «Защита информации»

Условно вся предметная область может быть разделена на две подгруппы. Первая — это основные понятия в области защиты информации. Вторая подгруппа — это понятия, связанные с организацией защиты информации.

Основные понятия в области защиты информации (термины и определения)

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

Защита информации — принятие правовых, организационных и технических мер, направленных:

1) на 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.

Защита информации от утечки — деятельность, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками.

Защита информации от несанкционированного воздействия — деятельность, направленная на предотвращение 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.

Защита информации от непреднамеренного воздействия — деятельность, направленная на предотвращение 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.

Защита информации от разглашения — деятельность, направленная на предотвращение несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации.

Защита информации от несанкционированного доступа — деятельность, направленная на предотвращение 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 быть: государство; юридическое лицо; группа физических лиц, в том числе общественная организация; отдельное физическое лицо.

Защита информации от разведки — деятельность, направленная на предотвращение получения защищаемой информации разведкой.

Примечание. Получение защищаемой информации может быть осуществлено как иностранной, так и отечественной разведкой.

Защита информации от технической разведки — деятельность, направленная на предотвращение получения защищаемой информации разведкой с помощью технических средств.

Защита информации от агентурной разведки — деятельность, направленная на предотвращение получения защищаемой информации агентурной разведкой.

Цель защиты информации — заранее намеченный 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.

Замысел защиты информации — основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

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.

Понятия, связанные с организацией защиты информации

Организация защиты информации — содержание и порядок действий, направленных на обеспечение защиты информации.

Система защиты информации — совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации.

Мероприятие по защите информации — совокупность действий, направленных на разработку и (или) практическое применение способов и средств защиты информации.

Мероприятие по контролю эффективности защиты информации — совокупность действий, направленных на разработку и (или) практическое применение 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 информации — информация или носитель информации, или информационный процесс, которые необходимо защищать 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 градации важности защищаемой информации (объекта защиты).

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

Все рассмотренные понятия являются общеметодологическими и применимы в целом для теории информационной безопасности. Основные понятия, связанные с защитой информации в информационных системах, определены также в Руководящем документе Гостехкомиссии «Термины и определения в области защиты от НСД к информации». Установленные термины обязательны для применения во всех видах документации. Для каждого понятия установлен один термин. Применение его синонимов не допускается.

Основные принципы построения систем защиты

Для защиты информации в информационных системах могут быть сформулированы следующие:

1. *Законность и обоснованность защиты.*

Принцип законности и обоснованности предусматривает то, что защищаемая информация по своему правовому статусу относится к информации, которой требуется защита в соответствии с законодательством.

2. *Системность*.

Системный подход к защите информационной системы предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов:

· при всех видах информационной деятельности и информационного проявления;

· во всех структурных элементах;

· при всех режимах функционирования;

· на всех этапах жизненного цикла;

· с учетом взаимодействия объекта защиты с внешней средой.

При обеспечении безопасности информационной системы необходимо учитывать все слабые, наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и пути несанкционированного доступа к информации. Система защиты должна строиться не только с учетом всех известных каналов проникновения, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

3. *Комплексность*.

Комплексное использование предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

4. *Непрерывность защиты*.

Защита информации — это непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационной системы, начиная с самых ранних стадий проектирования. Разработка системы защиты должна вестись параллельно с разработкой самой защищаемой системы.

5. *Разумная достаточность.*

Создать абсолютно непреодолимую систему защиты принципиально невозможно: при достаточных времени и средствах можно преодолеть любую защиту. Следовательно, возможно достижение лишь некоторого приемлемого уровня безопасности. Высокоэффективная система защиты требует больших ресурсов (финансовых, материальных, вычислительных, временных) и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень зашиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

6. *Гибкость*.

Внешние условия и требования с течением времени меняются. Принятые меры и установленные средства защиты могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровня защищенности средства защиты должны обладать определенной гибкостью.

7. *Открытость алгоритмов и механизмов защиты.*

Суть принципа открытости механизмов и алгоритмов защиты состоит в том, что знание алгоритмов работы системы защиты не должно давать возможности ее преодоления даже разработчику защиты. Однако это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна, необходимо обеспечивать защиту от угрозы раскрытия параметров системы.

8. *Простота применения средств защиты.*

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения малопонятных ему операций.

2. Понятия предметной области защиты информации. Основные принципы построения систем защиты.

3 Концепция комплексной защиты информации. Средства реализации комплексной защиты информации

Концепция комплексной защиты информации

Эффективное обеспечение защиты информации возможно только на основе комплексного использования всех известных методов и подходов к решению данной проблемы.

К концепции комплексной защиты предъявляется ряд требований:

1. Разработка и доведение до уровня регулярного использования всех необходимых механизмов гарантированного обеспечения требуемого уровня защищенности информации;
2. Существование механизмов практической реализации требуемого уровня защищенности;
3. Наличие средств рациональной реализации всех необходимых мероприятий по защите информации на базе достигнутого уровня развития науки и техники;
4. Разработка способов оптимальной организации и обеспечения проведения всех мероприятий по защите в процессе обработки информации.

В целях построения концепции, удовлетворяющей всей совокупности требований, в последнее время активно разрабатывается теория защиты информации, включающая понятия задачи защиты, средств защиты, системы защиты.

Функция защиты — совокупность однородных в функциональном отношении мероприятий, регулярно осуществляемых в информационной системе различными средствами и методами в целях создания, поддержания и обеспечения условий, объективно необходимых для надежной защиты информации.

Полное множество функций защиты:

· предупреждение возникновения условий, благоприятствующих появлению дестабилизирующих факторов;

· предупреждение непосредственного проявления дестабилизирующих факторов; · обнаружение проявившихся дестабилизирующих факторов;

· предупреждение воздействия на защищаемую информацию проявившихся дестабилизирующих факторов;

· обнаружение воздействия дестабилизирующих факторов;

· локализация воздействия дестабилизирующих факторов;

· ликвидация последствий локализованного воздействия дестабилизирующих факторов.

Полнота множества функций защиты имеет значение для оптимизации систем защиты информации. Осуществление функций защиты связано с расходованием ресурсов. Обозначим количество ресурсов (например, стоимость), расходуемых на осуществление i-го мероприятия по защите, как Ci . Вероятность успешного осуществления этого мероприятия Pi зависит от затраченных ресурсов

$$Pi = Pi (Ci).$$

Если требуется обеспечить определенный уровень (вероятность) защищенности информации Рз0, то следует выбирать такие мероприятия, которые обеспечат уровень защищенности не менее заданного: Рз > Рз0. С учетом этого задачу защиты информации можно сформулировать как оптимизационную: определить перечень мероприятий, при которых заданный уровень защиты обеспечивается при минимальных затратах. Возможна и другая постановка: достичь максимально возможного уровня защищенности информации при определенном уровне затрат на защиту. Осуществление функций защиты достигается решением задач защиты.

Задачи защиты информации

Все задачи, необходимые для осуществления функций обеспечения защиты, могут быть объединены в классы:

· введение избыточности элементов системы;

· резервирование элементов системы;

· регулирование доступа к элементам системы;

· регулирование использования элементов системы; · маскировка информации; · контроль элементов системы;

· регистрация сведений;

· уничтожение информации;

сигнализация;

· реагирование.

До сих пор не решена проблема оценки эффективности реализации функций защиты путем решения определенной задачи защиты.

Средства реализации комплексной защиты информации

Рассмотрим основные средства, используемые для создания механизмов защиты. Все средства защиты делятся на формальные (выполняющие защитные функции строго по заранее предусмотренной процедуре без непосредственного участия человека) и неформальные (определяются целенаправленной деятельностью человека либо регламентируют эту деятельность).

Технические средства реализуются в виде электрических, электромеханических и электронных устройств. Вся совокупность технических средств делится на аппаратные и физические.

Под аппаратными техническими средствами принято понимать устройства, встраиваемые непосредственно в телекоммуникационную аппаратуру, или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу. Из наиболее известных аппаратных средств можно отметить схемы контроля информации по четности, схемы защиты полей памяти — по ключу и т.п. Физические средства реализуются в виде автономных устройств и систем. Это могут быть, например замки на дверях помещений, где размещена аппаратура, решетки на окнах, электронно-механическое оборудование охранной сигнализации.

Программные средства представляют собой программное обеспечение, специально предназначенное для выполнения функций защиты информации.

Указанные выше средства и составляли основу механизмов защиты на первой фазе развития технологии обеспечения безопасности связи в каналах телекоммуникаций. При этом считалось, что основными средствами защиты являются программные. Первоначально программные механизмы защиты включались, как правило, в состав ОС, управляющих ЭВМ, или систем управления базами данных. Практика показала, что надежность подобных механизмов защиты является явно недостаточной. Особенно слабым звеном оказалась защита по паролю. Поэтому в дальнейшем механизмы защиты становились все более сложными, с привлечением других средств обеспечения безопасности.

Организационные средства защиты представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы системы на всех этапах их жизненного цикла (строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и эксплуатация).

Законодательные средства защиты определяются законодательными актами страны, которыми регламентируются правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

Морально-этические средства защиты реализуются в виде всевозможных норм, которые сложились традиционно или складываются по мере распространения вычислительной техники и средств связи в данной стране или обществе. Эти нормы большей частью не являются обязательными, как законодательные меры, однако несоблюдение их ведет обычно к потере авторитета и престижа человека.

Итак, информационная безопасность является важной составляющей национальной безопасности России. Политика государства в этой сфере деятельности направлена в первую очередь на организацию защиты государственной тайны и развитие правовых основ защиты информации. Правовая защита информации выступает как один из наиболее важных способов и методов защиты информации.

Выводы

· Знание основ теории информационной безопасности будет способствовать компетентному решению практических вопросов защиты информации, явится основой для профессиональной деятельности специалиста по информационной безопасности;

· Проблема защиты информации формулировалась по-разному в разные исторические эпохи и связана политикой, экономикой, технологиями.

· Проблема защиты информации в автоматизированных (информационных) системах была сформулирована в середине 70-х годов XX века и с тех пор претерпела существенные изменения, связанные с уровнем развития систем;

· Перспективным является путь комплексного обеспечения информационной безопасности, сочетающий формальный и неформальный подход к решению проблемы;

· Однозначное определение базовых понятий в области информационной безопасности необходимо в интересах как производителей, так и потребителей информационных систем, а также для полного и непротиворечивого описания процесса защиты информации.

4..

5. Основные свойства защищаемой информации. Виды и формы представления информации. Информационные ресурсы.

6. Структура и шкала ценности информации. Классификация информационных ресурсов. Правовой режим информационных ресурсов.

4 Понятие об информации как объекте защиты. Уровни представления информации

Понятие об информации как объекте защиты

В общем случае информация — это знания в широком значении этого слова. Не только образовательные или научные знания, а сведения и данные, которые присутствуют в любом объекте и необходимы для функционирования любых информационных систем (живых существ или созданных человеком).

Информация как объект познания имеет ряд особенностей:

· нематериальна по своей природе, отображается в виде символов на носителях;

· после записи на носитель информация приобретает определённые параметры и может быть измерена в объеме;

· информация, записанная на материальный носитель, может храниться, обрабатываться, передаваться по различным каналам связи;

· перемещаясь по линиям связи, информация создает физические поля, которые отражают ее содержание.

При обработке, хранении, передаче информация циркулирует в информационной системе. Простейшая информационная система состоит из источника информации, канала связи и получателя информации (рис. 1.1). Из этого следует, что нельзя поставить знак равенства между защитой информации и защитой информационной системы.

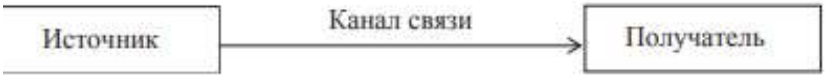

Рис. 1.1 - Простейшая информационная система

Уровни представления информации

Можно выделить несколько уровней представления информации:

· уровень носителей; · уровень средств взаимодействия с носителем;

· логический уровень;

· синтаксический уровень;

· семантический уровень.

Охарактеризуем каждый из них.

1) *Уровень носителей информации*

По своей природе информация не материальна и в чистом виде человеку не доступна. Для того чтобы человек воспринял информацию, должен быть материальный носитель: другой человек, вещество (вещественный носитель), энергия (энергетический носитель). Информация, являясь предметом защиты, требует защищенности тех объектов, в которых она присутствует в той или иной материальной форме.

Все носители имеют две категории информации:

· признаковая информация: информация носителя «о себе», о видовых признаках: форма, размер, структура, химические и физические свойства, энергетические параметры;

· семантическая информация: то, что не зависит от вида носителя, продукт абстрактного мышления на языке символов.

Роль **человека** по отношению к информации многообразна: человек может быть не только носителем информации, но и генератором новой информации, источником информации, владельцем, пользователем. По отношению к вопросам защиты человек может выступать и как нарушитель, и как защитник.

Как носитель человек нуждается не только в физической защите. Человека следует защищать от информации избыточной, бесполезной, от дезинформации, от разрушающей информации (информационно-психологическое оружие). Многие механизмы защиты работают у человека на биологическом уровне: при поступлении ненужной или избыточной информации снижается внимание, ухудшается запоминание, замедляется реакция. Так как часто на основе имеющейся информации принимаются решения, то важным является достаточная информированность человека. В этом случае опасна как неинформированность (возможно принятие неверных решений на основе неполной информации), так и сверхинформированность (сложности в определении приоритетов и основных факторов).

Вещественные носители разнообразны по своим качествам, среди них есть такие, которые используются уже тысячелетиями, есть созданные в последние годы. К наиболее распространённым в настоящее время относятся: бумага, электронные носители информации. Особенности вещественных носителей:

· придают информации свойство статичности (постоянства во времени), в связи с этим обычно используются для хранения информации;

· информация фиксируется прочно, её трудно уничтожить, не повредив носителя; · со временем вещественные носители разрушаются и стареют, при этом информация гибнет вместе с носителем;

· запись информации связана с изменением физических и химических свойств носителей.

Вещественные носители, как и любой материальный объект, следует защищать от повреждения, преждевременного износа, хищения, утери. Необходима также защита при копировании информации. Копирование — процесс переноса информации

на аналогичный или иной носитель без изменения количества и качества. Копирование легко обеспечивается при помощи современных технологий. Для документов на бумажном носителе копирование осуществляется при помощи ксерокса, сканера, фотоаппарата. Для электронных носителей операция копирования предусмотрена стандартным программным обеспечением. В результате копирования одна и та же информация размещается в разных точках пространства на разных носителях, следовательно, нужна охрана всех носителей во всех местах дислокации.

Энергетические носители — это электромагнитное и акустическое поля. Особенности энергетических носителей: · используются в основном для передачи информации;

· не стареют;

· бесконтрольно распространяются в пространстве;

· способны к взаимному преобразованию;

· запись информации связана с изменением параметров поля (различные виды модуляции).

Основные способы защиты информации на энергетическом носителе: обеспечение помехоустойчивости при выборе кодирования (модуляции), обеспечение требуемой энергетики сигнала, защита от утечки, в том числе через побочные электромагнитные излучения и наводки (ПЭМИН), защита от перехвата в основном канале.

2) *Уровень средств взаимодействия с носителем*

Непосредственное взаимодействие с носителем не всегда возможно и часто осуществляется через сложные технические устройства. Для защиты на этом уровне нужно следить за исправностью устройств считывания информации, за отсутствием технических средств несанкционированного доступа к информации (так называемых «закладок»), задачей которых является перехват или перенаправление потока считываемой информации.

3) *Логический уровень*

На логическом уровне в информационной системе информация может быть представлена в виде логических дисков, каталогов, файлов, …, секторов, кластеров. В современных операционных системах уровни отдельных байтов, кластеров, секторов не видны, поэтому часто забываются. Следует помнить, что удаление информации на высоком логическом уровне (например, на уровне файла) не приводит к удалению информации на нижних уровнях, откуда она может быть считана.

4) *Синтаксический уровень*

Синтаксический уровень представления информации связан с кодированием. Информация записывается и передаётся при помощи символов. Символ — это некоторый знак, которому

придаётся определённый смысл. Линейный набор символов образует алфавит. В процессе кодирования один алфавит может быть преобразован в другой.

В зависимости от целей различаются следующие виды кодирования:

· с целью устранения избыточности — архивирование, линейное кодирование;

· с целью устранения ошибок — помехоустойчивое кодирование;

· с целью недоступности информации — криптографическое кодирование.

5) *Семантический уровень*

Семантический уровень связан со смыслом передаваемой информации. Одинаковые лексические конструкции могут иметь различный смысл в разном контексте. Использование профессионализмов, многозначных слов и слов, значение которых изменилось с течением времени, может исказить смысл информации.

5 Понятие об информации как объекте защиты. Уровни представления информации

Основные свойства защищаемой информации

Информация как объект познания и объект защиты обладает множеством свойств. Перечислим важнейшие из них.

Ценность. Как предмет собственности информация имеет определенную ценность. Именно потому, что информация имеет ценность, ее необходимо защищать.

Секретность (*конфиденциальность*) информации — субъективно определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации. Эта характеристика обеспечивается способностью системы сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней. Объективные предпосылки подобного ограничения доступности информации для одних субъектов заключены в необходимости защиты законных интересов других субъектов информационных отношений.

Целостность информации — свойство информации существовать в неискаженном виде. Обычно интересует обеспечение более широкого свойства — достоверности информации, которое складывается из адекватности (полноты и точности) отображения состояния предметной области и непосредственно целостности информации, то есть ее неискаженности. Вопросы обеспечения адекватности отображения выходят за рамки проблемы обеспечения информационной безопасности.

Доступность информации — свойство системы, в которой циркулирует информация, обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

Концентрация. Суммарное количество информации может оказаться секретным, сводные данные обычно секретнее, чем одиночные.

Рассеяние. Ценная информация может быть разделена на части и перемешана с менее ценной с целью маскировки самого факта наличия информации. Примеры использования этого свойства — компьютерная стеганография.

Сжатие. Возможно сжатие без потери информации, например архивирование. Для уменьшения объема информации или увеличения пропускной способности канала передачи информации применяется сжатие с частичной потерей (например, сжатие в графических форматах типа jpg). Используется также необратимое сжатие (например, алгоритм электронно-цифровой подписи (ЭЦП), одностороннее ХЭШ-преобразование).

Прагматические свойства:

· важность;

· полнота (степень уменьшения априорной неопределенности);

· достоверность; · своевременность;

· целесообразность;

· соотносимость с фактами, явлениями.

Для удовлетворения законных прав и интересов владельцев информации необходимо прежде всего постоянно поддерживать секретность, целостность и доступность информации. При нарушении хотя бы одного из этих свойств ценность информации снижается либо теряется вообще:

· если ценность теряется при ее раскрытии, то говорят, что имеется опасность нарушения секретности информации;

· если ценность информации теряется при изменении или уничтожении информации, то говорят, что имеется опасность для целостности информации;

· если ценность информации теряется при ее неоперативном использовании, то говорят, что имеется опасность нарушения доступности информации. Ценность информации изменяется во времени.

К изменению ценности информации приводят распространение информации и ее использование. Характер изменения ценности во времени зависит от вида информации. Для большинства видов можно представить общую схему жизненного цикла информации (рис. 1.2).

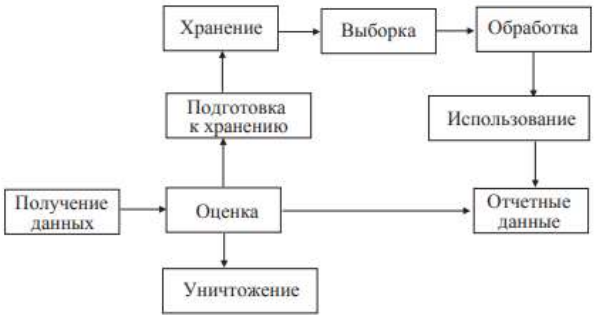

Рис. 1.2 - Жизненный цикл информации

Ценность большинства видов информации, циркулирующей в информационной системе, со временем уменьшается — информация стареет. Старение информации Си в первом приближении можно аппроксимировать выражением вида

$$C_0(t) = C_0 \exp(-2{,}3t/t_{ж.ц}),$$

где C_0 — ценность информации в момент ее возникновения (создания); t — время от момента возникновения информации до момента ее использования; $t_{ж.ц}$ — продолжительность жизненного цикла информации (от момента возникновения до момента устаревания). В соответствии с этим выражением за время жизненного цикла ценность информации уменьшается в 10 раз.

Виды и формы представления информации. Информационные ресурсы.

В соответствии с законодательством вводится понятие информационных ресурсов. *Информационные ресурсы* предприятия, организации, учреждения, компании и других государственных и негосударственных структур включают в себя отдельные документы и отдельные массивы документов (дела), документы и комплексы документов в информационных системах (библиотеках, архивах, фондах, банках данных электронно-информационных систем) на любых носителях, в том числе обеспечивающих работу вычислительной и организационной техники. Информационные ресурсы являются объектами отношений физических и юридических лиц между собой и с государством. В совокупности они составляют информационные ресурсы России и защищаются наравне с другими видами ресурсов. Обязательным условием для включения в информационные ресурсы является документирование информации.

Любая документированная информация имеет следующие реквизиты:

· наименование документа;

· гриф секретности или конфиденциальности (если таковые имеются);

· регистрационный номер;

· дату создания и регистрации;

· автора и (или) исполнителя;

· срок действия грифа секретности или конфиденциальности, если таковые имеются;

· атрибуты учреждения.

Кроме того, в реквизитах могут указываться адреса рассылки (пользователей). Документированная информация может быть представлена в виде справок, решений, приказов, распоряжений, заданий, отчетов, ведомостей, инструкций, комментариев, писем и записок, телеграмм, чеков, статей и др. Все эти виды документов могут отличаться по форме. Обычно в служебном и секретном делопроизводстве эти формы стандартизованы. Вразличных ведомствах они могут быть неодинаковыми. В информационных системах документированная информация представлена в виде файлов, папок, массивов, баз данных, программ.

Законодательством Российской Федерации или соглашением сторон могут быть установлены требования к документированию информации.

В федеральных органах исполнительной власти документирование информации осуществляется в порядке, устанавливаемом Правительством Российской Федерации. Правила делопроизводства и документооборота, установленные иными государственными органами, органами местного самоуправления в пределах их компетенции, должны соответствовать требованиям, установленным Правительством Российской Федерации в части делопроизводства и документооборота для федеральных органов исполнительной власти.

Электронное сообщение, подписанное электронной цифровой подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

6 Структура и шкала ценности информации. Классификация информационных ресурсов. Правовой режим информационных ресурсов

Структура и шкала ценности информации. Классификация информационных ресурсов

Ценность информации может быть стоимостной категорией и характеризовать конкретный размер прибыли при ее использовании или размер убытков при ее утрате. Степень ценности информации и необходимая надежность ее защиты находятся в прямой зависимости.

Информация часто становится ценной ввиду ее правового значения для фирмы или развития бизнеса, например учредительные документы, программы и планы, договоры с партнерами и посредниками и т.д. Ценность может проявляться в ее перспективном научном, техническом или технологическом значении.

Следует учитывать, что документ может быть не только управленческим (деловым), имеющим в большинстве случаев текстовую, табличную или анкетную форму. Большие объемы наиболее ценных документов представлены в изобразительной форме: конструкторские документы, картографические, научно-технические, документы на фотографических, магнитных и иных носителях.

В соответствии с этим обычно выделяются два вида интеллектуально ценной информации:

· техническая, технологическая: методы изготовления продукции, программное обеспечение, производственные показатели, химические формулы, рецептуры, результаты испытаний опытных образцов, данные контроля качества и т.п.;

· деловая: стоимостные показатели, результаты исследования рынка, списки клиентов, экономические прогнозы и т.п.

По принадлежности к виду собственности информационные ресурсы могут быть государственными или негосударственными, находиться в собственности граждан, органов государственной власти, исполнительных органов, органов местного самоуправления, государственных учреждений, организаций и предприятий, общественных организаций.

Защите подлежит любая официальная документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Таким образом, наличие права собственности на информацию как результат интеллектуальной деятельности определяет правовую целесообразность защиты информационных ресурсов. Существует также экономическая целесообразность защиты информационных ресурсов, основанная на потребительских свойствах информации, прежде всего на ее стоимости.

В соответствии с интересами обеспечения национальной безопасности и степенью ценности для государства, а также правовыми, экономическими и другими интересами информационные ресурсы могут быть открытыми, то есть общедоступными (используемыми в работе без специального разрешения, публикуемыми в средствах массовой информации, оглашаемыми в выступлениях и т.п.), и ограниченного доступа и использования, то есть содержащими сведения, составляющие тот или иной вид тайны и подлежащие защите, охране, наблюдению (рис. 1.3).

Рис. 1.3 - Классификация информационных ресурсов

Запрещается относить к информации ограниченного доступа:

· законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, исполнительных органов, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

· документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

· документы, содержащие информацию о деятельности органов государственной власти, исполнительных органов и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии и потребностях населения, за исключением сведений, относящихся к государственной тайне;

· документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, исполнительных органов, органов местного самоуправления, организаций, общественных объединений, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Ценная информация охраняется нормами права (патентного, авторского, смежных прав и др.), товарным знаком или защищается включением ее в категорию информации, составляющей определенный вид тайны.

Для информационных ресурсов ограниченного доступа вид тайны является определяющим основанием их классификации. Тайна — это нечто неизвестное, неведомое, неразгаданное, еще не познанное, нечто скрываемое от других, известное не всем. Выделяются две глобальные предметные сферы тайны:

· тайны природы, то есть объективные тайны: тайна Вселенной, тайны рождения и смерти и множество других тайн;

· тайны людей, то есть субъективные тайны: тайны личности, тайны производства, тайны искусства и т.п.

В понятие *тайны* включается не только документированная информация, а также базы данных, продукция, изделия, технологии, излучения, физические поля. Многообразие форм и субъектов собственности закрепляет за собственником право считать ту или иную ценную информацию тайной.

Состав видов тайны в современном российском законодательстве постоянно расширяется. В настоящее время основными видами тайны являются: государственная, служебная, профессиональная, коммерческая и личная. Каждый из этих видов имеет несколько подвидов.

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

Другие виды тайны являются негосударственными. Отнесение информации к информации ограниченного доступа осуществляется в порядке, установленном законодательством страны.

Служебная тайна содержит информацию ограниченного распространения, к которой относятся несекретные сведения, касающиеся деятельности организации, ограничения на распространение которых диктуются служебной необходимостью. К служебной информации относятся сведения, не подлежащие опубликованию в средствах массовой информации, использованию в отную тайну, тайну государственных банков, производственную тайну (до ее патентования) в некоммерческой сфере и др.

Профессиональная тайна — инструмент защиты персональных данных о гражданах и личной тайны граждан. Имеется в виду, что эти сведения переданы их собственником или находятся в распоряжении той или иной организации и необходимы ей для выполнения профессиональной деятельности: врачебная тайна, тайна страхования, тайна завещания, тайна голосования, тайна предприятий связи, тайна налоговых органов и др. Профессиональная тайна может быть также тайной мастерства, тайной профессионального умения, например тайна творчества, тайна рационализатора и др.

Коммерческая тайна — сведения, имеющие действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, когда к ним нет свободного

доступа на законном основании и обладатель этих сведений принимает меры к охране их конфиденциальности. Учитывая, что коммерческая тайна как таковая отражает в значительной степени торговые секреты, иногда в рамках этого же определения используется термин «предпринимательская тайна». В зарубежной практике обычно используются термины, разделяющие предпринимательскую тайну на две части — производственную и коммерческую. Коммерческая тайна рассматривается как обязательное условие добросовестной конкуренции предприятий на рынке товаров или услуг. В России коммерческая тайна охватывает негосударственную сферу или коммерческие направления производственной деятельности и включает производственную, финансовую, научную и другие подвиды тайны. В рамках этого вида тайны выделяется коммерческая тайна банка (банковская тайна), тайна фирмы. К коммерческой тайне относятся секреты предприятий, с которыми сотрудничает фирма, секреты клиентов, покупателей, поставщиков и т.п.

Личная тайна граждан определена в Конституции Российской Федерации, где указано, что каждый имеет право крытых документах, оглашению на конференциях, переговорах и выставках, например черновики и варианты готовящихся документов, служебные инструкции, тактика ведения переговоров, персональные данные работников и т.д. Разновидностями служебной тайны можно назвать судебно-следственна неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Не допускается сбор, хранение, использование и распространение информации о частной жизни граждан без их согласия. Семейную тайну можно считать разновидностью личной тайны. Она представляет собой тайну нескольких лиц, связанных родством, например: имущественное положение, взгляды и убеждения, отношения в семье, тайна факта усыновления.

Процесс выявления и регламентации реального состава информации ограниченного доступа важен для эффективной работы системы защиты информации.

Например, информация ограниченного доступа формируется в следующих направлениях деятельности предприятия:

· прогнозирование и планирование деятельности (расширение или свертывание производства, программы развития, планы инвестиций);

· управление предприятием (сведения о подготовке и принятии решений, применяемые методы управления);

· финансовая деятельность (баланс, сведения о состоянии счетов и уровне доходности, информация о получении кредитов);

· торговая деятельность (информация о рыночной стратегии, об эффективности коммерческой деятельности);

· производственная деятельность (производственные мощности, тип используемого оборудования, запасы сырья и готовой продукции);

· переговоры и совещания по направлениям деятельности предприятия (информация о подготовке и результатах проведения переговоров);

· формирование ценовой политики на продукцию и услуги (информация о структуре цен, методах расчета, размерах скидок);

· формирование состава партнеров, поставщиков и потребителей;

· изучение состава конкурентов;

· участие в торгах и аукционах; · научная и исследовательская деятельность по созданию новой техники и технологий;

· использование новых технологий;

· подбор и управление персоналом;

· организация безопасности предприятия.

При определении состава информации ограниченного доступа следует выделять ключевые элементы информации, являющиеся основными носителями секрета. Информация может быть отнесена к коммерческой тайне при соблюдении следующих условий:

· информация не должна отражать негативные стороны деятельности предприятия; · информация не должна быть общедоступной или общеизвестной;

· возникновение или получение информации должно быть законным и связано с расходованием материального, финансового или интеллектуального потенциала предприятия;

· персонал должен знать о ценности такой информации и обучен правилам работы с ней;

· должны быть выполнены реальные действия по защите этой информации (наличие системы защиты, нормативно-методического и технического обеспечения этой системы).

В соответствии с постановлением Правительства «О перечне сведений, которые не могут составлять коммерческую тайну» от 5 декабря 1991 г. к конфиденциальной информации нельзя относить:

· учредительные документы, уставы предпринимательских структур;

· документы, дающие право заниматься предпринимательской деятельностью (регистрационные удостоверения, лицензии, патенты);

· сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РФ;

· документы о платежеспособности;

· сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

· документы об уплате налогов и обязательных платежей; · сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства РФ и размерах причиненного при этом ущерба;

· сведения об участии должностных лиц предприятия в кооперативных, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

Состав ценной конфиденциальной информации, подлежащей защите, определяется ее собственником или владельцем. Предприятия однотипного профиля могут руководствоваться примерным составом защищаемых сведений.

При определении ценности информации следует определить возможный ущерб от реализации угроз безопасности. Определяя ущерб, важно оценить его в стоимостном выражении: стоимость продукции, которая не будет произведена или реализована, затраты на научные исследования и т.п.

В практической деятельности состав защищаемых сведений фиксируется в специальном Перечне конфиденциальных сведений. Определяется также перечень документов, не содержащих конфиденциальные сведения, но представляющих ценность для предприятия и подлежащих охране (например, устав, контракт и т.п.). (Перечень ценных и конфиденциальных документов).

Таким образом, ценная информация включается в документы, входящие в состав информационных ресурсов ограниченного доступа к ним персонала. В соответствии с тем, к какому виду тайны относятся ресурсы, документы делятся на секретные и несекретные. Обязательным признаком секретного документа является наличие в нем сведений, составляющих государственную тайну. Несекретные документы, включающие сведения, относимые к негосударственной тайне или содержащие персональные данные, называются конфиденциальными. Обязательным признаком конфиденциального документа является наличие в нем информации, подлежащей защите.

К документам ограниченного доступа относятся:

· в государственных структурах: документы, проекты документов и сопутствующие материалы, относимые к служебной информации ограниченного распространения (документы «для служебного пользования»), содержащие сведения, отнесенные к служебной тайне, имеющие рабочий характер и не подлежащие опубликованию в открытой печати;

· в предпринимательских структурах— документы, содержащие сведения, которые собственник или владелец в соответствии с законодательством имеет право отнести к коммерческой (предпринимательской) тайне, тайне мастерства;

· независимо от принадлежности — документы и базы данных, фиксирующие любые персональные (личные) данные о гражданах, а также содержащие профессиональную тайну, технические и технологические новшества (до их патентования), тайну предприятий связи, сферы обслуживания и т.п.

Называть документы ограниченного доступа секретными или ставить на них гриф секретности не допускается.

Ограничение доступа к документам имеет значительный разброс по срокам ограничения свободного доступа к ним персонала (от нескольких часов до значительного числа лет). Следует учитывать, что основная масса конфиденциальных документов после окончания их исполнения или работы с ними теряет свою ценность и конфиденциальность. Например, переписка до заключения контракта может иметь гриф конфиденциальности, но после его подписания этот гриф снимается.

Оставшиеся конфиденциальными исполненные документы, сохраняющие ценность для деятельности фирмы, формируются в дела в соответствии с номенклатурой дел.

Период ограничения доступа к документам может быть кратковременным или долговременным в зависимости от ценности информации, содержащейся в документах. Период ограничения доступа определяется по указанному выше перечню конфиденциальных сведений и зависит от специфики деятельности фирмы. Например, производственные, научно-исследовательские фирмы обладают более ценными документами, чем торговые, посреднические и др.

Документы долговременного периода ограничения доступа (программы и планы развития бизнеса, технологическая документация ноу-хау, изобретения и др.) имеют усложненный вариант обработки и хранения, обеспечивающий безопасность информации и ее носителя.

Документы кратковременного периода ограничения доступа, имеющие оперативное значение для деятельности фирмы, обрабатываются и хранятся по упрощенной схеме и могут не выделяться из технологической системы обработки открытых документов при наличии в этой системе минимальных защитных, контрольных и аналитических элементов.

Режим ограничения доступа к персональным данным снимается в случаях обезличивания этих данных или по истечении 75 лет срока их хранения, если иное не определено законом.

Правовой режим информационных ресурсов

Правовой режим информационных ресурсов определяется нормами, устанавливающими:

· порядок документирования информации; · право собственности на отдельные документы и их массивы;

· категорию информации по уровню доступа к ней;

· порядок правовой защиты информации. Государство имеет право выкупа документированной информации у физических и юридических лиц в случае отнесения этой информации к государственной тайне.

Собственник информационных ресурсов, содержащих сведения, отнесенные к государственной тайне, вправе распоряжаться этой собственностью только с разрешения соответствующих органов государственной власти.

Государственные информационные ресурсы РФ являются открытыми и общедоступными, исключение составляет документированная информация, отнесенная законом к категориям ограниченного доступа.

Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне и конфиденциальную.

Режим защиты информации устанавливается:

· в отношении сведений, отнесенных к государственной тайне, — уполномоченными органами на основании закона РФ «О государственной тайне» от 21.09.93 № 182-ФЗ;

· в отношении конфиденциальной информации — собственником информационных ресурсов или уполномоченным лицом на основании Федерального закона «Об информации, информационных технологиях и защите информации от 27.07.2006 № 149-ФЗ;

· в отношении персональных данных — Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.

Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, подлежащих защите, разрабатывающие и применяющие информационные технологии для формирования и использования информационных ресурсов с ограниченным доступом, руководствуются в своей деятельности Законодательством РФ.

Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно-технических средств защиты, а также обеспечение организационных мер защиты информационных ресурсов, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляется органами государственной власти.

Собственник информационных ресурсов имеет право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.

Риск, связанный с использованием несертифицированных систем и средств, лежит на собственнике (владельце) этих систем и средств. Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.

Персональные данные относятся к категории конфиденциальной информации, однако перечни этих данных должны быть закреплены на уровне федерального закона. В связи с этим деятельность

негосударственных организаций и частных лиц, связанная с обработкой и представлением пользователям персональных данных, подлежит обязательному лицензированию. Все информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации.

Автоматизированные системы органов государственной власти, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации

Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности.

Закон предусматривает *защиту прав на доступ к информации*. Отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке.

Во всех случаях лица, получившие недостоверную информацию, имеют право на возмещение понесенного ими ущерба.

Руководители, другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответственность в соответствии с уголовным, гражданским законодательством и законодательством об административных правонарушениях.

Выводы

· Характеристика понятия «информация», выделение основных свойств информации являются ключевыми моментами при определении того, что же подлежит защите.

· Выделены три основных свойства информации (конфиденциальность, целостность и доступность), защита которых обеспечивает сохранение ценности информации.

· Информация является объектом права собственности и информационные отношения регулируются соответствующими законодательными и нормативными актами.

· Информационные ресурсы классифицируются в зависимости от вида отражаемой ими тайны.