Содержание:

Введение

Информация является результатом отображения и обработки в человеческом сознании многообразия окружающего мира, представляет собой сведения об окружающих человека предметах, явлениях природы, деятельности других людей.

Одной из наиболее актуальных проблем современного информационного общества является защита этой информации, поскольку все виды данных, обрабатываемых и накапливаемых с помощью компьютерных технологий, в последнее время стали определять направление деятельности и многие другие аспекты жизнедеятельности современного социального организма.

С помощью незаконного владения информацией можно осуществлять различные противоправные действия, например, производить незаконный оборот финансовых ресурсов, получать доступ к секретной коммерческой информации и т.д.

Следует отметить, что конфиденциальная информация представляет большой интерес для конкурирующих фирм. Именно она становится причиной посягательств злоумышленников.

Многие проблемы информационной безопасности связаны с недооценкой важности такой угрозы, как конфиденциальность информации. В результате для предприятия это может привести к банкротству. Даже единичный случай халатности персонала предприятия может принести ему многомиллионные убытки, потерю репутации компании и доверия клиентов[1].

Под защитой информации в настоящее время понимается область науки и техники, которая включает совокупность средств, методов и способов человеческой деятельности, направленных на обеспечение защиты всех видов информации в организациях и предприятиях различных направлений деятельности и различных форм собственности.

Информация, которая подлежит защите, может быть представлена на любых носителях, может храниться, обрабатываться и передаваться различными способами и средствами.

Целями защиты информации являются:

- предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям;
- предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы;
- обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствие с законодательством;
- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

Информационная безопасность - это состояние защищенности информации среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств.

Угрозы информации выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности.

Цель данной работы состоит в определении видов угроз информационной безопасности и их состава.

Глава 1. Классификация угроз информационной безопасности

1.1 Виды угроз информационной безопасности

Для того чтобы обеспечить эффективную защиту информации, необходимо в первую очередь рассмотреть и проанализировать все факторы, представляющие

угрозу информационной безопасности.

Под угрозой информационной безопасности обычно понимают потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьим-либо интересам. Такие угрозы, воздействуя на информацию через компоненты КС, могут привести к уничтожению, искажению, копированию, несанкционированному распространению информации, к ограничению или блокированию доступа к ней. В настоящее время известен достаточно обширный перечень угроз, который классифицируют по нескольким признакам[2].

Таблица 1.

Классификация угроз ИБ по направлению угроз

№	Направление угрозы	Проявление	Варианты причин возникновения
1	Конфиденци-альность	Информация становится известной тому, кто не располагает полномочиями доступа к ней. «Утечка» информации.	Имеет место, когда получен доступ к некоторой информации ограниченного доступа, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Могут возникать вследствие «человеческого фактора» (например, случайное делегировании тому или иному пользователю привилегий другого пользователя), сбоев работе программных и аппаратных средств
2	Целостность	Появляется вероятность модификации той или иной информации, хранящейся в информационной системе	Может быть вызвано различными факторами – от умышленных действий персонала до выхода из строя оборудования

3	Доступность	Создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес-целей	Как правило вызван человеческим фактором, редко из-за технических проблем.

Все указанные в таблице 1 угрозы далее можно классифицировать по различным характеристикам (см. Таблица 2).

Таблица 2.

Классификация угроз по различным характеристикам

№	Характеристика	Виды угроз	Пояснение
1	Расположение источника угроз	Внутренние	Внутри системы
		Внешние	Вне системы
1	Степени воздействия на ИС	Пассивные	Структура и содержание системы не изменяются
		Активные	Структура и содержание системы подвергается изменениям
1	Размер наносимого ущерба	Общие	Причинение значительного ущерба системе в целом
		Локальные	Причинение вреда отдельным частям объекта безопасности

Частные	Причинение вреда отдельным свойствам элементов объекта безопасности		
13	Природа возникновения	Естественные (объективные)	Вызываются воздействием на ИС объективных физических процессов или стихийных природных явлений, не зависящих от воли человека
		Искусственные (субъективные), в том числе	Вызываются воздействием на информационную сферу человека
		Непреднамеренные (случайные)	Ошибки программного обеспечения, персонала, сбои в работе систем, отказы вычислительной и коммуникационной техники
		Преднамеренные (умышленные) угрозы —	Неправомерный доступ к информации, разработка специального программного обеспечения, используемого для осуществления неправомерного доступа, разработка и распространение вирусных программ и т.д.

Угроза информационной безопасности – совокупность условий и факторов, создающих опасность нарушения информационной безопасности.

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации (таблица 3): информационные, программные, физические, радиоэлектронные и организационно-правовые.

Таблица 3.

Классификация угроз по способам воздействия на объекты информационной безопасности

№	Способ воздействия	Виды угроз
1	Информационные	• несанкционированный доступ к информационным ресурсам; • незаконное копирование данных в информационных системах; • хищение информации из библиотек, архивов, банков и баз данных; • нарушение технологии обработки информации; • противозаконный сбор и использование информации.
2	Программные	• использование ошибок и уязвимостей в программном обеспечении; • компьютерные вирусы и вредоносные программы; • установка программных закладок.
3	Физические	• уничтожение или разрушение средств обработки информации и связи; • хищение носителей информации; • хищение программных или аппаратных ключей и средств криптографической защиты данных.
4	Радиоэлектронные	• внедрение электронных устройств перехвата информации в технические средства и помещения; • перехват, расшифровка, подмена и уничтожение информации в каналах связи.

5	Организационно-правовые	• закупки несовершенных или устаревших информационных технологий и средств информатизации; • нарушение требований законодательства и задержка в принятии необходимых нормативно-правовых решений в информационной сфере.

Основные проблемы информационной безопасности связаны прежде всего с умышленными угрозами, так как они обусловлены действиями людей и являются главной причиной преступлений и правонарушений[3].

В настоящее время практически вся информация, в том числе и имеющая коммерческую или иную ценность хранится, используется и передается в цифровом формате в некоторой компьютерной системе (КС). Все множество потенциальных угроз безопасности информации в КС может быть разделено на 2 основных класса (рис.1).

Рисунок 1. Угрозы информационной безопасности КС

Более подробно составы этих классов угроз рассмотрим в следующих параграфах.

1.2 Случайные угрозы

Угрозы, которые не связаны с преднамеренными действиями злоумышленников и реализуются в случайные моменты времени, называют случайными или непреднамеренными. Механизм реализации случайных угроз в целом достаточно хорошо изучен, накоплен значительный опыт противодействия этим угрозам.

Стихийные бедствия и аварии чреваты наиболее разрушительными последствиями для КС, так как последние подвергаются физическому разрушению, информация утрачивается или доступ к ней становится невозможен. Сбои и отказы сложных систем неизбежны. В результате сбоев и отказов нарушается работоспособность технических средств, уничтожаются и искажаются данные и программы, нарушается алгоритм работы устройств.

Ошибки при разработке КС, алгоритмические и программные ошибки приводят к последствиям, аналогичным последствиям сбоев и отказов технических средств.

Кроме того, такие ошибки могут быть использованы злоумышленниками для воздействия на ресурсы КС.

Согласно данным Национального Института Стандартов и Технологий США (NIST) 65% случаев нарушения безопасности информации происходит в результате ошибок пользователей и обслуживающего персонала[4]. Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками приводит к уничтожению, нарушению целостности и конфиденциальности информации, а также компрометации механизмов защиты.

1.3 Преднамеренные угрозы

Преднамеренные угрозы связаны с целенаправленными действиями нарушителя. Данный класс угроз изучен недостаточно, очень динамичен и постоянно пополняется новыми угрозами.

Методы и средства шпионажа и диверсий чаще всего используются для получения сведений о системе защиты с целью проникновения в КС, а также для хищения и уничтожения информационных ресурсов. К таким методам относят подслушивание, визуальное наблюдение, хищение документов и машинных носителей информации, хищение программ и атрибутов системы защиты, сбор и анализ отходов машинных носителей информации, поджоги.

Несанкционированный доступ к информации (НСД) происходит обычно с использованием штатных аппаратных и программных средств КС, в результате чего нарушаются установленные правила разграничения доступа пользователей или процессов к информационным ресурсам. Под правилами разграничения доступа понимается совокупность положений, регламентирующих права доступа лиц или процессов к единицам информации.

Основные методы получения несанкционированного доступа:

1) Перехват паролей.

Перехват паролей осуществляется с помощью специально разработанных программ. Когда пользователь пытается войти в систему / войти в систему, программа имитирует ввод имени пользователя и пароля и отправляет их злоумышленнику, а затем отображает окно ошибки на экране пользователя и прекращает свою работу. Таким образом, пользователь, считающий, что он

допустил ошибку при вводе, снова вводит информацию и получает доступ к системе, а злоумышленник, получивший информацию о учетных данных пользователя, может использовать ее в своих целях.

1. «Маскарад.»

Под атакой типа «маскарад» понимается способ нападения на информационную систему (ИС), при котором злоумышленник имитирует все штатные информационные и служебные процедуры ИС, создавая у реальных пользователей и административных служб иллюзию корректного функционирования сети[5].

Простейшим примером такой атаки может служить подделка MAC- или IP-адресов. Подделав адрес отправителя в заголовке IP-пакета, злоумышленник тем самым уже осуществляет атаку типа «маскарад», выдавая себя за того, кто пользуется доверием у атакуемой стороны. Это дает возможность перехватить и прослушать сетевой трафик.

«Маскарад» - это выполнение какого-либо действия одним пользователем от имени другого пользователя, имеющего соответствующие полномочия. Часто злоумышленник, который перехватывает учетные данные пользователя, выполняет некоторые действия в системе от его имени. Таким образом, целью «маскарада» является присвоение каких-либо действий другому пользователю или присвоение полномочий и привилегий другого пользователя. Примером может служить отправка сообщений от имени другого пользователя.

1. Атака "Салями"

Атаки «салями». Атаки такого рода более всего характерны для систем. работающими с денежными счетами или чеками. Естественно, что наибольшую опасность они представляют именно для банков, но при некотором незатруднительном видоизменении могут быть применены в кассовых системах торговых предприятий или даже в почтовых отделениях, принимающих платежи от населения за коммунальные или другие услуги.
Принцип атак «салями» построен на том факте, что при обработке счетов используются целые единицы (центы, копейки, рубли и т. д.), а при начислении процентов или при расчете уплат при приобретении множества товаров нередко получаются дробные суммы.

Например, 6,5 % годовых от 102, 87 $ за 31 день составит 0, 5495726 $. Любая банковская система округлит эту сумму до 0,55 $. Однако, если пользователь

имеет доступ к банковским счетам, или программам их обработки, он может округлить ее в другую сторону – 0, 54 $, а разницу в 1 цент записать на свой счет. Владелец счета вряд ли ее заметит, а если и обратит внимание, то спишет ее на погрешности обработки и не придаст значения. Злоумышленник же получит прибыль в один цент. При обработке 1000 счетов в день его прибыль составит 100 $, т. е. примерно 30 000 $ в год. Но многие банки, или учреждения, работающие с приемом денег обрабатывают еще большее количество счетов в день.

Отсюда и происходит название таких атак – как колбаса салями изготавливается из небольших частей разных сортов мяса, так и счет злоумышленника пополняется за счет различных вкладчиков.
Успех таких атак зависит не от величины сумм, так как для любого счета погрешность атаки одинакова, а от количества счетов (или операций). Таким образом, причинами атак «салями» являются, во-первых, погрешности выполнений, позволяющие трактовать правила округления в ту или иную сторону, а во-вторых, огромные объемы вычислений. Атаки «салями» довольно трудно распознаются, если только злоумышленник не начинает накапливать на одном счете крупные суммы.

1. «Сборка мусора»

Сбор мусора (восстановление физически не уничтоженных данных) может осуществляться не только на дисках компьютера, но и в оперативной памяти. В этом случае специальная программа, запущенная злоумышленником, выделяет доступную оперативную память, сканирует ее содержимое и копирует фрагменты, содержащие заранее заданные ключевые слова. Если ОС не предусматривает очистки памяти, злоумышленник может получить интересующую его информацию, например, содержимое области памяти, только что освобожденной текстовым редактором, в котором редактировался конфиденциальный документ.

Сбор мусора: если инструменты ОС позволяют восстанавливать ранее удаленные объекты, хакер может использовать эту возможность для доступа к объектам, удаленным другими пользователями (например, путем просмотра содержимого их мусорных ящиков).

Сборка мусора - это технология, позволяющая, с одной стороны, упростить Программирование, избавив программиста от необходимости вручную удалять объекты, созданные в динамической памяти, а с другой-устранить ошибки, вызванные неправильным ручным управлением памятью.

В системе сборки мусора обязанность освободить память от объектов, которые больше не используются, возлагается на среду выполнения программы. Программист только создает динамические объекты и использует их, он может не заботиться об удалении объектов, так как среда делает это за него. Для реализации сборки мусора в среду выполнения включен специальный программный модуль под названием “сборщик мусора". Этот модуль периодически запускается, определяет, какие из объектов, созданных в динамической памяти, больше не используются, и освобождает занимаемую ими память.

Частота, с которой запускается сборщик мусора, определяется особенностями системы. Коллектор может работать в фоновом режиме, начиная, когда программа неактивна (например, когда программа простаивает, ожидая ввода пользователя). Сборщик мусора запускается безоговорочно, прерывая выполнение программы на время ее работы, когда следующая операция выделения памяти не может быть выполнена из-за того, что вся доступная память исчерпана. После освобождения памяти прерванная операция выделения памяти возобновляется, и программа продолжает работать. Если оказывается, что освободить память невозможно, среда выполнения останавливает программу с сообщением об ошибке "недостаточно памяти".

1. Незаконное использование привилегий.

Большинство систем безопасности устанавливают определенные наборы привилегий для выполнения определенных функций. Каждый пользователь имеет свой собственный набор привилегий, например: обычные пользователи имеют минимальный набор привилегий, а администраторы-максимальный. Такой способ несанкционированного доступа возможен либо при наличии ошибок в системе защиты, либо из-за халатности ответственного лица при присвоении привилегий пользователям.

1. Электромагнитное излучение и несанкционированное изменение конструкций

Также стоит отметить электромагнитное излучение и несанкционированное изменение конструкций как средства несанкционированного доступа к информации. Электромагнитное излучение используется киберпреступниками не только для получения информации, но и для ее уничтожения. Они способны уничтожать информацию на магнитных носителях. Мощное электромагнитное и микроволновое излучение может повредить электронные компоненты компьютерных систем. Более того, для уничтожения информации на магнитных

носителях с расстояния в несколько десятков метров можно использовать сравнительно небольшое устройство.

Несанкционированное изменение структуры компьютерных систем на этапах разработки и модернизации называется «закладка». Алгоритмические, программно-аппаратные «закладки» используются либо для прямого вредного воздействия на компьютерные системы, либо для обеспечения неконтролируемого входа в систему. Вредное воздействие закладок на компьютерные системы осуществляется при поступлении соответствующей команды извне (в основном характерной для аппаратных закладок) и при возникновении определенных событий в системе.

Процесс обработки и передачи информации техническими средствами КС сопровождается электромагнитными излучениями в окружающее пространство и наведением электрических сигналов в линиях связи. Они получили названия побочных электромагнитных излучений и наводок (ПЭМИН).

С помощью специального оборудования сигналы принимаются, выделяются, усиливаются и могут либо просматриваться, либо записываться в запоминающихся устройствах (ЗУ). Электромагнитные излучения используются злоумышленниками не только для получения информации, но и для ее уничтожения.

Большую угрозу безопасности информации в КС представляет несанкционированная модификация алгоритмической, программной и технической структур системы, которая получила название “закладка”. Как правило, “закладки” внедряются в специализированные системы и используются либо для непосредственного вредительского воздействия на КС, либо для обеспечения неконтролируемого входа в систему.

Одним из основных источников угроз безопасности является использование специальных программ, получивших общее название “вредительские программы”. К таким программам относятся:

- “компьютерные вирусы” – небольшие программы, которые после внедрения в ЭВМ самостоятельно распространяются путем создания своих копий, а при выполнении определенных условий оказывают негативное воздействие на КС;
- “черви” – программы, которые выполняются каждый раз при загрузке системы, обладающие способностью перемещаться в КС или сети и самовоспроизводить копии. Лавинообразное размножение программ

приводит к перегрузке каналов связи, памяти, а затем к блокировке системы;

“троянские кони” – программы, которые имеют вид полезного приложения, а на деле выполняют вредные функции (разрушение программного обеспечения, копирование и пересылка злоумышленнику файлов с конфиденциальной информацией и т.п.).

Глава 2. Угрозы безопасности персональных данных

2.1 Виды угрозы безопасности персональных данных

Наиболее актуальным и распространенным видом информации, с которой работают практически все организации Российской Федерации, являются персональные данные. В связи с их распространенностью, они требуют особой бдительности в их обработке и безопасности. Информационные системы, обрабатывающие персональные данные, могут подвергаться различным атакам из-за определенных уязвимостей.

Основной проблемой является доступность персональных данных в любой организации, коммерческой или государственной. Утечка таких данных может привести к финансовым потерям, административным или уголовным последствиям. Наряду с ростом технических возможностей копирования и распространения информации возросла необходимость своевременного принятия мер по качественной защите персональных данных[6].

Уровень информационных технологий на данном этапе развития человечества достаточно высок. Из-за этого самозащита информационных прав перестала эффективно функционировать. В современных реалиях человек физически не может добиться секретности от обилия используемых по отношению к нему аппаратных и программных средств и методов сбора или кражи данных, поэтому одной из наиболее актуальных проблем является проблема защиты персональных данных.

Нормативно-правовое регулирование защиты персональных данных в Российской Федерации осуществляется на основе

- Конституции РФ;
- Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) «О персональных данных»[7];
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (Выписка) (утверждена Федеральной службой по техническому и экспортному контролю РФ 15.02.2008)[8]
- Требования к защите персональных данных при их обработке в информационных системах персональных данных[9].

Для построения адекватной системы защиты персональных данных на начальном этапе составляется перечень реальных угроз безопасности Приложение 1.

Состав и содержание угрозы безопасности персональных данных (УБПДн) определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональных данных (ПДн).

Совокупность таких условий и факторов формируется с учетом характеристик информационной системы (ИСПДн), свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы. Реализация одной из УПДн перечисленных классов или их совокупности может привести к различным уровням последствий для субъектов ПДн.

Угрозы утечки ПДн по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки ПДн.

Угрозы, связанные с несанкционированным доступом (НСД), представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения информационной системы ПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации, директориев, каталогов, файлов с ПДн или самих ПДн) и возможных деструктивных действий. Такое представление описывается следующей формализованной записью:

Угроза НСД: = <источник угрозы>, <уязвимость программного или аппаратного обеспечения>, <способ реализации угрозы>, <объект воздействия>, <несанкционированный доступ>.

Глава 3. Угрозы информационной безопасности Российской Федерации

3.1 Виды угроз информационной безопасности РФ

Если в предыдущей главе мы рассматривали в основном информационную безопасность предприятия, ну или максимум корпорации, то в настоящей главе мы рассмотрим угрозы глобальной информационной безопасности, в масштабах страны. В частности, Российской Федерации.

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

1. угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
2. угрозы информационному обеспечению государственной политики Российской Федерации;
3. угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
4. угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России могут являться:

1. принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных

правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

2. создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем;
3. противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
4. нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
5. противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
6. неисполнение федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
7. неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;
8. дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
9. нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
10. вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;
11. девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
12. снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;

13. манипулирование информацией (дезинформация, сокрытие или искажение информации).

Угрозами информационному обеспечению государственной политики Российской Федерации могут являться:

- 1. монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
  2. блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;
  3. низкая эффективность информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Угрозами развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов могут являться[10]:

1. противодействие доступу Российской Федерации к новейшим информационным технологиям, взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов, а также создание условий для усиления технологической зависимости России в области современных информационных технологий;
2. закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
3. вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
4. увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут являться:

1. противоправные сбор и использование информации;
2. нарушения технологии обработки информации;
3. внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
4. разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
5. уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
6. воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
7. компрометация ключей и средств криптографической защиты информации;
8. утечка информации по техническим каналам;
9. внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;
10. уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
11. перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;
12. использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
13. несанкционированный доступ к информации, находящейся в банках и базах данных;
14. нарушение законных ограничений на распространение информации.

3.2 Источники угроз информационной безопасности РФ

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние.

К внешним источникам относятся:

1. деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
2. стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
3. обострение международной конкуренции за обладание информационными технологиями и ресурсами;
4. деятельность международных террористических организаций;
5. увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
6. деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
7. разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся:

критическое состояние отечественных отраслей промышленности;

1. неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;
2. недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;
3. недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

4. неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;
5. недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
6. недостаточная экономическая мощь государства;
7. снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
8. недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
9. отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

3.3 Угрозы национальной безопасности Российской Федерации

Состояние отечественной экономики, несовершенство системы организации государственной власти и гражданского общества, социально-политическая поляризация российского общества и криминализация общественных отношений, рост организованной преступности и увеличение масштабов терроризма, обострение межнациональных и осложнение международных отношений создают широкий спектр внутренних и внешних угроз национальной безопасности страны [11].

В сфере экономики угрозы имеют комплексный характер и обусловлены прежде всего существенным сокращением внутреннего валового продукта, снижением инвестиционной, инновационной активности и научно-технического потенциала, стагнацией аграрного сектора, разбалансированием банковской системы, ростом внешнего и внутреннего государственного долга, тенденцией к преобладанию в экспортных поставках топливно-сырьевой и энергетической составляющих, а в импортных поставках - продовольствия и предметов потребления, включая

предметы первой необходимости.

Ослабление научно-технического и технологического потенциала страны, сокращение исследований на стратегически важных направлениях научно-технического развития, отток за рубеж специалистов и интеллектуальной собственности угрожают России утратой передовых позиций в мире, деградацией наукоемких производств, усилением внешней технологической зависимости и подрывом обороноспособности России.

Негативные процессы в экономике лежат в основе сепаратистских устремлений ряда субъектов Российской Федерации. Это ведет к усилению политической нестабильности, ослаблению единого экономического пространства России и его важнейших составляющих - производственно-технологических и транспортных связей, финансово-банковской, кредитной и налоговой систем.

Экономическая дезинтеграция, социальная дифференциация общества, девальвация духовных ценностей способствуют усилению напряженности во взаимоотношениях регионов и центра, представляя собой угрозу федеративному устройству и социально-экономическому укладу Российской Федерации.

Этноэгоизм, этноцентризм и шовинизм, проявляющиеся в деятельности ряда общественных объединений, а также неконтролируемая миграция способствуют усилению национализма, политического и религиозного экстремизма, этносепаратизма и создают условия для возникновения конфликтов.

Единое правовое пространство страны размывается вследствие несоблюдения принципа приоритета норм Конституции Российской Федерации над иными правовыми нормами, федеральных правовых норм над нормами субъектов Российской Федерации, недостаточной отлаженности государственного управления на различных уровнях.

Угроза криминализации общественных отношений, складывающихся в процессе реформирования социально-политического устройства и экономической деятельности, приобретает особую остроту. Серьезные просчеты, допущенные на начальном этапе проведения реформ в экономической, военной, правоохранительной и иных областях государственной деятельности, ослабление системы государственного регулирования и контроля, несовершенство правовой базы и отсутствие сильной государственной политики в социальной сфере, снижение духовно-нравственного потенциала общества являются основными факторами, способствующими росту преступности, особенно ее организованных

форм, а также коррупции.

Последствия этих просчетов проявляются в ослаблении правового контроля за ситуацией в стране, в сращивании отдельных элементов исполнительной и законодательной власти с криминальными структурами, проникновении их в сферу управления банковским бизнесом, крупными производствами, торговыми организациями и товаропроводящими сетями. В связи с этим борьба с организованной преступностью и коррупцией имеет не только правовой, но и политический характер.

Масштабы терроризма и организованной преступности возрастают вследствие зачастую сопровождающегося конфликтами изменения форм собственности, обострения борьбы за власть на основе групповых и этнонационалистических интересов. Отсутствие эффективной системы социальной профилактики правонарушений, недостаточная правовая и материально-техническая обеспеченность деятельности по предупреждению терроризма и организованной преступности, правовой нигилизм, отток из органов обеспечения правопорядка квалифицированных кадров увеличивают степень воздействия этой угрозы на личность, общество и государство.

Угрозу национальной безопасности России в социальной сфере создают глубокое расслоение общества на узкий круг богатых и преобладающую массу малообеспеченных граждан, увеличение удельного веса населения, живущего за чертой бедности, рост безработицы.

Угрозой физическому здоровью нации являются кризис систем здравоохранения и социальной защиты населения, рост потребления алкоголя и наркотических веществ.

Последствиями глубокого социального кризиса являются резкое сокращение рождаемости и средней продолжительности жизни в стране, деформация демографического и социального состава общества, подрыв трудовых ресурсов как основы развития производства, ослабление фундаментальной ячейки общества - семьи, снижение духовного, нравственного и творческого потенциала населения.

Углубление кризиса во внутриполитической, социальной и духовной сферах может привести к утрате демократических завоеваний.

Основные угрозы в международной сфере обусловлены следующими факторами:

1. стремление отдельных государств и межгосударственных объединений принизить роль существующих механизмов обеспечения международной безопасности, прежде всего ООН и ОБСЕ;
2. опасность ослабления политического, экономического и военного влияния России в мире;
3. укрепление военно-политических блоков и союзов, прежде всего расширение НАТО на восток;
4. возможность появления в непосредственной близости от российских границ иностранных военных баз и крупных воинских контингентов;
5. распространение оружия массового уничтожения и средств его доставки;
6. ослабление интеграционных процессов в Содружестве Независимых Государств:
7. возникновение и эскалация конфликтов вблизи государственной границы Российской Федерации и внешних границ государств - участников Содружества Независимых Государств;
8. притязания на территорию Российской Федерации.

Угрозы национальной безопасности Российской Федерации в международной сфере проявляются в попытках других государств противодействовать укреплению России как одного из центров влияния в многополярном мире, помешать реализации национальных интересов и ослабить ее позиции в Европе, на Ближнем Востоке, в Закавказье, Центральной Азии и Азиатско-Тихоокеанском регионе.

Серьезную угрозу национальной безопасности Российской Федерации представляет терроризм. Международным терроризмом развязана открытая кампания в целях дестабилизации ситуации в России.

Усиливаются угрозы национальной безопасности Российской Федерации в информационной сфере. Серьезную опасность представляют собой стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Возрастают уровень и масштабы угроз в военной сфере.

Возведенный в ранг стратегической доктрины переход НАТО к практике силовых (военных) действий вне зоны ответственности блока и без санкции Совета Безопасности ООН чреват угрозой дестабилизации всей стратегической обстановки в мире.

Увеличивающийся технологический отрыв ряда ведущих держав и наращивание их возможностей по созданию вооружений и военной техники нового поколения создают предпосылки качественно нового этапа гонки вооружений, коренного изменения форм и способов ведения военных действий.

Активизируется деятельность на территории Российской Федерации иностранных специальных служб и используемых ими организаций.

Усилению негативных тенденций в военной сфере способствуют затянувшийся процесс реформирования военной организации и оборонного промышленного комплекса Российской Федерации, недостаточное финансирование национальной обороны и несовершенство нормативной правовой базы. На современном этапе это проявляется в критически низком уровне оперативной и боевой подготовки Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, в недопустимом снижении укомплектованности войск (сил) современным вооружением, военной и специальной техникой, в крайней остроте социальных проблем и приводит к ослаблению военной безопасности Российской Федерации в целом.

Угрозы национальной безопасности и интересам Российской Федерации в пограничной сфере обусловлены:

1. экономической, демографической и культурно-религиозной экспансией сопредельных государств на российскую территорию;
2. активизацией деятельности трансграничной организованной преступности, а также зарубежных террористических организаций.

Угроза ухудшения экологической ситуации в стране и истощения ее природных ресурсов находится в прямой зависимости от состояния экономики и готовности общества осознать глобальность и важность этих проблем. Для России эта угроза особенно велика из-за преимущественного развития топливно-энергетических отраслей промышленности, неразвитости законодательной основы природоохранной деятельности, отсутствия или ограниченного использования природосберегающих технологий, низкой экологической культуры. Имеет место тенденция к использованию территории России в качестве места переработки и

захоронения опасных для окружающей среды материалов и веществ.

В этих условиях ослабление государственного надзора, недостаточная эффективность правовых и экономических механизмов предупреждения и ликвидации чрезвычайных ситуаций увеличивают риск катастроф техногенного характера во всех сферах хозяйственной деятельности.

Заключение

Угроза защищаемой информации – совокупность явлений, факторов и условий, создающих опасность нарушения статуса информации.

Самым опасным источником дестабилизирующего воздействия на информацию является человек, потому как на защищаемую информацию могут оказывать воздействие различные категории людей.

Разнообразие видов и способов дестабилизирующего воздействия на защищаемую информацию говорит о необходимости комплексной системы защиты информации.

Современная Доктрина информационной безопасности Российской Федерации наиболее полно раскрывает виды и источники угроз информационной безопасности, а также методы обеспечения информационной безопасности.

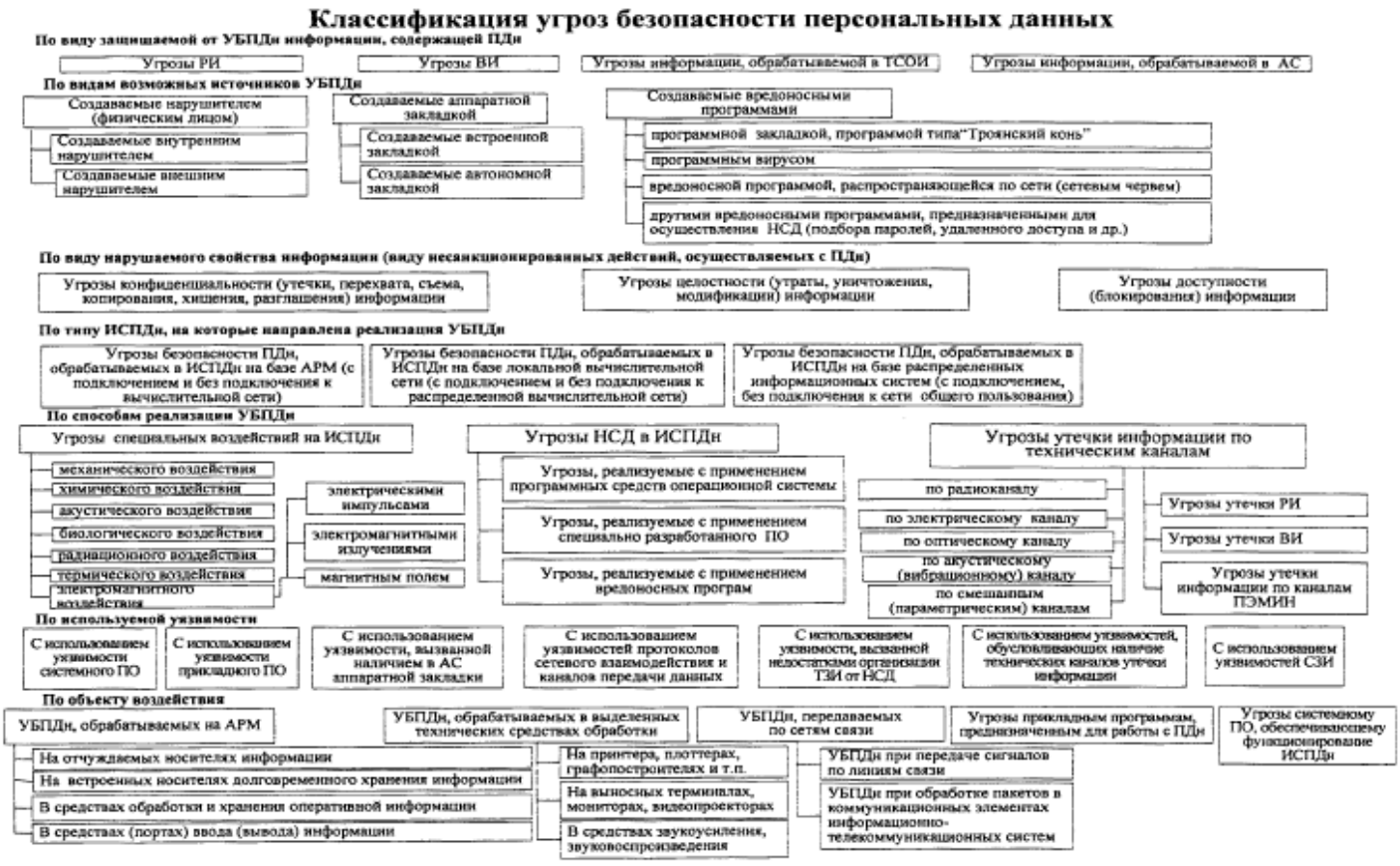
Список использованной литературы

1. Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895.
2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка) (утв. ФСТЭК РФ 15.02.2008). http://www.consultant.ru/document/cons_doc_LAW_99662/(Дата обращения 15.11.19)
3. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". Электронный ресурс. http://www.consultant.ru/document/cons_doc_LAW_137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/#dst100009 (Дата обращения 15.11.19)

4. Гончаренко Ю.Ю., Кушнарев А.А., Исаков С.А. Программная реализация методики определения актуальных угроз безопасности персональных данных // Научный результат. Информационные технологии. – Т.4, №1, 2019. с.9-14. (Дата обращения 15.11.19)
5. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) «О персональных данных». http://www.consultant.ru/document/cons_doc_LAW_61801/(Дата обращения 15.11.19)
6. Трунова А.В. Обеспечение информационной безопасности предприятия// Современные инновации. №4 (26). – 2018. с. 33-35.
7. Гришина, Н. В. Информационная безопасность предприятия. Учебное пособие / Н.В. Гришина. - М.: Форум, 2015. - 240 с
8. Алексеев Д.М., Иваненко К.Н., Убирайло В.Н. Классификация угроз информационной безопасности // Символ науки. 2016. №9-1, с. 18-19.
9. National Institute of Standards and Technology Special Publication 800-53, Revision 5 Natl. Inst. Stand. Technol. Spec. Publ. 800-53, Rev. 5, 494 pages (August 2017)
10. Атака типа "Маскарад". Угрозы безопасности инф-системам. URL: https://www.sites.google.com/site/ugrozybezopasno/home/ataka-tipa-maskarad
11. Мысев А.Э., Морозов Н.В. Правовое регулирование информационной безопасности в Российской Федерации// Отечественная юриспруденция. № 3 (35). – 2019. – с. 51-55.
12. Бигаева Д.Б., Бигаев А.Б. Система информационной безопасности Российской Федерации// Вестник науки и образования, Том. 2, №7 (31). – 2017. – с. 14-17.

ПРИЛОЖЕНИЯ

Приложение 1.



1. Трунова А.В. Обеспечение информационной безопасности предприятия// Современные инновации. №4 (26). – 2018. с. 33-35. ↑

2. Гришина, Н. В. Информационная безопасность предприятия. Учебное пособие / Н.В. Гришина. - М.: Форум, 2015. - 240 с ↑

3. Алексеев Д.М., Иваненко К.Н., Убирайло В.Н. Классификация угроз информационной безопасности // Символ науки. 2016. №9-1, с. 18-19. ↑

4. National Institute of Standards and Technology Special Publication 800-53, Revision 5 Natl. Inst. Stand. Technol. Spec. Publ. 800-53, Rev. 5, 494 pages (August 2017) ↑

5. Атака типа "Маскарад". Угрозы безопасности инф-системам. URL: https://www.sites.google.com/site/ugrozybezopasno/home/ataka-tipa-maskarad ↑

6. Гончаренко Ю.Ю., Кушнарев А.А., Исаков С.А. Программная реализация методики определения актуальных угроз безопасности персональных данных // Научный результат. Информационные технологии. – Т.4, №1, 2019. с.9-14. (Дата обращения 15.11.19) ↑

7. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) «О персональных данных». http://www.consultant.ru/document/cons_doc_LAW_61801/(Дата обращения 15.11.19) ↑

8. **Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка) (утв. ФСТЭК РФ 15.02.2008). http://www.consultant.ru/document/cons обращения 15.11.19)**

   ↑

9. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных". Электронный ресурс. http://www.consultant.ru/document/cons_doc_LAW _137356/8c86cf6357879e861790a8a7ca8bea4227d56c72/#dst100009 (Дата обращения 15.11.19) ↑

10. Мысев А.Э., Морозов Н.В. Правовое регулирование информационной безопасности в Российской Федерации// Отечественная юриспруденция. № 3 (35). – 2019. – с. 51-55. ↑

11. Бигаева Д.Б., Бигаев А.Б. Система информационной безопасности Российской Федерации// Вестник науки и образования, Том. 2, №7 (31). – 2017. – с. 14-17. ↑