Содержание:

Введение

Информация считается итогом отображения и обработки в человеческом сознании обилия окружающего мира, дает собой сведения об находящихся вокруг человека предметах, явлениях природы, деятельности других людей.

Под защитой информации в настоящее время понимается область науки и техники, которая включает совокупность средств, способов и методик людской работы, нацеленных на обеспечение защиты всех видов информации в организациях и предприятиях всевозможных направлений работы и всевозможных форм собственности.

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

Целями защиты информации считаются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных действий по устранению, трансформации, искажению, копированию, блокированию информации; предотвращение иных форм нелегального вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав людей на сбережение личной тайны и конфиденциальности индивидуальных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и использовании 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 несоблюдении ее единства, конфиденциальности, полноты и доступности.

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

Глава 1. Понятие и структура угроз защищаемой информации

Понятие угрозы защищаемой информации

Угроза – это потенциальная возможность определенным образом нарушить информационную безопасность, т.е. угрозы информации выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности.

При рассмотрении вопросов защиты информации понятие угрозы трактуется несколько в узком смысле как потенциальная возможность несанкционированного или случайного воздействия на информацию, приводящее к ее утрате, искажению, модификации и т.д.

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

Есть три различных подхода в определении угроз, которые включают в себя следующее:

1. угроза рассматривается как потенциально существующая ситуация (возможность, опасность) нарушения безопасности информации, при этом безопасность информации значит, что информация располагается в таком защищённом виде, который способен противостоять любым дестабилизирующим воздействиям;
2. угроза трактуется как явление (событие, случай или же вероятность их возникновения), следствием которых могут быть нежелательные влияния на информацию;

3. угроза ориентируется как реальные или же потенциально вероятные действия, или же обстоятельства, приводящие к той или другой форме проявления уязвимости информации.

Любая угроза не объединяется к чему-то конкретному, она состоит из определённых взаимосвязанных компонентов, каждый из которых сам по себе не составляет угрозу, но является её частью. Сама угроза появляется только при совокупном их содействии.

Подчеркнем, что само понятие "угроза" в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать — вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Угрозы защищаемой информации связаны с её уязвимостью, то есть неспособностью информации автономно противостоять дестабилизирующим воздействиям, нарушающим её статус. А несоблюдение статуса защищаемой информации состоит в несоблюдении её физической сохранности, логической структуры и содержания, доступности для правомочных пользователей, конфиденциальности (закрытости для посторонних лиц), и выражается по средствам реализации шести форм проявления уязвимости информации.

Прежде всего угроза обязана иметь некие сущностные проявления, а каждое проявление принято именовать явлением, значит, одним из признаков и вместе с тем одной из составляющих угроз должно быть явление.

В базе любого явления лежат составляющие причины, которые считаются его движущей мощью и которые в собственную очередь обоснованы определёнными жизненными обстоятельствами или же предпосылками. Эти предпосылки и условия относятся к моментам, формирующим вероятность дестабилизирующего влияния на информацию. Таким образом, факторы являются её одним признаком и составляющей угрозы

Еще одним определённым признаком угрозы считается её направленность, то есть итог, к которому может привести дестабилизирующее влияние на информацию.

Структура угроз

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

Для раскрытия структуры угроз нужно признаки угроз конкретизировать содержательной частью, которые в свою очередь обязаны раскрыть характер явлений и факторов, квалифицировать их состав и состав условий.

К сущностным проявлениям угрозы относятся:

1. источник дестабилизирующего воздействия на информацию (от кого или чего исходят эти воздействия);
2. виды дестабилизирующего воздействия на информацию (каким образом);
3. способы дестабилизирующего воздействия на информацию (какими приёмами, действиями осуществляются и реализуются виды дестабилизирующего воздействия).

К факторам кроме причин и обстоятельств следует отнести наличие каналов и способов несанкционированного доступа к конфиденциальной информации для влияния на информацию со стороны лиц, не имеющих к ней разрешённого доступа.

А так же, в качестве классифицирующего признака угроз информационной безопасности могут быть применены их направленность и происхождение.

По направленности угрозы информационной безопасности могут быть классифицированы следующим образом:

а) для личности:

– нарушение конституционных прав и свобод граждан на поиск, получение, передачу, производство и распространение объективной информации;

– лишение права граждан на неприкосновенность частной жизни;

– нарушение права граждан на защиту своего здоровья от неосознаваемой человеком вредной информации;

– посягательства на объекты интеллектуальной собственности;

б) для общества:

– препятствия в построении информационного общества;

– лишение права на духовное обновление общества, сохранение его нравственных ценностей, утверждение в обществе идеалов высокой нравственности, патриотизма и гуманизма, развитие многовековых духовных традиций Отечества, пропаганду национального, культурного наследия, норм морали и общественной нравственности;

– манипулирование массовым сознанием;

– создание атмосферы, препятствующей приоритетному развитию современных телекоммуникационных технологий, сохранению и развитию отечественного научного и производственного потенциала;

в) для государства:

– противодействие:

– защите интересов личности и общества;

– построению правового государства;

– формированию институтов общественного контроля за органами государственной власти;

– формированию системы подготовки, принятия и реализации решений органами государственной власти, обеспечивающей баланс интересов личности, общества и государства;

– защите государственных информационных систем и государственных информационных ресурсов;

– защите единого информационного пространства страны.

По происхождению основные угрозы жизненно важным интересам личности, общества и государства в информационной сфере включают:

а) внутренние:

– отставание России от ведущих стран мира по уровню информатизации;

– ослабление роли русского языка как государственного языка Российской Федерации;

– размывание единого правового пространства страны вследствие принятия субъектами Российской Федерации нормативных правовых актов, противоречащих Конституции Российской Федерации и федеральному законодательству;

– разрушение единого информационного и духовного пространства России, активизация различного рода религиозных сект, наносящих значительный ущерб духовной жизни общества, представляющих прямую опасность для жизни и здоровья граждан;

– отсутствие четко сформулированной информационной политики, отвечающей национальным целям, ценностям и интересам;

б) внешние:

– целенаправленное вмешательство и проникновение в деятельность и развитие информационных систем Российской Федерации;

– стремление сократить использование русского языка как средства общения за пределами России;

– попытки не допустить участия России на равноправной основе в международном информационном обмене;

– подготовка к информационным войнам и использование информационного оружия.

Глава 2. Угрозы нарушения конфиденциальности, доступности и целостности информации

Источники дестабилизирующего влияния

К источникам дестабилизирующего влияния на информацию относятся:

1. люди;

2. технические способы отображения, хранения, обработки, проигрывания, передачи информации, способы связи;

3. системы обеспечения функционирования технических средств;

4. технологические процессы отдельных категорий промышленных объектов;

5. природные появления.

Наиболее распространенным, разнообразным и опасным источником дестабилизирующего влияния на защищаемую информацию считаются люди. Он таков, вследствие того, что на защищаемую информацию влияют всевозможные категории людей, как работающих, так и неработающих на предприятии.

К данному источнику относятся:

а) сотрудники данного предприятия;

б) лица, не работающие на предприятии, но имеющие доступ к защищаемой информации в силу служебного положения;

в) сотрудники государственных органов разведки иных государств и конкурирующих предприятий;

г) лица из преступных структур.

Технические способы считаются вторыми по значению источником дестабилизирующего влияния на защищаемую информацию в силу их многообразия.

К данному источнику относятся:

1. электронно-вычислительная техника;
2. электрические и автоматические машинки и копировально-множительная техника;
3. средства видео и звукозаписывающей и воспроизводящей техники;
4. средства телефонной, телеграфной, факсимильной, громкоговорящей;
5. средства радиовещания и телевидения;
6. средства кабельной и радиосвязи.

Третий источник дестабилизирующего влияния на информацию подключает системы электроснабжения, водоснабжения, теплоснабжения, кондиционирования. К данному источнику примыкают вспомогательные электронные и радиоэлектронные системы и способы.

К четвертому источнику относятся технологические процессы обработки всевозможных объектов ядерной энергетики, химической индустрии,

радиоэлектроники, а еще объекты по приготовлению кое-каких видов вооружения и военнослужащей техники, которые изменяют естественную структуру окружающей среды.

Пятый источник – это природные явления, которые включают в себя две составляющие:

1. стихийные бедствия;
2. атмосферные явления.

Виды дестабилизирующих влияний

Со стороны людей возможно следующие виды дестабилизирующих воздействий:

- 1. непосредственное влияние на носители защищаемой информации;
  2. несанкционированное распространение конфиденциальной информации;
  3. нарушение режима работы технических средств отображение хранения, обработки, воспроизведения, передачи информации, средств связи и технологий обработки информации;
  4. вывод из строя технических средств и средств связи;
  5. вывод из строя и несоблюдение режима работы систем обеспечения функционирования названных средств.

Методами конкретного влияния на носители защищаемой информации могут быть:

1. физическое разрушение носителя информации;
2. создание аварийных ситуации для носителей;
3. удаление информации с носителей;
4. создание искусственных магнитных полей для размагничивания носителей;
5. внесение фальсифицированной информации.

Несанкционированное распространение конфиденциальной информации может осуществляться следующим образом:

1. словесная передача информации (разбалтывание);
2. передача копий носителя информации;
3. показ носителей информации;
4. ввод информации в вычислительные сети и системы;
5. опубликование информации в открытой печати;

6. использование информации в открытых публичных выступлениях;
7. к несанкционированному распространению информации может так же принести и потеря носителей информации.

Методами несоблюдения работы технических средств и обработки информации могут быть:

1. повреждения отдельных составляющих средств
2. нарушение правил эксплуатации средств
3. внесение изменений в порядок обработки информации
4. заражение программ обработки информации вредоносными программами
5. выдача неправильных программных команд
6. превышение расчетного числа запросов
7. создание помех в радио-эфире с помощью дополнительного звукового или шумового фона, изменение (наложение) частот передачи информации
8. передача ложных сигналов
9. подключение подавляющих фильтров в информационные цепи, цепи питание и заземления
10. нарушение режима работы систем обеспечения функционирования средств.

К четвертому виду можно отнести следующие способы:

- 1. неправильный монтаж технических средств;
  2. разрушение (поломка) средств, в том числе, повреждения (разрыв) кабельных линий связи;
  3. создание аварийных ситуаций для технических средств;
  4. отключение средств от сетей питания;
  5. вывод из строя или нарушения режима работы систем обеспечения функционирования средств;
  6. монтирование в электронно-вычислительную технику разрушающих радио и программных закладок.

Способом вывода из строя и нарушения режима работы систем обеспечения функционирования технических средств можно отнести:

1. не правильный монтаж систем;
2. разрушение или поломка систем или их отдельных элементов;
3. создание аварийных ситуаций для систем;
4. отключение систем от источников питания;
5. нарушения правил эксплуатации систем.

К видам дестабилизирующего воздействия второго источника относятся:

1. выход средств из строя;
2. сбои в работе средств;
3. создание электромагнитных излучений;

Способы дестабилизирующего влияния

Основными способами дестабилизирующего воздействия второго источника являются:

1. технические поломки и аварии;
2. возгорание технических средств;
3. выход из строя систем обеспечения функционирования средств;
4. негативные воздействия природных явлений;
5. воздействия измененной структуры окружающего магнитного поля;
6. воздействия вредоносных программных продуктов;
7. разрушение или повреждение носителя информации;
8. возникновение технических неисправностей элементов средств.

Видами третьего источника дестабилизирующего воздействия на информацию являются:

1. выход систем из строя;
2. сбои в работе системы.

К способам этого вида относятся:

1. поломки и аварии;
2. возгорания;
3. выход из строя источников питания;
4. воздействия природных явлений;
5. появление технических неисправностей элементов системы;
6. изменения естественного радиационного фона окружающей среды (на объектах ядерной энергетики);
7. изменения химического состава окружающей среды (на объектах химической промышленности);
8. изменения локальной структуры магнитного поля происходящего вследствие деятельности объектов радиоэлектроники и при изготовлении некоторых

видов вооружения и военной технике.

К стихийным бедствиям и одновременно видам воздействия следует отнести землетрясения, наводнения, ураган (смерч), оползни, лавины, извержения вулканов.

К атмосферным явлениям (видам воздействия) относятся: гроза, дождь, снег, град, мороз, жара, изменения влажности воздуха и магнитные бури.

Глава 3. Защита информации в информационных системах

Средства защиты информации

Средства защиты информации — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

- Технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они препятствуют доступу к информации, в том числе с помощью её маскировки. К аппаратным средствам относятся: генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны — недостаточная гибкость, относительно большие объём и масса, высокая стоимость.

- Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств — универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки — ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).
- Смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства.
- Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки — высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

По степени распространения и доступности выделяются программные средства, другие средства применяются в тех случаях, когда требуется обеспечить дополнительный уровень защиты информации.

Рисунок 1. Классификация средств инженерно-технической защиты

Аппаратные средства защиты информации

К аппаратным средствам защиты относятся различные электронные, электронно-механические, электронно-оптические устройства. К настоящему времени разработано значительное число аппаратных средств различного назначения, однако наибольшее распространение получают следующие:

- специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или уровней секретности;
- устройства измерения индивидуальных характеристик человека (голоса, отпечатков) с целью его идентификации;
- схемы прерывания передачи информации в линии связи с целью периодической проверки адреса выдачи данных.
- устройства для шифрования информации (криптографические методы);
- модули доверенной загрузки компьютера.

Рисунок 2. Аппаратные средства защиты информации

Аппаратные средства защиты используются для решения следующих задач:

- проведение особых изучений технических средств обеспечения производственной работы на наличие возможных каналов утечки информации.
- выявление каналов утечки информации на различных объектах и в помещениях.
- локализация каналов утечки информации.
- поиск и обнаружение средств промышленного шпионажа.
- сопротивление несанкционированному доступу к источникам секретной информации и иным действиям.

Программные средства защиты информации

Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации на подобии временных файлов, тестового контроля системы защиты и др. Преимущества программных средств — универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Дефекты — ограниченная работоспособность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, вероятная зависимость от типов компьютеров (их аппаратных средств).

Рисунок 3. Программные средства защиты информации

- Интегрированные средства защиты информации
- Антивирусная программа (антивирус) — программа для обнаружения компьютерных вирусов и лечения зараженных файлов, а также для

профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом.

- Специализированные программные средства защиты информации от несанкционированного доступа обладают в целом лучшими возможностями и характеристиками, чем интегрированные средства. Не считая программ шифрования и криптографических систем, есть большое количество иных доступных внешних средств защиты информации.
- Межсетевые экраны (также именуемые брандмауэрами или же файрволами). Между локальной и глобальной сетями формируются особые промежуточные серверы, которые проверяют и фильтруют весь проходящий через них трафик сетевого/транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет данную угрозу полностью. Более защищенная разновидность метода — это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик направляется от имени firewall-сервера, делая локальную сеть практически невидимой.
- Proxy-servers (proxy — доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью — маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через особые серверы-посредники. Бесспорно, что при данном обращения из глобальной сети в локальную становятся неосуществимыми в принципе. Данный способ не дает необходимой защиты против атак на более высоких уровнях — к примеру, на уровне приложения (вирусы, код Java и JavaScript).
- VPN (виртуальная частная сеть) разрешает транслировать секретную информацию через сети, в которых возможно прослушивание трафика посторонними людьми. Применяемые технологии: PPTP, PPPoE, IPSec.

Глава 4. Типы угроз информационной безопасности РФ

По своей совместной направленности угрозы информационной безопасности Российской Федерации разделяются на следующие типы:

1. угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной работы, персональному, массовому и социальному сознанию, духовному возрождению России;

2. угрозы информационному обеспечению государственной политики Российской Федерации;

3. угрозы развитию российской промышленности информации, охватывая промышленность средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу данной продукции на мировой рынок, а еще обеспечению скопления, сохранности и действенного применения российских информационных ресурсов;

4. угрозы защищенности информационных и телекоммуникационных средств и систем, как уже развернутых, например и формируемых на территории РФ.

Угрозами конституционным правам и свободам человека и гражданина в области духовной жизни и информационной работы, персональному, массовому и социальному сознанию, духовному возрождению РФ имеют все шансы считаться:

1. принятие федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы людей в области духовной жизни и информационной деятельности;
2. создание монополий на составление, получение и распространение информации в Российской Федерации, в том числе с внедрением телекоммуникационных систем;
3. противодействие, в том числе со стороны преступных структур, реализации горожанами собственных конституционных прав на собственную и семейную тайну, тайну переписки, телефонных переговоров и других сообщений;
4. нерациональное, излишнее лимитирование доступа к общественно важной информации;
5. противоправное использование особых средств влияния на личное, массовое и социальное сознание;
6. дезорганизация и разрушение системы скопления и хранения культурных ценностей, охватывая архивы;
7. нарушение конституционных прав и свобод человека и господина в области глобальной информации;
8. вытеснение российских информационных агентств, средств глобальной информации с внутреннего информационного рынка и ужесточение зависимости духовной, финансовой и политической сфер социальной жизни РФ от иностранных информационных структур;

9. снижение духовного, нравственного и креативного потенциала населения РФ, собственно что значимо осложнит подготовку трудовых ресурсов для внедрения и применения новейших технологий, в том числе информационных;
10. манипулирование информацией (дезинформация, сокрытие или же искажение информации).

Угрозами информационному обеспечению государственной политики РФ могут являться:

- 1. монополизация информационного рынка РФ, его отдельных разделов отечественными и зарубежными информационными структурами;
  2. блокирование работы государственных средств глобальной информации по информированию российской и зарубежной аудитории;
  3. низкая эффективность информационного обеспечения государственной политики РФ вследствие недостатка обученных сотрудников, недоступности системы формирования и реализации государственной информационной политики.

Угрозами развитию отечественной индустрии информации, охватывая индустрию средств информатизации, телекоммуникации и связи, обеспечению необходимостей внутреннего рынка в ее продукции и выходу данной продукции на мировой рынок, а еще обеспечению накопления, сохранности и действенного применения отечественных информационных ресурсов могут считаться:

1. противодействие доступу Российской Федерации к новым информационным технологиям, взаимовыгодному и равноправному участию российских изготовителей в крупном делении труда в индустрии информационных предложений, средств информатизации, телекоммуникации и связи, информационных товаров, а еще создание критерий для усиления технологической зависимости РФ в области передовых информационных технологий;
2. закупка органами государственной власти привезенных из других стран средств информатизации, телекоммуникации и связи при наличии российских аналогов, не уступающих по собственным характеристикам зарубежным образцам;
3. вытеснение с российского рынка российских изготовителей средств информатизации, телекоммуникации и связи;

Угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, например и формируемых на территории РФ, имеют все шансы считаться:

1. противоправные сбор и внедрение информации;
2. нарушения технологии обработки информации;
3. внедрение в аппаратные и программные изделия компонент, реализующий функции, не предусмотренные документацией на эти изделия;
4. разработка и распространение программ, нарушающих обычное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
5. уничтожение, повреждение, радиоэлектронное угнетение или же разрушение средств и систем обработки информации, телекоммуникации и связи;
6. уничтожение, повреждение, разрушение или же хищение машинных и иных носителей информации;

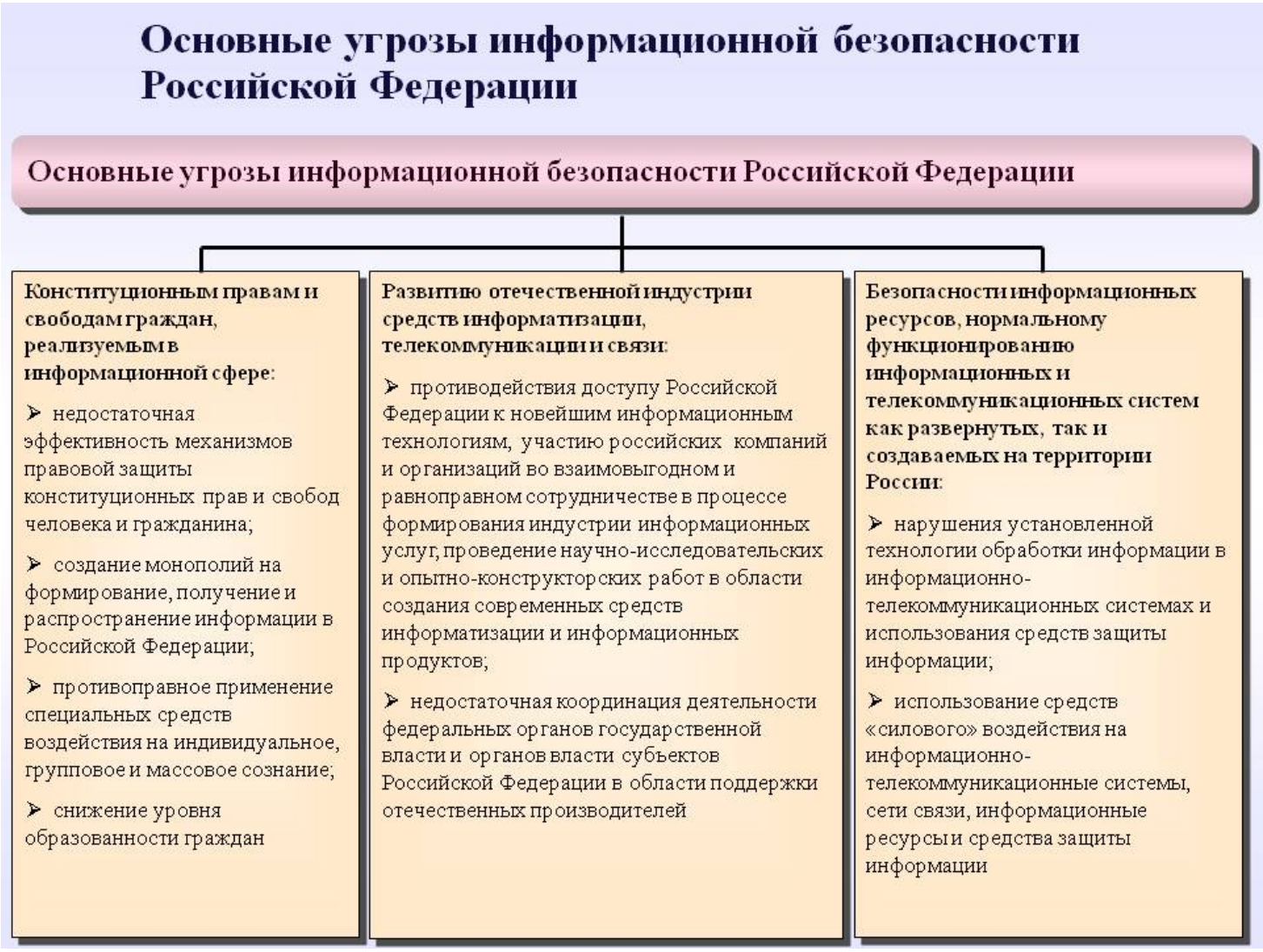

Рисунок 4. Угрозы информационной безопасности РФ

Глава 5. Источники угроз информационной безопасности РФ

Источники угроз информационной безопасности РФ разделяются на внешние и внутренние.

К внешним источникам относятся:

- работа зарубежных политических, финансовых, боевых, разведывательных и информационных структур, нацеленная против интересов РФ в информационной сфере;
- влечение ряда государств к преобладанию и ущемлению интересов РФ в крупном информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение интернациональной конкуренции за обладание информационными технологиями и ресурсами;
- работа интернациональных террористических организаций; наращивание технологического отрыва основных держав мира и наращивание их вероятностей по противодействию созданию конкурентоспособных российских информационных технологий;
- работа галактических, воздушных, морских и наземных технических и других средств (видов) разведки зарубежных государств;
- разработка вблизи стран концепций информационных войн, предусматривающих создание средств небезопасного влияния на информационные сферы иных государств мира, несоблюдение обычного функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

Рисунок 5. Источники информационных угроз для РФ

К внутренним источникам относят:

- неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и преступных структур в информационной сфере, получения криминальными структурами доступа к секретной информации, усиления воздействия санкционированной преступности на жизнь общества, понижения степени безопасности легитимных интересов людей, общества и страны в информационной сфере;
- недостающая координация работы федеральных органов государственной власти, органов государственной власти субъектов РФ по формированию и реализации единой государственной политики в области обеспечения информационной защищенности РФ;

- недостающая разработанность нормативной правовой базы, регулирующей дела в информационной сфере, а еще недостающая правоприменительная практика;
- неразвитость ВУЗов гражданского общества и недостающий муниципальный контроль, за развитием информационного рынка России;
- недостающее финансирование событий по обеспечению информационной защищенности РФ;
- недостающая финансовая сила государства;
- понижение производительности системы образования и воспитания, недостающее численность обученных сотрудников в области обеспечения информационной безопасности;
- недостающая энергичность федеральных органов государственной власти, органов государственной власти субъектов РФ в информировании общества о собственной работе, в объяснении принимаемых заключений, в формировании раскрытых муниципальных ресурсов и развитии системы доступа к ним граждан;
- отставание РФ от основных государств мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления, кредитно-финансовой сферы, индустрии, сельского хозяйства, образования, здравоохранения, сферы предложений и обстановки людей.

Заключение

Угроза защищаемой информации – совокупность явлений, моментов и критерий, создающих угрозы нарушения статуса информации.

Наиболее небезопасным источником дестабилизирующего влияния на информацию считается человек, вследствие того как на защищаемую информацию могут оказывать влияние всевозможные категории людей.

Многообразие видов и методик дестабилизирующего влияния на защищаемую информацию говорит о надобности комплексной системе защиты информации.

Прогрессивная Доктрина информационной безопасности РФ более полно открывает виды и источники опасностей информационной защищенности, а еще способы обеспечения информационной защищенности.

Таким образом, список угроз и источников их появления довольно разнообразен. Сопротивление проявлениям угроз исполняется по разным направлениям, с внедрением совершенного арсенала способов и средств защиты.

Список использованной литературы

1. Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895.
2. Концепция национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 17 декабря 1997 г. № 1300 (с изменениями и дополнениями от 10 января 2000 г. № 24).
3. Алексинцев А.И. «Безопасность информационных технологий» - 2001г. - №3.
4. Живерский А.А. «Защита информации. Проблемы теории и практики» - М.: 1996г.
5. Федеральный Закон РФ N 85-ФЗ. Принят Государственной Думой 04 июля 1996г. "Об участии в международном информационном обмене".
6. http://ebiblio.ru/book/bib/01_informatika/Inform_bezopast/2014/sg.html#_Toc433984081
7. https://studopedia.ru/7_65650_vidi-i-sostav-ugroz-informatsionnoy-bezopasnosti.html