Содержание:

ВВЕДЕНИЕ

Под информации в время область и которая совокупность методов и человеческой направленных на защиты всех информации в и различных деятельности и форм

Информация, подлежит может быть на носителях, храниться, и различными и

Актуальность обусловлена тем, что информация результатом и в сознании окружающего представляет сведения об человека явлениях деятельности людей.

Целями информации предотвращение утечки и доступа к сведениям; противоправных по модификации, копированию, информации; других форм вмешательства в ресурсы и системы; правового документированной как собственности; конституционных прав на личной и персональных имеющихся в системах; государственной конфиденциальности информации в с обеспечение прав в процессах и при производстве и информационных технологии и их

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.

В соответствие с целью поставлены следующие задачи:

1. охарактеризовать виды и состав угроз информационной безопасности;

2. определить источники угроз информационной безопасности

Российской Федерации.

Глава 1. Виды и состав угроз информационной безопасности

1.1. Понятие информационной безопасности

Информационная является важнейшей общей отдельно человека и в Не что против развязана и полномасштабная война с средств информации и сетей. Это и ведущих и СМИ о ЦРУ тайной против в на российское в ход президентской кампании.

Под безопасностью защищенность и ее от случайных или воздействий, которых явиться ущерба информации, ее или инфраструктуре[1].

Информационная организации - защищенности среды обеспечивающее её использование и

В социуме сфера две информационно-техническую созданный мир технологий и и (естественный мир природы, и человека). в случае безопасность (государства) представить составными информационно-технической и (психофизической)

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

– - информации, при доступ к ней только имеющие на него

– - несанкционированной информации;

– - временного или сокрытия от получивших доступа.

Выделяют и не обязательные модели

– неотказуемость или - отказа от

– - идентификации доступа и его

– - соответствия поведению или

– или - гарантирующее, что или идентичны

Действия, могут ущерб безопасности можно на категорий:

1. осуществляемые пользователями. В эту попадают: кража или данных на станции или повреждение пользователей в неосторожных

2. методы осуществляемые Под понимаются занимающиеся преступлениями как (в том в конкурентной так и из К методам несанкционированное в сети;

Целью несанкционированного проникновения извне в сеть предприятия может быть нанесение вреда (уничтожения данных), кража конфиденциальной информации и использование ее в незаконных целях, использование сетевой инфраструктуры для организации атак на узлы третьих фирм, кража средств со счетов и т.п.

Атака типа DOS (сокр. от Denial of Service - «отказ в обслуживании») ? это внешняя атака на узлы сети предприятия, отвечающие за ее безопасную и эффективную работу (файловые, почтовые сервера). Злоумышленники организуют массированную отправку пакетов данных на эти узлы, чтобы вызвать их перегрузку и, в итоге, на какое-то время вывести их из строя. Это, как правило, влечет за собой нарушения в бизнес-процессах компании-жертвы, потерю клиентов, ущерб репутации и т.п.

3. Компьютерные вирусы. Отдельная категория электронных методов воздействия – компьютерные вирусы и другие вредоносные программы. Они представляют собой реальную опасность для современного бизнеса, широко использующего компьютерные сети, Интернет и электронную почту. Проникновение вируса на узлы корпоративной сети может привести к нарушению их функционирования, потерям рабочего времени, утрате данных, краже конфиденциальной информации и даже прямым хищениям финансовых средств. Вирусная программа, проникшая в корпоративную сеть, может предоставить злоумышленникам частичный или полный контроль над деятельностью компании.

4. Спам. Всего за несколько лет спам из незначительного раздражающего фактора превратился в одну из серьезнейших угроз безопасности: электронная почта в последнее время стала главным каналом распространения вредоносных программ; спам отнимает массу времени на просмотр и последующее удаление сообщений, вызывает у сотрудников чувство психологического дискомфорта; как частные лица, так и организации становятся жертвами мошеннических схем, реализуемых

спамерами; вместе со спамом нередко удаляется важная корреспонденция, что может привести к потере клиентов, срыву контрактов и другим неприятным последствиям; опасность потери корреспонденции особенно возрастает при использовании черных списков RBL и других «грубых» методов фильтрации спама.

5. «Естественные» угрозы. На информационную безопасность компании могут влиять разнообразные внешние факторы: причиной потери данных может стать неправильное хранение, кража компьютеров и носителей, форс-мажорные обстоятельства и т.д[2].

Таким образом, в современных условиях наличие развитой системы информационной безопасности становится одним из важнейших условий конкурентоспособности и даже жизнеспособности любой компании.

Общение с использованием новейших средств коммуникации вобрал в себя Интернет. Всемирная информационная сеть развивается большими темпами, количество участников постоянно растет. По некоторым данным, в сети зарегистрировано около 1,5 миллиарда страниц. Некоторые «живут» до полугода, а некоторые работают на своих владельцев в полную силу и приносят большую прибыль. Информация в сети охватывает все стороны жизнедеятельности человека и общества. Пользователи доверяют этой форме себя и свою деятельность. Однако опыт работы в области компьютерных технологий полон примеров недобросовестного использования ресурсов Интернет.

Специалисты говорят, что главная причина проникновения в компьютерные сети - беспечность и неподготовленность пользователей. Это характерно не только для рядовых пользователей, но и для специалистов в области компьютерной безопасности. Вместе с тем, причина не только в халатности, но и в сравнительно небольшом опыте специалистов по безопасности в сфере информационных технологий. Связано это со стремительным развитием рынка сетевых технологий и самой сети Интернет.

По данным лаборатории Касперского, около 90% от общего числа проникновений на компьютер вредоносных программ используется посредством Интернет, через электронную почту и просмотр Web_страниц. Особое место среди таких программ занимает целый класс - Интернет-червь.

Само распространяющиеся, не зависимо от механизма работы выполняют свои основные задачи по изменению настроек компьютера-жертвы, воруют адресную книгу или ценную информацию, вводят в заблуждение самого пользователя,

создают рассылку с компьютера по адресам, взятым из записной книжки, делают компьютер чьим-то ресурсом или забирают часть ресурсов для своих целей или в худшем случае самоликвидируются, уничтожая все файлы на всех дисках.

Все эти и другие с ними связанные проблемы можно решить с помощью наличия в организации проработанного документа, отражающего политику информационной безопасности компании. В таком документе должны быть четко прописаны следующие положения:

– как ведется работа с информацией предприятия;

– кто имеет доступ;

– система копирования и хранения данных;

– режим работы на ПК;

– наличие охранных и регистрационных документов на оборудование и программное обеспечение;

– выполнение требований к помещению, где располагается ПК и рабочее место пользователя;

– наличие инструкций и технической документации;

– наличие рабочих журналов и порядок их ведения.

Кроме того, необходимо постоянно отслеживать развитие технических и информационных систем, публикуемых в периодической печати или следить за событиями, обсуждаемыми на подобных семинарах.

Так согласно Указа Президента РФ «О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена»[3], запрещено подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются госорганы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу РФ, в том числе к Интернету.

1.2 Основные виды и угрозы

Существует три подхода в угроз, включают в себя

1. угроза как существующая (возможность, нарушения информации, при этом информации что находится в защищённом который противостоять дестабилизирующим
2. угроза как (событие, или их следствием могут быть воздействия на
3. угроза как или возможные или приводящие к той или форме уязвимости

Любая не к однозначному, она из взаимосвязанных каждый из сам по себе не угрозу, но её Сама возникает лишь при их

Угрозы информации с её то есть информации противостоять воздействиям, её А статуса информации в её сохранности, структуры и доступности для пользователей, (закрытости для посторонних и по реализации форм уязвимости

Прежде , должна какие-то проявления, а проявление называть следовательно, из и с тем из угроз быть

В любого лежат причины, являются его силой и в свою обусловлены обстоятельствами или Эти и относятся к создающим дестабилизирующего на Таким факторы её признаком и угрозы.

Ещё определённым угрозы её то есть к может дестабилизирующее на

Угроза информации – явлений, и создающих нарушения информации.

Для структуры необходимо угроз содержательной которые в свою должны характер явлений и определить их и условий.

К проявлениям относятся:

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

К помимо и следует наличие и несанкционированного к информации для на со лиц, не к ней доступа.

Источники, виды и дестабилизирующего

К дестабилизирующего на относятся:

1. люди;
2. технические отображения, обработки, передачи средства
3. системы функционирования средств;
4. технологические отдельных промышленных
5. природные

Самым многообразным и источником воздействия на информацию люди. Он потому что на информацию оказывать категории как так и на

К источнику

1. сотрудники предприятия;
2. лица, не на но доступ к информации в силу положения;
3. сотрудники органов других и предприятий;
4. лица из криминальных структур.

Технические средства являются вторыми по значению источником дестабилизирующего воздействия на защищаемую информацию в силу их многообразия.

К этому 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 воздействия на информацию включает системы электроснабжения, водоснабжения, теплоснабжения, кондиционирования. К этому источнику примыкают вспомогательные электрические и радиоэлектронные системы и средства[4].

К четвертому источнику относятся технологические процессы обработки различных объектов ядерной энергетики, химической промышленности, радиоэлектроники, а также объекты по изготовлению некоторых видов вооружения и военной техники, которые изменяют естественную структуру окружающей среды.

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

1. стихийные бедствия;
2. атмосферные явления.

Со стороны людей возможно следующие виды дестабилизирующих воздействий:

- 1. непосредственное воздействие 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 нарушение режима работы систем обеспечения функционирования названных средств.

Способами непосредственного воздействия 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.

Способами нарушение работы технических средств и обработки информации могут быть:

1. повреждения отдельных элементов 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 дестабилизирующего второго относятся:

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

Основными дестабилизирующего второго являются:

1. технические и
2. возгорание средств;
3. выход из систем функционирования
4. негативные природных
5. воздействия структуры магнитного
6. воздействия программных
7. разрушение или носителя
8. возникновение неисправностей средств.

Видами источника воздействия на являются:

1. выход из
2. сбои в системы.

К этого вида

1. поломки и
2. возгорания;
3. выход из источников
4. воздействия явлений;
5. появление неисправностей системы;
6. изменения естественного радиационного фона окружающей среды (на объектах ядерной энергетики);
7. изменения химического состава окружающей среды (на объектах химической промышленности);
8. изменения структуры поля вследствие объектов и при некоторых вооружения и технике.

К бедствиям и видам следует землетрясения, ураган оползни, извержения

К явлениям воздействия) гроза, снег, мороз, изменения воздуха и бури.

Формы уязвимости информации

1. хищение информации или в нём (кража);
2. потеря информации
3. несанкционированное носителя или в нём (разрушение);
4. искажение (несанкционированное модификация, фальсификация и
5. блокирование информации (временное или постоянное);
6. разглашение информации (несанкционированное распространение или раскрытие информации).

Глава 2. Информационная безопасность в Российской Федерации

2.1. Источники угроз информационной безопасности Российской Федерации

По общей угрозы безопасности Федерации на виды:

1. угрозы правам и человека и в духовной и деятельности, групповому и сознанию, возрождению
2. угрозы обеспечению политики Федерации;
3. угрозы отечественной информации, индустрию информатизации, и обеспечению внутреннего в ее и этой на рынок, а обеспечению сохранности и использования информационных
4. угрозы информационных и средств и как уже так и на России.

Угрозами правам и человека и в духовной и деятельности, групповому и сознанию, возрождению могут [5]

1. принятие органами власти, государственной субъектов Федерации правовых ущемляющих права и граждан в духовной и деятельности;

2. создание на получение и распространение в Федерации, в том с телекоммуникационных

3. противодействие, в том со криминальных реализации своих прав на и тайну, переписки, переговоров и иных

1. нерациональное, ограничение к необходимой
2. противоправное специальных воздействия на групповое и сознание;
3. неисполнение органами власти, государственной субъектов Федерации, местного организациями и требований законодательства, отношения в сфере;
4. неnlравомерное dostlупа к инфоlрмационным федеlральных государlственной оlрганов власти Российской оlрганов самоупlравления, к аlрхивным к откlрытой значимой
5. дезоlрганизация и системы и культуlрных включая
6. наlрушение nlрав и человека и в массовой
7. вытеснение российских инфоlрмационных агентств, сlредств массовой инфоlрмации с внутlреннего инфоlрмационного рынка и усиление зависимости dlуховной, экономической и политической сфеlр общественной жизни России от заlрубежных инфоlрмационных структур;
8. девальвация ценностей, образцов культуры, на насилия, на и ценностях, ценностям, в обществе;
9. снижение нравственного и потенциала России, что осложнит трудовых для и новейших в том информационных;
10. манипулирование (дезинформация, или информации)[6].

Угрозами обеспечению политики Федерации являться:

- 1. монополизация рынка его сектоlров и инфоlрмационными
  2. блокиlрование государlственных массовой по российской и аудитории;
  3. низкая инфоlрмационного государlственной Российской вследствие квалифициlрованных отсlутствия фоlрмирования и государlственной политики.

Углрозамиотечественнойинфоlрмациииндустlриюинфоlрматизации,и обеспечениювнутlреннеговвееиэтойнарынок,аобеспечениюсохlранностии использованияинфоlрмационныхмогlут

1. nlротиводействие dostlупу Российской Федеlрации к новейшим инфоlрмационным технологиям, взаимовыгодномly и равноправному участию российских nlроизводителей в миlровом разделении tlруда в индустlрии инфоlрмационных услуг, сlредств инфоlрматизации, телекоммlуникации и связи, инфоlрмационных nlродуктов, а также создание условий для усиления

2. технологической России в современных технологий;
3. закупка государственной импортных информатизации, и при отечественных не по характеристикам образцам;
4. вытеснение с рынка производителей информатизации, и
5. увеличение за специалистов и интеллектуальной

Угрозами информационных и средств и как уже так и на России, являться:

1. противоправные сбор и информации;
2. нарушения обработки
3. внеdрение в и изделия реализующих не докlументацией на эти
4. разработка и пlрограмм, нolрмальное инфolрмационных и систем, в том систем информации;
5. уничтожение, радиоэлектронное или сlредств и обlработки телекоммlуникации и
6. воздействие на системы автоматизиlрованных обlработки и информации;
7. компlрометация и кlриптографической информации;
8. утечка по каналам;
9. внеdрение устlройств для инфolрмации в сlредства хlранения и инфolрмации по связи, а в помещения 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.

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.

2.2. 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[7]
.

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. Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 №351 (ред. 22.05.2015);

2. Концепция национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 31 декабря 2015 г. № 683.

3. Алексинцев А.И. «Безопасность информационных технологий» - 2012. - №3.

4. Галатенко, В.А. Основы информационной безопасности. Интернет-университет информационных технологий, 2014;

5. Живерский А.А. «Защита информации. Проблемы теории и практики» - М.: 2016.

6. Лопатин, В.Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества. М.: 2015. - 428 с;

7. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. ? М.: ДМК Пресс, 2014. - 544 с.

8. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный мир, 2016. - 352 с.

1. Алексинцев А.И. «Безопасность информационных технологий» - 2012. - №3. ↑

2. Галатенко, В.А. Основы информационной безопасности. Интернет-университет информационных технологий, 2014; ↑

3. Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17.03.2008 №351 (ред. 22.05.2015); ↑

4. Живерский А.А. «Защита информации. Проблемы теории и практики» - М.: 2016. ↑

5. Лопатин, В.Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества. М.: 2015. - 428 с; ↑

6. Лопатин, В.Н. Информационная безопасность России: Человек, общество, государство. Серия: Безопасность человека и общества. М.: 2015. - 428 с ↑

7. Алексинцев А.И. «Безопасность информационных технологий» - 2012. - №3. ↑