**СОДЕРЖАНИЕ**

Введение

Глава 1 Теоретическое исследование

1.1. История и Государственная политика в области информационной безопасности

1.2. Проблемы информационной безопасности и борьба с терроризмом. Угрозы и их показатели.

1.3. Методика реализации политики безопасности

1.4. Стандарты безопасности Гостехкомиссии. Стандарты Европы и США

1.5. Стеганография и ее применение в информационной безопасности

1.6. Классы информационной безопасности

1.7. Информационная безопасность Российской Федерации

Приложение

Вывод

Литература

### **ВВЕДЕНИЕ**

Вопросы информационной безопасности играют сегодня огромную роль в сфере высоких технологий, где именно информация (особенно цифровая) становится одновременно «продуктом и сырьём». Огромный мегаполис IT построен на всемирных реках данных из разных точек планеты. Её производят, обрабатывают, продают и, к сожалению, зачастую воруют.

Говоря об информационной безопасности, в настоящее время имеют в виду, собственно говоря, безопасность компьютерную. Действительно, информация, находящаяся на электронных носителях играет все большую роль в жизни современного общества. Уязвимость такой информации обусловлена целым рядом факторов: огромные объемы, многоточечность и возможная анонимность доступа, возможность "информационных диверсий"... Все это делает задачу обеспечения защищенности информации, размещенной в компьютерной среде, гораздо более сложной проблемой, чем, скажем, сохранение тайны традиционной почтовой переписки.

Если говорить о безопасности информации, сохраняющейся на "традиционных" носителях (бумага, фотоотпечатки и т.п.), то ее сохранность достигается соблюдением мер физической защиты (т.е. защиты от несанкционированного проникновения в зону хранения носителей). Другие аспекты защиты такой информации связаны со стихийными бедствиями и техногенными катастрофами. Таким образом, понятие "компьютерной" информационной безопасности в целом является более широким по сравнению с информационной безопасностью относительно "традиционных" носителей.

Если говорить о различиях в подходах к решению проблемы информационной безопасности на различных уровнях (государственном, региональном, уровне одной организации), то такие различия просто не существуют. Подход к обеспечению безопасности Государственной автоматизированной системы "Выборы" не отличается от подхода к обеспечению безопасности локальной сети в маленькой фирме.

Потому жизненно необходимы методы защиты информации для любого человека современной цивилизации, особенно использующего компьютер. По этой причине практически любой пользователь ПК в мире так или иначе «подкован» в вопросах борьбы с вирусами, «троянскими конями» и другими вредоносными программами, а также личностями стоящими за их созданием и распространением — взломщиками, спамерами, крэкерами, вирусмэйкерами (создателями вирусов) и просто мошенниками, обманывающих людей в поисках наживы — корпоративной информации, стоящей немалых денег.

Причём последние зачастую осуществляют задуманное руками своих жертв. А потому «технические» и «физические» методы защиты информации должны совмещаться с образованием пользователей в области компьютерных технологий и в частности компьютерной безопасности.

Одними из первых эти проблемы осознали и предприняли решительный шаг к их решению государственные ведомства США в конце 60-х годов, когда компьютеры стоили сотни тысяч долларов, а интернет зарождался из немногочисленных чисто военных и научных сетей.

Невозможно переоценить роль Средств Массовой Информации в их влиянии на формирование или деформирование институтов общества. Современный уровень таких наук, как социология и социальная психология в соединении с различными видами искусств, управляемых законами рекламы и маркетинга, позволяет использовать слово, кино- и видеоизображение в качестве новых инструментов управления. Завоевания новейшей демократии – свобода слова и плюрализм мнений, к сожалению, не могут послужить преградой Силам, желающим использовать эти свободы в своекорыстных интересах, обращенных во зло обществу.

Каждое человеческое общество имеет общую систему ценностей, обусловленную историей и менталитетом страны, нации. Эта система ценностей выработана опытом предшествующих поколений и представляет собой наиболее целесообразный, успешный способ существования, обеспечивающий интеграцию различных слоев общества. Для России это - христианские, православные моральные ценности. Все проблемы, встающие перед обществом, решаются в контексте этих ценностей. Их разрушение ведет к аномии, возникающей в эпохи крушения, моральному коллапсу, дезинтегрирующему социум.

До последнего времени проблема обеспечения безопасности компьютерной информации в нашей стране не только не выдвигалась на передний край, но фактически полностью игнорировалась. Считалось, что путем тотальной секретности, различными ограничениями в сфере передачи и распространения информации, можно решить проблему обеспечения информационной безопасности.

Существуют, так называемые, правовые меры обеспечения информационной безопасности.  К ним относится регламентация законом и нормативными актами действий с информацией и оборудованием, и наступление ответственности за нарушение правильности таких действий.

**Цель исследования:** определить существует ли в природе система, которая защитит информацию от взлома.

**Задачи исследования**:

* Определить, защищенность информации от взлома.
* Выявить проблемы информационной безопасности.
* Рассмотреть виды информационной безопасности.

*Объектом исследования* является информационная безопасность.

*Предметом исследования* являются проблемы информационной безопасности, законы, регулирующие информационную безопасность, угрозы и их показатели, стандарты безопасности и применение.

**Глава 1 Теоретическое исследование**

## **История и Государственная политика в области информационной безопасности**

При объединении и синхронизации вышеупомянутых сетей остро встал вопрос защиты «от шпионов» секретной государственной информации, особенно учитывая то насколько легко и быстро можно скопировать информацию в цифровом виде.

В 1967 под патронажем Национального Комитета Стандартов была учреждена Инициативная Группа исследователей по вопросам компьютерной безопасности, в которую вошли представители университетов, компаний по производству компьютеров, научно-исследовательских центров и других организаций.

Результатом объединения усилий промышленных и научных специалистов, множества теоретических исследований в широкой области математики — теории информации, а также огромного опыта в реальной индустрии, оказалась «радужная серия» - ряд стандартов и требований предъявляемых к оборудованию, программному обеспечению и персоналу так называемых систем автоматической обработки данных — компьютерных сетей, принадлежавших таким гос. структурам США как : NASA, Министерство Обороны, Национальный комитет стандартов, Министерство Труда, Отдел по охране окружающей среды, Министерство по контролю за вооружением, Национальное научное общество, Федеральная резервная система и наконец Центр Объединенного Командования ВС.

Был даже создан Национальный Центр Компьютерной Безопасности, занимавшийся этими вопросами.

А в 1981 был создан подобный центр при Министерстве Обороны, разработавший и внедривший «радужную серию» в 1985 году. Наиболее значимым для истории в силу своей общности и направленности не только на сугубо внутренние цели, но и на некую оценку качества коммерческих продуктов так или иначе обрабатывающих и хранящих конфиденциально важную информацию, стал стандарт «Критерии оценки доверенных компьютерных систем», названный Оранжевой книгой в силу цвета обложки (кстати говоря, оранжевую обложку имеет не только этот мировой стандарт — по меньшей мере спецификации на лазерный аудиодиск и на шейдерную модель OpenGL называют оранжевыми книгами). Её целью были максимальная гибкость и универсальность оценки безопасности.

Системы безопасности появились, чтобы защитить её от шпионом и от других взломов.

Информационная безопасность -состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Под информационной безопасностью РоссийскойФедерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Под национальными интересами Российской Федерации понимается:

* Информационное обслуживание руководства
* Сохранность инфраструктуры
* Развитие информационных средств
* Защита прав человека в информационной сфере
* Защита прав на частную информацию
* Защита баз данных
* Достоверность передаваемой информации

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

***Государственная политика обеспечения информационной безопасности Российской Федерации*** определяет основные направления деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации в этой области, порядок закрепления их обязанностей и ответственности за защищенность интересов Российской Федерации в информационной сфере в рамках закрепленных за ними направлений деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

***Государственная политика Российской Федерации в области информационной безопасности*** основывается на следующих принципах:

* Федеральная программа ИБ
* Нормативно-правовая база
* Регламентация доступа к информации
* Юридическая ответственность за сохранность информации
* Контроль за разработкой и использованием средств защиты информации
* Предоставление гражданам доступа к мировым информационным системам

Государство в процессе реализации своих функций по обеспечению информационной безопасности Российской Федерации:

* проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности Российской Федерации, разрабатывает меры по ее обеспечению;
* организует работу законодательных (представительных) и исполнительных органов государственной власти Российской Федерации по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации;
* поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;
* осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;
* проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории Российской Федерации и принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;
* способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;
* формулирует и реализует государственную информационную политику России;
* организует разработку федеральной программы обеспечения информационной безопасности Российской Федерации, объединяющей усилия государственных и негосударственных организаций в данной области;
* способствует интернационализации глобальных информационных сетей и систем, а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, является приоритетным направлением государственной политики в области обеспечения информационной безопасности Российской Федерации.

Политика государства заключается в том, чтобы защитить информацию в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

## **Проблемы информационной безопасности** **и борьба с терроризмом. Угрозы и их показатели**

Широкое внедрение информационных технологий в жизнь современного общества привело к появлению ряда общих проблем информационной безопасности:

* необходимо гарантировать непрерывность и корректность функционирования важнейших информационных систем (ИС), обеспечивающих безопасность людей и экологической обстановки;
* необходимо обеспечить защиту имущественных прав граждан, предприятий и государства в соответствии с требованиями гражданского, административного и хозяйственного права (включая защиту секретов и интеллектуальной собственности);
* необходимо защитить гражданские права и свободы, гарантированные действующим законодательством (включая право на доступ к информации).

Следует знать, что любая информационная система потенциально уязвима. И эта уязвимость по отношению к случайным и предумышленным отрицательным воздействиям выдвинула проблемы информационной безопасности в разряд важнейших, определяющих принципиальную возможность и эффективность применения ряда ИС в гражданских и военных отраслях.

Основная работа по снижению дестабилизирующих факторов в области информационной безопасности - раскрыть собственно суть проблемы, конкретизировать дестабилизирующие факторы и представить основные методы, способные значительно повысить защищенность ИС. Эта проблема в значительной степени решается посредством методов, средств и стандартов, поддерживающих системный анализ, технологию разработки и сопровождения программных систем (ПС) и баз данных (БД). Для достижения поставленной цели в необходимо рассмотреть исходные данные и факторы, определяющие технологическую безопасность сложных информационных систем:

* показатели, характеризующие технологическую безопасность информационных систем;
* требования, предъявляемые к архитектуре ПС и БД для обеспечения безопасности ИС;
* ресурсы, необходимые для обеспечения технологической безопасности ИС;
* внутренние и внешние дестабилизирующие факторы, влияющие на безопасность функционирования программных средств и баз данных;
* методы и средства предотвращения и снижения влияния угроз безопасности ИС со стороны дефектов программ и данных;
* оперативные методы и средства повышения технологической безопасности функционирования ПС и БД путем введения в ИС временной, программной и информационной избыточности;
* методы и средства определения реальной технологической безопасности функционирования критических ИС.

Основываясь на полученных данных необходимо выработать стратегию и тактику направленную на уменьшение факторов способных вызвать те или иные деструктивные последствия.

Проблема информационной безопасности заключается в том, что любую систему можно взломать.

Терроризм, как выражение крайнего экстремизма, основанное на различного рода разногласиях (как национального, так и транснационального масштаба) в политике, экономике, на религиозной или криминальной почве, обсуждается и осуждается давно. При современном уровне развития высоких технологий расширяются возможности их использования для совершения террористических действий. Во многих странах сегодня ведется активная работа по анализу потенциальных возможностей подобных проявлений и выработке мер по борьбе с этим злом.

Терроризм - совокупность противоправных действий, связанных с покушениями на жизнь людей, угрозами расправ, деструктивными действиями в отношении материальных объектов, искажением объективной информации или рядом других действий, способствующих нагнетанию страха и напряженности в обществе с целью получения преимуществ при решении политических, экономических или социальных проблем.

Направления противоправных, злоумышленных действий на сетевой среде с целью использования их результатов для проведения террористических актов можно представить в виде следующих:

* Разрушение инфраструктуры сети корпоративного, национального или транснационального масштаба посредством вывода из строя системы управления ею или отдельных подсистем.
* Несанкционированный (неправомерный) доступ к сетевой информации, охраняемой законом и носящей высокий уровень секретности, нарушение ее целостности, конструктивной управляемости и защищенности.

Следует отличать террористические действия от действий террористов с использованием сетевых ресурсов (в том числе собственных в Интернет) в целях пропаганды своих взглядов, нагнетания обстановки страха, напряженности и т. д.

Ущерб от террористических действий на сетевой среде связан:

* с человеческими жертвами или материальными потерями, вызванными деструктивным использованием элементов сетевой инфраструктуры;
* с возможными потерями (в том числе гибелью людей) от несанкционированного использования информации с высоким уровнем секретности или сетевой инфраструктуры управления в жизненно важных (критических) для государства сферах деятельности;
* с затратами на восстановление управляемости сети, вызванными действиями по ее разрушению или повреждению;
* с моральным ущербом как владельца сетевой инфраструктуры, так и собственного информационного ресурса;
* с другими возможными потерями от несанкционированного использования информации с высоким уровнем секретности.

Отличие подходов к предотвращению и реагированию на действия в случае террористического характера целей от других противоправных действий в сетях общего пользования связано с более высоким уровнем требований к безопасности систем, обусловленных их назначением, целями и средой безопасности, и, соответственно, величиной издержек от подобных злоумышленных действий.

В качестве понятия, интегрирующего противодействия кибертерроризму, рассмотрим антитеррористическую информационную безопасность с тем, чтобы подчеркнуть отличие от традиционной информационной безопасности.

Антитеррористическая информационная безопасность - совокупность механизмов, инструментальных средств, методов, мер и мероприятий, позволяющих предотвратить, обнаружить, а в случае обнаружения, - оперативно реагировать на действия, способные привести:

* к разрушению инфраструктуры сети посредством вывода из строя системы управления ею или отдельных ее элементов;
* к несанкционированному доступу к информации, охраняемой законом и носящей высокий уровень секретности, нарушению ее целостности, конструктивной управляемости и защищенности.

Основа антитеррористических действий с использованием сетевой среды - традиционная информационная безопасность, ее методология, модели, механизмы и инструментальные средства. Разработка, построение и сопровождение систем информационной безопасности для отдельных продуктов, изделий и комплексов на сетевой среде, особенно на сетях пакетной коммутации и Интернет, - сложная, многоплановая задача.

Антитеррористическая информационная безопасность является важным пунктом в информационной безопасности и ему уделяется особое значение.

Угроза безопасности информации ***-*** совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее.

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

К информационным угрозам относятся:

* 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;
* использование информационного оружия.

К программным угрозам относятся:

* использование ошибок и "дыр" в ПО;
* компьютерные вирусы и вредоносные программы;
* установка "закладных" устройств;

К физическим угрозам относятся:

* уничтожение или разрушение средств обработки информации и связи;
* хищение носителей информации;
* хищение программных или аппаратных ключей и средств криптографической защиты данных;
* воздействие на персонал;

К радиоэлектронным угрозам относятся:

* внедрение электронных устройств перехвата информации в технические средства и помещения;
* перехват, расшифровка, подмена и уничтожение информации в каналах связи.

К организационно-правовым угрозам относятся:

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

Словарь терминов Гостехкомиссии определяет понятие угроз национальной безопасности России в информационной сфере следующим образом:

***Угрозами национальной безопасности России в информационной сфере*** являются:

* 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, получения несанкционированного доступа к ним.

К мерам противодействия указанным угрозам необходимо отнести:

* постановку и проведение научных исследований, направленных на получение методик исследования программного обеспечения и выявления закладных устройств;
* развитие отечественной индустрии в области создания и производства оборудования элементов телекоммуникационных систем;
* минимизацию числа иностранных фирм - поставщиков;
* координацию действий по проверке надежности указанных фирм;
* уменьшению номенклатуры поставляемого оборудования;
* переходу от поставок оборудования к поставкам комплектующих на элементарном уровне;
* установлению приоритета в использовании отечественных средств защиты этих систем.

Существует много видов угроз.

## **Методика реализации политики безопасности**

Первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности Российской Федерации являются:

* разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере, а также подготовка концепции правового обеспечения информационной безопасности Российской Федерации;
* разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой информации, осуществления государственной информационной политики;
* принятие и реализация федеральных программ, предусматривающих формирование общедоступных архивов информационных ресурсов федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, повышение правовой культуры и компьютерной грамотности граждан, развитие инфраструктуры единого информационного пространства России, комплексное противодействие угрозам информационной войны, создание безопасных информационных технологий для систем, используемых в процессе реализации жизненно важных функций общества и государства, пресечение компьютерной преступности, создание информационно-телекоммуникационной системы специального назначения в интересах федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, обеспечение технологической независимости страны в области создания и эксплуатации информационно-телекоммуникационных систем оборонного назначения;
* развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности Российской Федерации;
* гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления, информационных и телекоммуникационных систем общего и специального назначения.

Также существует система обеспечения информационной безопасности Российской Федерации. Она предназначена для реализации государственной политики в данной сфере.

Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:

* разработка нормативной правовой базы в области обеспечения информационной безопасности Российской Федерации;
* создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;
* определение и поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информации;
* оценка состояния информационной безопасности Российской Федерации, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;
* координация деятельности федеральных органов государственной власти и других государственных органов, решающих задачи обеспечения информационной безопасности Российской Федерации;
* предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;
* развитие отечественной информационной инфраструктуры, а также индустрии телекоммуникационных и информационных средств, повышение их конкурентоспособности на внутреннем и внешнем рынке;
* проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации;
* организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации;
* защита государственных информационных ресурсов, прежде всего в федеральных органах государственной власти и органах государственной власти субъектов Российской Федерации, на предприятиях оборонного комплекса;
* обеспечение контроля за созданием и использованием средств защиты информации посредством обязательного лицензирования деятельности в данной сфере и сертификации средств защиты информации;
* осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Компетенция федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяется федеральными законами, нормативными правовыми актами Президента Российской Федерации и Правительства Российской Федерации.

Функции органов, координирующих деятельность федеральных органов государственной власти, органовгосударственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяются отдельными нормативными правовыми актами Российской Федерации.

Информационная безопасность Российской Федерации затрагивает все сферы общественной жизни.

## **Стандарты безопасности Гостехкомиссии. Стандарты Европы и США**

РД Гостехкомиссии России составляют основу нормативной базы в области защиты от НСД к информации в нашей стране. Наиболее значимые из них, определяющие критерии для оценки защищенности АС (СВТ), рассматриваются ниже.

Критерии для оценки механизмов защиты программно-технического уровня, используемые при анализе защищенности АС и СВТ, выражены в РД Гостехкомиссии РФ "АС. Защита от НСД к информации. Классификация АС и требования по защите информации" и "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации".

***РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"***

РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации" устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований. (Основным "источником вдохновения" при разработке этого документа послужила знаменитая американская "Оранжевая книга"). Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс седьмой, самый высокий - первый. Классы подразделяются на четыре группы, отличающиеся уровнем защиты:

**Первая группа** содержит только один седьмой класс, к которому относят все СВТ, не удовлетворяющие требованиям более высоких классов;

**Вторая группа** характеризуется дискреционной защитой и содержит шестой и пятый классы;

**Третья группа** характеризуется мандатной защитой и содержит четвертый, третий и второй классы;

**Четвертая группа** характеризуется верифицированной защитой содержит только первый класс.

***РД "АС. Защита от НСД к информации. Классификация АС и требования по защите информации"***

РД "АС. Защита от НСД к информации. Классификация АС и требования по защите информации" устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

* наличие в АС информации различного уровня конфиденциальности;
* уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
* режим обработки данных в АС - коллективный или индивидуальный.

Устанавливается девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности и конфиденциальности информации и, следовательно, иерархия классов защищенности АС.

***РД "СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации"***

При анализе системы защиты внешнего периметра корпоративной сети в качестве основных критериев целесообразно использовать РД "СВТ. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации". Данный документ определяет показатели защищенности межсетевых экранов (МЭ). Каждый показатель защищенности представляет собой набор требований безопасности, характеризующих определенную область функционирования МЭ. Всего выделяется пять показателей защищенности:

* Управление доступом;
* Идентификация и аутентификация;
* Регистрация событий и оповещение;
* Контроль целостности;
* Восстановление работоспособности.

На основании показателей защищенности определяются следующие пять классов защищенности МЭ:

* Простейшие фильтрующие маршрутизаторы - 5 класс;
* Пакетные фильтры сетевого уровня - 4 класс;
* Простейшие МЭ прикладного уровня - 3 класс;
* МЭ базового уровня - 2 класс;
* Продвинутые МЭ - 1 класс.

МЭ первого класса защищенности могут использоваться в АС класса 1А, обрабатывающих информацию "Особой важности". Второму классу защищенности МЭ соответствует класс защищенности АС 1Б, предназначенный для обработки "совершенно секретной" информации и т.п.

Также к стандартам России в области информационной безопасности относятся:

* Гост 28147-89 – блочный шифр с 256-битным ключом;
* Гост Р 34.11-94 –функция хэширования;
* Гост Р 34.10-94 –алгоритм цифровой подписи.

Существует много защит информационной безопасности.

Европейские стандарты безопасности

***ISO 15408: Common Criteria for Information Technology Security Evaluation***

Наиболее полно критерии для оценки механизмов безопасности программно-технического уровня представлены в международном стандарте ISO 15408: Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности информационных технологий), принятом в 1999 году.

Общие критерии оценки безопасности информационных технологий (далее "Общие критерии") определяют функциональные требования безопасности (security functional requirements) и требования к адекватности реализации функций безопасности (security assurance requirements).

Хотя применимость "Общих критериев" ограничивается механизмами безопасности программно-технического уровня, в них содержится определенный набор требований к механизмам безопасности организационного уровня и требований по физической защите, которые непосредственно связаны с описываемыми функциями безопасности.

Первая часть "Общих критериев" содержит определение общих понятий, концепции, описание модели и методики проведения оценки безопасности ИТ. В ней вводится понятийный аппарат, и определяются принципы формализации предметной области.

Требования к функциональности средств защиты приводятся во второй части "Общих критериев" и могут быть непосредственно использованы при анализе защищенности для оценки полноты реализованных в АС (СВТ) функций безопасности.

Третья часть "Общих критериев" содержит классы требований гарантированности оценки, включая класс требований по анализу уязвимостей средств и механизмов защиты под названием AVA: Vulnerability Assessment. Данный класс требований определяет методы, которые должны использоваться для предупреждения, выявления и ликвидации следующих типов уязвимостей:

* Наличие побочных каналов утечки информации;
* Ошибки в конфигурации либо неправильное использование системы, приводящее к переходу в небезопасное состояние;
* Недостаточная надежность (стойкость) механизмов безопасности, реализующих соответствующие функции безопасности;
* Наличие уязвимостей ("дыр") в средствах защиты информации, дающих возможность пользователям получать НСД к информации в обход существующих механизмов защиты.

***ISO 17799: Code of Practice for Information Security Management***

Наиболее полно критерии для оценки механизмов безопасности организационного уровня представлены в международном стандарте ISO 17799: Code of Practice for Information Security Management (Практические правила управления информационной безопасностью), принятом в 2000 году. ISO 17799 является ни чем иным, как международной версией британского стандарта BS 7799.

ISO 17799 содержит практические правила по управлению информационной безопасностью и может использоваться в качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты.

Практические правила разбиты на следующие 10 разделов:

* Политика безопасности;
* Организация защиты;
* Классификация ресурсов и их контроль;
* Безопасность персонала;
* Физическая безопасность;
* Администрирование компьютерных систем и вычислительных сетей;
* Управление доступом;
* Разработка и сопровождение информационных систем;
* Планирование бесперебойной работы организации;
* Контроль выполнения требований политики безопасности.

В этих разделах содержится описание механизмов безопасности организационного уровня, реализуемых в настоящее время в правительственных и коммерческих организациях во многих странах мира.

Десять средств контроля, предлагаемых в ISO 17799 (они обозначены как ключевые), считаются особенно важными. Под средствами контроля в данном контексте понимаются механизмы управления информационной безопасностью организации.

Ключевыми являются следующие средства контроля:

* Документ о политике информационной безопасности;
* Распределение обязанностей по обеспечению информационной безопасности;
* Обучение и подготовка персонала к поддержанию режима информационной безопасности;
* Уведомление о случаях нарушения защиты;
* Средства защиты от вирусов;
* Планирование бесперебойной работы организации;
* Контроль над копированием программного обеспечения, защищенного законом об авторском праве;
* Защита документации организации;
* Защита данных;
* Контроль соответствия политике безопасности.

Процедура аудита безопасности АС включает в себя проверку наличия перечисленных ключевых средств контроля, оценку полноты и правильности их реализации, а также анализ их адекватности рискам, существующим в данной среде функционирования. Составной частью работ по аудиту безопасности АС также является анализ и управление рисками.

Стандарты безопасности США

***"Оранжевая книга "***

"Department of Defense Trusted Computer System Evaluation Criteria"

OK принята стандартом в 1985 г. Министерством обороны США (DOD). Полное

название документа "Department of Defense Trusted Computer System Evaluation Criteria".

OK предназначается для следующих целей:

* Предоставить производителям стандарт, устанавливающий, какими средствами безопасности следует оснащать свои новые и планируемые продукты, чтобы поставлять на рынок доступные системы, удовлетворяющие требованиям гарантированной защищенности (имея в виду, прежде всего, защиту от раскрытия данных) для использования при обработке ценной информации;
* Предоставить DOD метрику для военной приемки и оценки защищенности ЭСОД, предназначенных для обработки служебной и другой ценной информации;
* Обеспечить базу для исследования требований к выбору защищенных систем.

Рассматривают два типа оценки:

* без учета среды, в которой работает техника;
* в конкретной среде (эта процедура называется аттестованием).

Во всех документах DOD, связанных с ОК, принято одно понимание фразы обеспечение безопасности информации. Это понимание принимается как аксиома и формулируется следующим образом: безопасность = контроль за доступом.

Классы систем, распознаваемые при помощи критериев оценки гарантированно защищенных вычислительных систем, определяются следующим образом. Они представлены в порядке нарастания требований с точки зрения обеспечения безопасности ЭВМ.

1. Класс (D): Минимальная защита
2. Класс (C1): Защита, основанная на разграничении доступа (DAC)
3. Класс (С2): Защита, основанная на управляемом контроле доступом
4. Класс(B1): Мандатная защита, основанная на присваивании меток объектам и субъектам, находящимся под контролем ТСВ
5. Класс (B2): Структурированная защита
6. Класс (ВЗ): Домены безопасности
7. Класс (A1): Верифицированный проект

***FIPS 140-2 "Требования безопасности для криптографических модулей"***

В федеральном стандарте США FIPS 140-2 "Требования безопасности для криптографических модулей" под криптографическим модулем понимается набор аппаратных и/или программных (в том числе встроенных) компонентов, реализующих утвержденные функции безопасности (включая криптографические алгоритмы, генерацию и распределение криптографических ключей, аутентификацию) и заключенных в пределах явно определенного, непрерывного периметра.

В стандарте FIPS 140-2 рассматриваются криптографические модули, предназначенные для защиты информации ограниченного доступа, не являющейся секретной. То есть речь идет о промышленных изделиях, представляющих интерес для основной массы организаций. Наличие подобного модуля — необходимое условие обеспечения защищенности сколько-нибудь развитой информационной системы; однако, чтобы выполнять предназначенную ему роль, сам модуль также нуждается в защите, как собственными средствами, так и средствами окружения (например, операционной системы).

***Стандарт шифрования DES***

Также к стандартам информационной безопасности США относится алгоритм шифрования DES, который был разработан в 1970-х годах, и который базируется на алгоритме DEA.

Исходные идеи алгоритма шифрования данных DEA (data encryption algorithm) были предложены компанией IBM еще в 1960-х годах и базировались на идеях, описанных Клодом Шенноном в 1940-х годах. Первоначально эта методика шифрования называлась lucifer (разработчик Хорст Фейштель), название dea она получила лишь в 1976 году. Lucifer был первым блочным алгоритмом шифрования, он использовал блоки размером 128 бит и 128-битовый ключ. По существу этот алгоритм являлся прототипом DEA.

## **Стеганография и ее применение в информационной безопасности**

Задача надежной защиты информации от несанкционированного доступа является одной из древнейших и не решенных до настоящего времени проблем. Способы и методы скрытия секретных сообщений известны с давних времен, причем, данная сфера человеческой деятельности получила название **стеганография.** Это слово происходит от греческих слов steganos (секрет, тайна) и graphy (запись) и, таким образом, означает буквально “тайнопись”, хотя методы стеганографии появились, вероятно, раньше, чем появилась сама письменность (первоначально использовались условные знаки и обозначения).

Компьютерные технологии придали новый импульс развитию и совершенствованию стеганографии, появилось новое направление в области защиты информации — ***компьютерная стеганография*** (КС).

К. Шеннон дал нам общую теорию тайнописи, которая является базисом стеганографии как науки. В современной компьютерной стеганографии существует два основных типа файлов: сообщение - файл, который предназначен для скрытия, и контейнер - файл, который может быть использован для скрытия в нем сообщения. При этом контейнеры бывают двух типов. Контейнер-оригинал (или “Пустой” контейнер) -это контейнер, который не содержит скрытой информации. Контейнер-результат (или “Заполненный” контейнер) - это контейнер, который содержит скрытую информацию. Под ключом понимается секретный элемент, который определяет порядок занесения сообщения в контейнер.

Основными положениями современной компьютерной стеганографии являются следующие:

1. Методы скрытия должны обеспечивать ***аутентичность и целостность*** файла.
2. Предполагается, что противнику полностью известны возможные стеганографии-ческие методы.
3. Безопасность методов основывается на ***сохранении*** стеганографическим преобразованием основных ***свойств*** открыто передаваемого файла при внесении в него секретного сообщения и некоторой неизвестной противнику информации - ключа.
4. Даже если факт скрытия сообщения стал известен противнику через сообщника, извлечение самого секретного сообщения представляет сложную вычислительную задачу.

В связи с возрастанием роли глобальных компьютерных сетей становится все более важным значение стеганографии. Анализ информационных источников компьютерной сети Internet позволяет вделать вывод, что в настоящее время стеганографические системы активно используются для решения следующих основных задач:

1. Защита конфиденциальной информации от несанкционированного доступа;
2. Преодоление систем мониторинга и управления сетевыми ресурсами;
3. Камуфлирования программного обеспечения;
4. Защита авторского права на некоторые виды интеллектуальной собственности.

В настоящее время методы компьютерной стеганографии развиваются по двум основным направлениям:

1. Методы, основанные на использовании специальных свойств компьютерных форматов;
2. Методы, основанные на избыточности аудио и визуальной информации.

Анализ тенденций развития КС показывает, что в ближайшие годы интерес к развитию методов КС будет усиливаться всё больше и больше. Предпосылки к этому уже сформировались сегодня. В частности, общеизвестно, что актуальность проблемы информационной безопасности постоянно растет и стимулирует поиск новых методов защиты информации (ЗИ).

Компьютерная стеганография - компьютерная защита информации.

## **Классы информационной безопасности**

Сама оценка безопасности основывается, как уже упоминалось, на иерарархической классификации. В оригинальном тексте каждый класс каждого уровня описывается с нуля, т.е. наследуемые требования с более низких классов каждый раз повторяются. Для сокращения далее приведены лишь различия, появляющиеся по возрастанию уровня «доверяемости». Всего введены четыре уровня доверия - D, C, B и A, которые подразделяются на классы. Классов безопасности всего шесть - C1, C2, B1, B2, B3, A1 (перечислены в порядке ужесточения требований).

Уровень D.

Данный уровень предназначен для систем, признанных неудовлетворительными - «заваливших экзамен».

Уровень C.

Иначе - произвольное управление доступом.

**Класс C1**

Политика безопасности и уровень гарантированности для данного класса должны удовлетворять следующим важнейшим требованиям:

1. доверенная вычислительная база должна управлять доступом именованных пользователей к именованным объектам;

2. пользователи должны идентифицировать себя, причем аутентификационная информация должна быть защищена от несанкционированного доступа;

3. доверенная вычислительная база должна поддерживать область для собственного выполнения, защищенную от внешних воздействий;

4. должны быть в наличии аппаратные или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов доверенной вычислительной базы;

5. защитные механизмы должны быть протестированы (нет способов обойти или разрушить средства защиты доверенной вычислительной базы);

6. должны быть описаны подход к безопасности и его применение при реализации доверенной вычислительной базы.

Примеры продуктов: некоторые старые версии UNIX , IBM RACF.

**Класс C2**

(в дополнение к C1):

1. права доступа должны гранулироваться с точностью до пользователя. Все объекты должны подвергаться контролю доступа.

2. при выделении хранимого объекта из пула ресурсов доверенной вычислительной базы необходимо ликвидировать все следы его использования.

3. каждый пользователь системы должен уникальным образом идентифицироваться. Каждое регистрируемое действие должно ассоциироваться с конкретным пользователем.

4. доверенная вычислительная база должна создавать, поддерживать и защищать журнал регистрационной информации, относящейся к доступу к объектам, контролируемым базой.

5. тестирование должно подтвердить отсутствие очевидных недостатков в механизмах изоляции ресурсов и защиты регистрационной информации.

Примеры продуктов: практически все ныне распространенные ОС и БД -

Windows NT (а значит сюда можно отнести и все его потомки вплоть до Vista), ещё сюда бы попали все современные UNIX-системы, так же DEC VMS, IBM OS/400, Novell NetWare 4.11, Oracle 7, DG AOS/VS II.

Уровень B.

Также именуется - принудительное управление доступом.

**Класс B1**

(в дополнение к C2):

1. доверенная вычислительная база должна управлять метками безопасности, ассоциируемыми с каждым субъектом и хранимым объектом.

2. доверенная вычислительная база должна обеспечить реализацию принудительного управления доступом всех субъектов ко всем хранимым объектам.

3. доверенная вычислительная база должна обеспечивать взаимную изоляцию процессов путем разделения их адресных пространств.

4. группа специалистов, полностью понимающих реализацию доверенной вычислительной базы, должна подвергнуть описание архитектуры, исходные и объектные коды тщательному анализу и тестированию.

5. должна существовать неформальная или формальная модель политики безопасности, поддерживаемой доверенной вычислительной базой.

Примеры продуктов: сюда относятся гораздо более специализированные ОСи - HP-UX BLS, Cray Research Trusted Unicos 8.0, Digital SEVMS, Harris CS/SX, SGI Trusted IRIX.

**Класс B2**

(в дополнение к B1):

1. снабжаться метками должны все ресурсы системы (например, ПЗУ), прямо или косвенно доступные субъектам.

2. к доверенной вычислительной базе должен поддерживаться доверенный коммуникационный путь для пользователя, выполняющего операции начальной идентификации и аутентификации.

3. должна быть предусмотрена возможность регистрации событий, связанных с организацией тайных каналов обмена с памятью.

4. доверенная вычислительная база должна быть внутренне структурирована на хорошо определенные, относительно независимые модули.

5. системный архитектор должен тщательно проанализировать возможности организации тайных каналов обмена с памятью и оценить максимальную пропускную способность каждого выявленного канала.

6. должна быть продемонстрирована относительная устойчивость доверенной вычислительной базы к попыткам проникновения.

7. модель политики безопасности должна быть формальной. Для доверенной вычислительной базы должны существовать описательные спецификации верхнего уровня, точно и полно определяющие ее интерфейс.

8. в процессе разработки и сопровождения доверенной вычислительной базы должна использоваться система конфигурационного управления, обеспечивающая контроль изменений в описательных спецификациях верхнего уровня, иных архитектурных данных, реализационной документации, исходных текстах, работающей версии объектного кода, тестовых данных и документации.

9. тесты должны подтверждать действенность мер по уменьшению пропускной способности тайных каналов передачи информации.

Примеры продуктов: Honeywell Multics (знаменитый предок UNIX),

Cryptek VSLAN, Trusted XENIX.

**Класс B3**

(в дополнение к B2):

1. для произвольного управления доступом должны обязательно использоваться списки управления доступом с указанием разрешенных режимов.

2. должна быть предусмотрена возможность регистрации появления или накопления событий, несущих угрозу политике безопасности системы. Администратор безопасности должен немедленно извещаться о попытках нарушения политики безопасности, а система, в случае продолжения попыток, должна пресекать их наименее болезненным способом.

3. доверенная вычислительная база должна быть спроектирована и структурирована таким образом, чтобы использовать полный и концептуально простой защитный механизм с точно определенной семантикой.

4. процедура анализа должна быть выполнена для временных тайных каналов.

5. должна быть специфицирована роль администратора безопасности. Получить права администратора безопасности можно только после выполнения явных, протоколируемых действий.

6. должны существовать процедуры и/или механизмы, позволяющие произвести восстановление после сбоя или иного нарушения работы без ослабления защиты.

7. должна быть продемонстрирована устойчивость доверенной вычислительной базы к попыткам проникновения.

Примеры продуктов: единственная система -

Getronics/Wang Federal XTS-300.

Уровень A.

Носит название - верифицируемая безопасность.

**Класс A1**

(в дополнение к B3):

1. тестирование должно продемонстрировать, что реализация доверенной вычислительной базы соответствует формальным спецификациям верхнего уровня.

2. помимо описательных, должны быть представлены формальные спецификации верхнего уровня. Необходимо использовать современные методы формальной спецификации и верификации систем.

3. механизм конфигурационного управления должен распространяться на весь жизненный цикл(Life Cycle) и все компоненты системы, имеющие отношение к обеспечению безопасности.

4. должно быть описано соответствие между формальными спецификациями верхнего уровня и исходными текстами.

Примеры продуктов: Boeing MLS LAN (для создания надежных самолетов нужна надежная сеть), Gemini Trusted Network Processor, Honeywell SCOMP.

Существуют классы такие, как Класс C1, Класс C2, Класс B1, Класс B2, Класс B3, Класс A1.

## **Информационная безопасность Российской Федерации**

Национальные интересы Российской Федерации в информационной сфере и их обеспечение.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать.

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Для достижения этого требуется :повысить эффективность использования информационной инфраструктуры в интересах общественного развития, консолидации российского общества, духовного возрождения многонационального народа Российской Федерации;

Усовершенствовать систему формирования, сохранения и рационального использования информационных ресурсов, составляющих основу научно-технического и духовного потенциала Российской Федерации;

Обеспечить конституционные права и свободы человека и гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом, получать достоверную информацию о состоянии окружающей среды;

обеспечить конституционные права и свободы человека и гражданина на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, на защиту своей чести и своего доброго имени;

Укрепить механизмы правового регулирования отношений в области охраны интеллектуальной собственности, создать условия для соблюдения установленных федеральным законодательством ограничений на доступ к конфиденциальной информации;

Гарантировать свободу массовой информации и запрет цензуры;

не допускать пропаганду и агитацию, которые способствуют разжиганию социальной, расовой, национальной или религиозной ненависти и вражды;

Обеспечить запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и другой информации, доступ к которой ограничен федеральным законодательством.

Вторая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Для достижения этого требуется:

укреплять государственные средства массовой информации, расширять их возможности по своевременному доведению достоверной информации до российских и иностранных граждан;

Интенсифицировать формирование открытых государственных информационных ресурсов, повысить эффективность их хозяйственного использования.

Третья составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности. Для достижения этого требуется: развивать и совершенствовать инфраструктуру единого информационного пространства Российской Федерации.

Развивать отечественную индустрию информационных услуг и повышать эффективность использования государственных информационных ресурсов; Развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем. Обеспечить государственную поддержку отечественных фундаментальных и прикладных исследований, разработок в сферах информатизации, телекоммуникации и связи. Четвертая составляющая национальных интересов Российской Федерации в информационной сфере включает в себя защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России. В этих целях необходимо: повысить безопасность информационных систем, включая сети связи, прежде всего безопасность первичных сетей связи и информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер. Сферы хозяйственной деятельности, а также систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами.

Интенсифицировать развитие отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью; обеспечить защиту сведений, составляющих государственную тайну. Расширять международное сотрудничество Российской Федерации в области развития и безопасного использования информационных ресурсов, противодействия угрозе развязывания противоборства в информационной сфере.

Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению

За последние годы в Российской Федерации реализован комплекс мер по совершенствованию обеспечения ее информационной безопасности.

Начато формирование базы правового обеспечения информационной безопасности. Приняты Закон Российской Федерации "О государственной тайне", Основы законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах, федеральные законы "Об информации, информатизации и защите информации", "Об участии в международном информационном обмене", ряд других законов, развернута работа по созданию механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.

Осуществлены мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, на предприятиях, в учреждениях и организациях независимо от формы собственности. Развернуты работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти. Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют государственная система защиты информации, система защиты государственной тайны, системы лицензирования деятельности в области защиты государственной тайны и системы сертификации средств защиты информации. Вместе с тем анализ состояния информационной безопасности Российской Федерации показывает, что ее уровень не в полной мере соответствует потребностям общества и государства. Современные условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение.

Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере приводят к серьезным негативным последствиям. Так, недостаточность нормативного правового регулирования отношений в области реализации возможностей конституционных ограничений свободы массовой информации в интересах защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороноспособности страны и безопасности государства существенно затрудняет поддержание необходимого баланса интересов личности, общества и государства в информационной сфере. Несовершенное нормативное правовое регулирование отношений в области массовой информации затрудняет формирование на территории Российской Федерации конкурентоспособных российских информационных агентств и средств массовой информации. Необеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.

Закрепленные в Конституции Российской Федерации права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки практически не имеют достаточного правового, организационного и технического обеспечения. Неудовлетворительно организована защита собираемых федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления данных о физических лицах (персональных данных). Нет четкости при проведении государственной политики в области формирования российского информационного пространства, развития системы массовой информации, организации международного информационного обмена и интеграции информационного пространства России в мировое информационное пространство, что создает условия для вытеснения российских информационных агентств, средств массовой информации с внутреннего информационного рынка и деформации структуры международного информационного обмена. Недостаточна государственная поддержка деятельности российских информационных агентств по продвижению их продукции на зарубежный информационный рынок. Ухудшается ситуация с обеспечением сохранности сведений, составляющих государственную тайну.

Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов. Отставание отечественных информационных технологий вынуждает федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации и органы местного самоуправления при создании информационных систем идти по пути закупок импортной техники и привлечения иностранных фирм, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно-телекоммуникационных систем, интеграцией отечественных информационных систем и международных информационных систем возросли угрозы применения "информационного оружия" против информационной инфраструктуры России. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании. Недостаточное внимание уделяется развитию средств космической разведки и радиоэлектронной борьбы.

Сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательного решения таких задач, как: разработка основных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации, а также мероприятий и механизмов, связанных с реализацией этой политики; развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Российской Федерации, а также системы противодействия этим угрозам; разработка федеральных целевых программ обеспечения информационной безопасности Российской Федерации; разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации, а также сертификации этих систем и средств; совершенствование нормативной правовой базы обеспечения информационной безопасности Российской Федерации, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации; установление ответственности должностных лиц федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности; координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, предприятий, учреждений и организаций независимо от формы собственности в области обеспечения информационной безопасности Российской Федерации. Развитие научно-практических основ обеспечения информационной безопасности Российской Федерации с учетом современной геополитической ситуации, условий политического и социально-экономического развития России и реальности угроз применения "информационного оружия".

Разработка и создание механизмов формирования и реализации государственной информационной политики России. Разработка методов повышения эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации; обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность, и в первую очередь в области создания специализированной вычислительной техники для образцов вооружения и военной техники. Разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами; развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны. Создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время; расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи; обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем; создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

Общие методы обеспечения информационной безопасности Российской Федерации

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на правовые, организационно-технические и экономические.

К правовым методам обеспечения информационной безопасности Российской Федерации относится разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности Российской Федерации. Наиболее важными направлениями этой деятельности являются: внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности, в целях создания и совершенствования системы обеспечения информационной безопасности Российской Федерации, устранения внутренних противоречий в федеральном законодательстве противоречий, связанных с международными соглашениями, к которым присоединилась Российская Федерация, и противоречий между федеральными законодательными актами и законодательными актами субъектов Российской Федерации. А также в целях конкретизации правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности Российской Федерации; законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан.

Разработка и принятие нормативных правовых актов Российской Федерации, устанавливающих ответственность юридических и физических лиц за несанкционированный доступ к информации, ее противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверной информации, противоправное раскрытие конфиденциальной информации, использование в преступных и корыстных целях служебной информации или информации, содержащей коммерческую тайну; уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов, а также инвесторов при привлечении иностранных инвестиций для развития информационной инфраструктуры России; законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи; определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций; создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.

Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются: создание и совершенствование системы обеспечения информационной безопасности Российской Федерации; усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере. Разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения. Создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи; выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации. Сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации; совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности; контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации; формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя: разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования; совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.

Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности. Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

**Приложение**

Законы, регулирующие информационную безопасность:

* "О федеральных органах правительственной связи и информации" от 19.02.92 № 4524-1;
* "О безопасности" от 05.03.92 № 2446-1;
* "О правовой охране программ для электронно-вычислительных машин и баз данных" от 23.09.92 № 3523-1;
* "О правовой охране топологий интегральных микросхем" от 23.09.92 № 3526-1;
* "О сертификации продукции и услуг" от 10.06.93 № 5151-1;
* "О стандартизации" от 10.06.93 № 5154-1;
* "Об архивном фонде Российской Федерации и архивах" от 07.07.93 № 5341-1;
* "О государственной тайне" от 21.07.93 № 485-1;
* "О связи" от 16.02.95 № 15-ФЗ;
* "Об информации, информатизации и защите информации" от 20.02.95 № 24-ФЗ;
* "Об органах федеральной службы безопасности в Российской федерации" от 03.04.95 № 40-ФЗ;
* "Об оперативно-розыскной деятельности" от 12.08.95 № 144-ФЗ;
* "Об участии в международном информационном обмене" от 04.07.96 № 85-ФЗ;
* "Об электронной цифровой подписи" от 10.01.2002 № 1-ФЗ.

Нормативные правовые акты Президента Российской Федерации:

* "Об основах государственной политики в сфере информатизации" от 20.01.94 № 170;
* "Вопросы межведомственной комиссии по защите государственной тайны" от 20.01.96 № 71;
* "Об утверждении перечня сведений конфиденциального характера" от 06.03.97 № 188;
* "О некоторых вопросах межведомственной комиссии по защите государственной тайны" от 14.06.97 № 594;
* "О перечне сведений, отнесенных к государственной тайне" от 24.01.98 № 61;
* "Вопросы Государственной технической комиссии при Президенте Российской Федерации" от 19.02.99 № 212;
* "О концепции национальной безопасности Российской Федерации" от 10.01.2000 N 24;
* "Об утверждении перечня должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне" от 17.01.2000 N 6-рп;
* Доктрина информационной безопасности Российской Федерации от 09.09.2000 № ПР 1895.

Нормативные правовые акты Правительства Российской Федерации:

* "Об установлении порядка рассекречивания и продления сроков засекречивания архивных документов Правительства СССР" от 20.02.95 N 170;
* "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны" от 15.04.95 N 333;
* "О сертификации средств защиты информации" от 26.06.95 N 608;
* "Об утверждении правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности" 04.09.95 N 870;
* "О подготовке к передаче сведений, составляющих государственную тайну, другим государствам" от 02.08.97 N 973;
* "О лицензировании отдельных видов деятельности" от 11.04.00 N 326.http://www.infosecurity.ru/\_site/content/laws/akt15.zip

Руководящие документы Гостехкомиссии России:

* Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации;
* Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники;
* Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;
* Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации;
* Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации;
* Защита информации. Специальные защитные знаки. Классификация и общие требования;
* Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.

### **ВЫВОД**

Самыми частыми и самыми опасными, с точки зрения размера ущерба, являются непреднамеренные ошибки пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы. Иногда такие ошибки являются угрозами: неправильно введенные данные, ошибка в программе, а иногда они создают слабости, которыми могут воспользоваться злоумышленники - таковы обычно ошибки администрирования. Согласно исследованиям, 65% потерь - следствие непреднамеренных ошибок. Пожары и наводнения можно считать пустяками по сравнению с безграмотностью и невнимательностью. Очевидно, самым радикальным способом борьбы с непреднамеренными ошибками является максимальная автоматизация и строгий контроль за правильностью совершаемых действий.

На втором месте по размерам ущерба располагаются кражи и подлоги. Согласно имеющимся данным, в 1992 году в результате подобных противоправных действий с использованием ПК американским организациям был нанесен суммарный ущерб в размере 882 млн. долл. Можно предположить, что подлинный ущерб намного больше, поскольку многие организации по понятным причинам скрывают такие инциденты. В большинстве расследованных случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и защитными мерами. Это еще раз свидетельствует о том, что внутренняя угроза гораздо опаснее внешней.

Весьма опасны так называемые "обиженные сотрудники" - действующие и бывшие. Как правило, их действиями руководит желание нанести вред организации-обидчику, например:

- повредить оборудование;

- встроить логическую бомбу, которая со временем разрушит программы и/или данные;

- ввести неверные данные;

- удалить данные;

- изменить данные.

"Обиженные сотрудники", даже бывшие, знакомы с порядками в организации и способны вредить весьма эффективно. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа к информационным ресурсам аннулировались.

Угрозы, исходящие от окружающей среды, к сожалению, отличаются большим разнообразием. В первую очередь, следует выделить нарушения инфраструктуры: аварии электропитания, временное отсутствие связи, перебои с водоснабжением, гражданские беспорядки и т.п. Опасны, разумеется, стихийные бедствия и техногенные катастрофы. Принято считать, что на долю огня, воды и аналогичных "врагов", среди которых самый опасный - низкое качество электропитания, приходится 13% потерь, нанесенных информационным системам.

Много говорят и пишут о хакерах, но исходящая от них угроза зачастую преувеличивается. Верно, что почти каждый Internet-сервер по несколько раз в день подвергается попыткам проникновения; верно, что иногда такие попытки оказываются удачными; верно, что изредка подобные действия связаны со шпионажем. Однако в целом ущерб от деятельности хакеров по сравнению с другими угрозами представляется не столь уж значительным. Скорее всего, больше пугает фактор непредсказуемости действий людей такого сорта. Представьте себе, что в любой момент к вам в квартиру могут забраться посторонние люди. Даже если они не имеют злого умысла, а зашли просто так, посмотреть, нет ли чего интересного, - приятного в этом мало.

Много говорят и пишут и о программных вирусах. Причем в последнее время говорят уже о вирусах, воздействующих не только на программы и данные, но и на пользователей. Так, в свое время появилось сообщение о жутком вирусе 666, который, выводя каждую секунду на монитор некий 25-й кадр, вызывает у пользователей кровоизлияние в мозг и смерть (впоследствии это сообщение не подтвердилось).

Однако, говоря о "вирусной" угрозе, обратим внимание на следующий факт. Как показали проведенные в США в 1993 году исследования, несмотря на экспоненциальный рост числа известных вирусов, аналогичного роста количества инцидентов, вызванных вирусами, не зарегистрировано. Соблюдение несложных правил компьютерной гигиены сводит риск заражения практически к нулю. Там где работают, а не играют в компьютерные игры (именно это явление приводит к использованию непроверенных на наличие вирусов программ), число зараженных компьютеров составляет лишь доли процента.

Таковы основные угрозы, на долю которых приходится львиная доля урона, наносимого информационным системам. Рассмотрим теперь иерархию защитных мероприятий, способных противостоять угрозам.

Самыми частыми и самыми опасными, с точки зрения размера ущерба, являются непреднамеренные ошибки пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы. От вирусов и других факторов ущерба оказывается меньше.

**ЛИТЕРАТУРА**

1. Закон РФ "О государственной тайне" 2008 г. 32 стр.
2. Закон РФ "Об информации, информатизации и защите информации" 2006г. 24стр.
3. Доктрина информационной безопасности Российской Федерации от 09.09.2000 № ПР 1895. 2004г. 48стр.
4. Словарь терминов Гостехкомиссии при президенте РФ
5. http://prikladnayainformatika.ru/keywords
6. Носов В.А. Вводный курс по дисциплине “Информационная безопасность” 2004г. 50стр.
7. Соколов А.В. «Методы информационной защиты объектов и компьютерных сетей». 2000г. 272стр.
8. Б. Анин «Защита компьютерной информации». 2000г. 384стр.
9. Малюк «Информационная безопасность: концептуальные и методологические основы защиты информации». 2004г. 280стр.
10. Галатенко В.А. «Стандарты информационной безопасности». 2004г. 328стр.
11. П. Ю. Белкин, О. О. Михальский, А. С. Першаков, Д. И. Правиков, В. Г. Проскурин, Г. В. Фоменков «Защита программ и данных». 1999г.
12. http://www.jetinfo.ru/2002/7/1/article1.7.200231.html - Нормативная база анализа защищенности
13. http://www.sbcinfo.ru/articles/doc/gtc\_doc/contents.htm
14. http://counter-terrorism.narod.ru/magazine1/kotenko-8-1.htm - Вопросы ИБ и терроризма
15. http://snoopy.falkor.gen.nz/~rae/des.html - описание алгоритма DES
16. http://markova-ne.narod.ru/infbezop.html - Вопросы ИБ и СМИ
17. http://www.ctta.ru/ - Некоторые проблемы ИБ
18. http://st.ess.ru/steganos.htm - Вопросы стеганографии
19. http://www.infosecurity.ru/\_site/problems.shtml - Суть проблемы Информационной Безопасности
20. http://www.jetinfo.ru/2004/11/3/article3.11.2004.html - Федеральный стандарт США FIPS 140-2