Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования

АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Институт информационных технологий и коммуникаций

Кафедра «Информационная безопасность»

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Курс лекций

для студентов специальности
10.05.03 «Информационная безопасность автоматизированных систем» и направления
10.03.01 «Информационная безопасность»

Астрахань 2015

Составитель: Сибикина И.В., доцент кафедры «Информационная безопасность», Космачева И.М., доцент кафедры «Информационная безопасность».

Рецензент: Попов Г.А., д.т.н., профессор, заведующий кафедрой «Информационная безопасность».

Курс лекций «Основы информационной безопасности» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» и направления 10.03.01 «Информационная безопасность» / АГТУ; Сост.: И.В. Сибикина, И.М. Космачева,. 2015. – 56с.

Дисциплина «Основы информационной безопасности» является базовой при подготовке специалистов в области информационных технологий (IT), информационной безопасности. Дисциплина изучает вопросы национальной безопасности РФ, безопасности информационных ресурсов РФ, классификацию угроз информационной безопасности и их источников, вопросы стандартизации и меры защиты информационной безопасности

Данные учебный материал может быть использован для подготовки студентов к лабораторным занятиям и экзамену, а также рекомендуется к использованию его в качестве учебного пособия при последующем изучении дисциплин, связанных обеспечением информационной безопасности.

Учебное пособие утверждено на заседании кафедры 12 ноября 2015 г., протокол № 3

СОДЕРЖАНИЕ

1. ОСНОВНЫЕ ПОНЯТИЯ И ЗАДАЧИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Рассмотрим основные понятия информационной безопасности.

Информация – сведения (сообщения, данные) независимо от формы их представления».

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Доступ к информации – возможность получения информации и ее использования.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

Документированная информация –информация зафиксированная на материальном носителе путем документирования с реквизитами, позволяющими определить такую информацию.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Защищаемая информация – «информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации».

Согласно закону № 149-ФЗ, информация в зависимости от категории доступа к ней подразделяется на *общедоступную информацию*, а также на информацию, доступ к которой ограничен федеральными законами - *информация ограниченного доступа*.

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. «Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации».

По закону, информация в зависимости от порядка предоставления или распространения подразделяется на информацию:

1. свободно распространяемую;
2. предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
3. подлежащую предоставлению или распространению в соответствии с федеральными законами;

4. ограниченную или запрещенную для распространения в РФ.

Закон РФ «О средствах массовой информации», принятый в 1991 (редакция от 13.07.2015) г., определяет понятие «массовая информация» как предназначенные для неограниченного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы.

Под *средством массовой информации* понимается периодическое печатное издание, сетевое издание, телеканал, радиоканал, телепрограмма, радиопрограмма, видеопрограмма, кинохроникальная программа, иная форма периодического распространения массовой информации под постоянным наименованием

Довольно специфичной информацией являются так называемые «кредитные истории» и «персональные данные», которые рассматриваются специальными законами.

Согласно закону № 149-ФЗ «Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1. обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2. соблюдение конфиденциальности информации ограниченного доступа,
3. реализацию права на доступ к информации».

Понятие «безопасность».

Рассмотрим понятие безопасность.

Вл. Даль: «безопасность – есть отсутствие опасности, сохранность, надежность». Толковый словарь Ожегова С.И. «безопасность – состояние, в котором не угрожает опасность, есть защита от опасности».

1. *Угроза* – совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства [ФЗ «О безопасности» 05.03.1992].

2. *Угроза* – потенциальный источник возникновения ущерба [ГОСТ Р 51898-2002 п. 3.5].

3. *Угроза* – потенциальная причина *инцидента*, который может нанести ущерб системе или организации [ISO/IEC 13335-1:2004].

Инцидент информационной безопасности (information security incident)[ГОСТ ИСО/МЭК 13335-1] – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

В качестве некоторых примеров инцидентов в ГОСТ указаны:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политик или рекомендаций;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои ПО и отказы технических средств;
- нарушение правил доступа.

Нарушение может вызываться либо ошибкой людей, либо неправильным функционированием технических средств, либо природными факторами (например, пожар или наводнение), либо преднамеренными злоумышленными действиями, приводящими к нарушению конфиденциальности, целостности, доступности или неотказуемости.

С инцидентом связано понятие *воздействие* (impact) – результат нежелательного инцидента информационной безопасности.

Говоря об угрозах, часто используется понятие «модели угроз», которая, согласно стандарту СТО БР ИББС 1.0-2006, «включает описание источников угроз, уязвимостей, используемых угрозами, методов и объектов нападений, пригодных для реализации угрозы, типов возможной потери, масштабов потенциального ущерба».

Разберем понятие *«модели угроз»* по составляющим.

Источник угроз – субъект, материальный объект или физическое явление, создающее угрозу безопасности информации.

Для источников угроз – людей – разрабатывается *модель нарушителя*.

В модели нарушителя конкретизируются субъекты, их средства, знания и опыт, с помощью которых они могут реализовать угрозы и нанести ущерб объектам, а также мотивации их действий.

Частным видом нарушителя является злоумышленник.

Злоумышленник – основной субъект угроз, источник противоборства с собственником в борьбе за активы и доходы.

Уязвимость – недостатки или слабые места активов, которые могут быть использованы угрозой [СТО БР ИББС-1.0-2006].

Наличие уязвимости без присутствия угрозы не причиняет ущерба, но все уязвимости должны контролироваться на предмет изменения ситуации.

Угрозы, не имеющие соответствующих уязвимостей, не приводят к ущербу, но должны учитываться.

Ущерб – физическое повреждение или другой вред здоровью людей, имуществу (активам) или окружающей среде. Количественная величина ущерба не всегда поддается оценке. В этих случаях для оценки ущерба может использоваться качественное описание.

Отечественный ГОСТ Р 51898-2002 определяет, что «безопасность – отсутствие недопустимого риска».

Риск – сочетание вероятности нанесения ущерба и тяжести этого ущерба [ГОСТ Р 51898-2002. Аспекты безопасности].

В этом документе [ГОСТ Р 51898-2002] также сказано, что термин «риск» обычно используют только тогда, когда существует возможность негативных последствий, а в некоторых ситуациях риск обусловлен возможностью отклонения от ожидаемого результата или события.

На практике можно встретить различные виды рисков: стратегический риск, ИТ- риск, риск информационной безопасности и другие.

Информационный риск (ИТ-риск) – это опасность возникновения убытков или ущерба в результате применения информационных технологий. ИТ-риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи (М. Мур).

Остаточный риск (residual risk) – риск, остающийся после его обработки.

Анализ риска (risk analysis) – систематический процесс определения величины риска.

Оценка риска (risk assessment) – процесс, объединяющий идентификацию риска, анализ риска и оценивание риска.

Обработка риска (risk treatment) – процесс выбора и осуществления мер по модификации риска.

Обработка риска включает: предотвращение, перенос, снижение и принятие риска. После обработки рисков могут оставаться остаточные риски.

Защитная мера (или мера защиты, контрмера, мера контроля) – мера, используемая для уменьшения риска [ГОСТ Р 51898-2002, ISO/IEC Guide 51].

Базовые защитные меры (baseline controls) – минимальный набор защитных мер, установленный для системы или организации [ГОСТ Р ИСО/МЭК 13335-1]. Они соответствуют базовому уровню безопасности (Baseline Security) – обязательный минимальный уровень защищенности для информационных систем.

Контрмеры базового уровня служат для защиты от стандартного набора наиболее распространенных угроз (вирусы, сбои оборудования, не санкционируемый доступ и т.д.).

В целом средства контроля могут обеспечивать один или несколько из следующих видов защиты:

- предупреждение;
- сдерживание;
- обнаружение;
- снижение;
- восстановление;
- исправление;
- мониторинг и информированность.

Защитные меры (контроли) имеют разветвленную сложную структуру и состоят из организационных и программно-технических мер (или средств) на верхнем уровне. В свою очередь, организационные меры включают законодательные, административные и процедурные меры защиты.

Система обеспечения безопасности - включает силы и средства обеспечения безопасности, которые действуют и используются на основе разработанных заранее и закрепленных некоторым формальным образом принципов и правил (в виде нормативно-правовых актов, ведомственных инструкций, положений и т.п.).

Сущность функционирования системы безопасности заключается в выявлении, прогнозировании, предотвращении, нейтрализации, пресечении, локализации,

устранении, отражении и уничтожении угроз защищаемому объекту, а также формировании условий, благоприятствующих деятельности данного объекта, достижения им своих целей, защиты его интересов.

Система обеспечения безопасности того или иного объекта решает следующие задачи:

1. Своевременное выявление и прогнозирование внешних и внутренних угроз.
2. Осуществление комплекса оперативных и долговременных мер по предупреждению и нейтрализации внутренних и внешних угроз.
3. Создание и поддержание в готовности сил и средств для обеспечения безопасности.
4. Управление силами и средствами обеспечения безопасности в нормальных (повседневных) условиях и при возникновении чрезвычайных ситуаций.
5. Осуществление системы мер по нормальному функционированию объектов безопасности после возникновения чрезвычайных ситуаций.
6. Участие в мероприятиях по обеспечению безопасности за пределами своего объекта в соответствии с договоренностями (соглашениями) внутри корпорации или объединения фирм (предприятий).

«*Система комплексной безопасности*» - это совокупность организационных мероприятий и действий подразделений охраны и служб безопасности организаций и автоматизированных систем по защите информации, направленных на обеспечение установленного режима, порядка и правил поведения, предотвращение, обнаружение и ликвидацию угроз жизни, среде обитания, имуществу и информации, а также поддержание работоспособности технических средств и систем на охраняемом объекте с целью ограничения или предотвращения действий нарушителя для осуществления опасных

несанкционированных операций на объекте, приводящих к частичному или полному нарушению функционирования данного объекта».

В Доктрине информационной безопасности РФ от 2000 г под «информационной безопасностью Российской Федерации» понимается – состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Информационная безопасность автоматизированных систем – область науки и техники, охватывающая совокупность программно-аппаратных, криптографических, технических и организационно-правовых методов и средств обеспечения безопасности информации в автоматизированных системах при ее обработке, хранении и передаче с использованием информационных технологий.

Доступность (availability) – свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта [ИСО/МЭК 7498-2].

Или проще, доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Целостность (integrity) – свойство сохранения правильности и полноты активов [ГОСТ Р ИСО/МЭК 13335-1].

Или целостность – это актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность (confidentiality) – свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса. [ИСО/МЭК 7498-2].

По ГОСТ Р ИСО/МЭК 13335-1:2005 : информационная безопасность (information security) – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки.

Рассмотрим понятие конфиденциальность.

С этим понятием связано понятие «тайна», которое имеет множество производных: государственная тайна, коммерческая тайна, адвокатская тайна, банковская тайна, врачебная тайна, налоговая тайна, нотариальная тайна, персональные данные, личная и семейная тайна, служебная тайна, тайна голосования, тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, тайна следствия и судопроизводства, тайна совещания судей, тайна страхования, тайна усыновления (удочерения), аудиторская тайна и др. (всего около 40).

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Коммерческая тайна – режим конфиденциальной информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

Информационная безопасность включает в себя:

- компьютерную безопасность;
- безопасность информационных систем и процессов;

– безопасность среды для реализации информационных процессов.

Компьютерная безопасность – свойство компьютерной информации, ЭВМ, системы ЭВМ, сети ЭВМ, при котором обеспечивается защита компьютерной информации (данных) от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, копирования, блокирования, а также защита ЭВМ, системы ЭВМ, сети ЭВМ от неправомочного доступа, создания, использования и распространения вредоносных программ, нарушения правил эксплуатации, несанкционированной модификации программ и т.п..

Политика информационной безопасности.

Политика безопасности организации – одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.

Политика безопасности информационно-телекоммуникационных технологий (ICT security policy) – правила, сложившаяся практика, которые определяют, как управлять информацией, защищать и распределять её.[ГОСТ Р 13335-1].

Согласно [ГОСТ Р ИСО/МЭК 17799-2005] политика ИБ должна быть утверждена высшим руководством, издана и доведена до сведения всех сотрудников и соответствующих внешних сторон.

Документ о политике ИБ должен устанавливать ответственность руководства и излагать подход организации к управлению ИБ.

Политика информационной безопасности должна пересматриваться через запланированные промежутки времени или в случае появления существенных изменений в целях обеспечения ее непрерывной стабильности, адекватности и эффективности.

Политика информационной безопасности должна иметь владельца, который утвердил административную ответственность за развитие, пересмотр и оценку политики безопасности.

Пересмотр должен включать возможности оценки для улучшения политики информационной безопасности организации и подход к управлению информационной безопасностью в ответ на изменения в организационной среде, деловой ситуации, юридических условиях или технической среде.

2. ИНТЕРЕСЫ И УГРОЗЫ В ОБЛАСТИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ.

Национальная безопасность РФ - безопасность ее народа как носителя суверенитета (суверенитéт-независимость государства во внешних и верховенство государственной власти во внутренних делах) и источника власти в РФ.

Национальные интересы России - это совокупность сбалансированных интересов личности, общества и государства в различных сферах жизнедеятельности.

В области внутренней и внешней политики государства этими интересами определяются основные цели этой политики, стратегические и текущие задачи.

Национальные интересы обеспечиваются институтами государственной власти, осуществляющими свои функции, в том числе во взаимодействии с действующими на основе Конституции РФ, и законодательства РФ, а также общественными организациями.

Интересы личности - реализация конституционных прав и свобод, обеспечение личной безопасности, повышение качества жизни, физическое, духовное и интеллектуальное развитие гражданина.

Интересы общества - упрочение демократии, создание правового, социального государства, достижение общественного согласия, духовное обновление России.

Интересы государства - незыблемость конституционного строя, суверенитета и территориальной целостности России, политическая, экономическая и социальная стабильность.

Реализация национальных интересов России возможна на основе устойчивого развития экономики.

Национальные интересы во ***внутриполитической сфере*** состоят в сохранении стабильности конституционного строя, институтов государственной власти, в обеспечении гражданского мира и национального согласия, территориальной целостности, единства правового пространства.

Национальные интересы в ***социальной сфере*** заключаются в обеспечении высокого уровня жизни народа.

Национальные интересы в ***духовной сфере*** состоят в сохранении и укреплении нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Национальные интересы в ***международной сфере*** состоят в обеспечении суверенитета, упрочении позиций России, в развитии равноправных и взаимовыгодных отношений со всеми странами и интеграционными объединениями, в соблюдении прав и свобод человека и недопустимости применения при этом двойных стандартов.

Национальные интересы в ***информационной сфере*** состоят в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

Национальные интересы в ***военной сфере*** заключаются в защите ее независимости, суверенитета, государственной и территориальной целостности, в предотвращении военной агрессии против России и ее союзников, в обеспечении условий для мирного, демократического развития государства.

Национальные интересы в ***пограничной сфере*** состоят в создании политических, правовых, организационных и других условий для обеспечения надежной охраны государственной границы РФ, в соблюдении установленных законодательством РФ порядка и правил осуществления экономической и иных видов деятельности в пограничном пространстве РФ.

Национальные интересы в ***экологической сфере*** заключаются в сохранении и оздоровлении окружающей среды.

Составляющие национальных интересов России – это защита личности, общества и государства: от терроризма; от чрезвычайных ситуаций природного и техногенного характера и их последствий; в военное время - от опасностей, возникающих при ведении военных действий или вследствие этих действий.

Достижению национальных интересов препятствуют те или иные угрозы.

Угроза - это совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства, это возможная опасность.

Причины возникновения внутренних и внешних угроз национальной безопасности:

- состояние отечественной экономики,
- несовершенство системы организации государственной власти и гражданского общества;
- криминализация общественных отношений;

– рост организованной преступности и увеличение масштабов терроризма;

– обострение межнациональных и осложнение международных отношений;

– криминализация общественных отношений, складывающихся в процессе реформирования социально-политического устройства и экономической деятельности;

– 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 ;

– отсутствие сильной государственной политики в социальной сфере;

– снижение духовно-нравственного потенциала общества.

Последствия:

– ослабление правового контроля за ситуацией в стране;

– сращивание отдельных элементов исполнительной и законодательной власти с криминальными структурами;

– проникновение криминальных структур в сферу управления банковским бизнесом, крупными производствами, торговыми организациями и товаропроводящими сетями.

Борьба с организованной преступностью и коррупцией имеет не только правовой, но и политический характер.

Угрозы национальной безопасности России в социальной сфере:

- расслоение общества на узкий круг богатых и преобладающую массу малообеспеченных граждан;
- увеличение удельного веса населения, живущего за чертой бедности;
- рост безработицы;
- кризис систем здравоохранения и социальной защиты населения;
- рост потребления алкоголя и наркотических веществ;
- 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.

Угрозы в международной сфере

- стремление отдельных государств и межгосударственных объединений принизить роль существующих механизмов обеспечения международной безопасности, прежде всего ООН (организация объединённых наций) и ОБСЕ (организация безопасности стран Европы);
- опасность ослабления политического, экономического и военного влияния России в мире;
- укрепление военно-политических блоков и союзов, расширение НАТО на восток;
- возможность появления вблизи от российских границ иностранных военных баз и крупных воинских контингентов;
- распространение оружия массового уничтожения;

- ослабление интеграционных процессов в СНГ;
- возникновение и эскалация (постепенное увеличение, усиление) конфликтов вблизи государственной границы РФ и внешних границ государств СНГ
- притязания на территорию РФ.
- попытки других государств противодействовать укреплению России как одного из центров влияния в мире.
- Помехи в реализации национальных интересов РФ и ослаблении ее позиции в Европе, на Ближнем Востоке, в Закавказье, Центральной Азии и Азиатско-Тихоокеанском регионе.
- Международный терроризм.

Угрозы национальной безопасности РФ в информационной сфере.

- стремление ряда стран к доминированию в мировом информационном пространстве;
- вытеснение 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;
- нарушение сохранности информационных ресурсов и получение несанкционированного доступа к ним.
- стремление ряда стран к доминированию в мировом информационном пространстве;
- вытеснение 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;
- нарушение сохранности информационных ресурсов и получение несанкционированного доступа к ним.

Угрозы в военной сфере

- Применение НАТО (North Atlantic Treaty Organization –организация Северо-атлантического договора - союз государств с целью совместных действий для решения общих политических, экономических и военных задач*)* военных действий вне зоны ответственности блока и без санкции Совета Безопасности ООН приводит к угрозе дестабилизации всей стратегической обстановки в мире.
- технологический отрыв ряда ведущих держав и наращивание их возможностей по созданию вооружений и военной техники нового поколения создающие предпосылки гонки вооружений;
- коренное изменения форм и способов ведения военных действий.
- активная деятельность на территории РФ иностранных специальных служб и используемых ими организаций.
- угрозы в военной сфере возникают
- при недостаточном финансирование национальной обороны и несовершенстве нормативной правовой базы;
- при низком уровне оперативной и боевой подготовки Вооруженных сил, других войск, воинских формирований и органов;
- при снижении укомплектованности войск (сил) современным вооружением, военной и специальной техникой.

Угрозы национальной безопасности и интересам РФ в пограничной сфере :

- экономическая, демографическая и культурно-религиозная экспансия сопредельных государств на российскую территорию;
- активизация деятельности трансграничной организованной преступности, а также зарубежных террористических организаций.

Угрозы в экологической сфере

Угрозы ухудшения экологической ситуации в РФ и истощения ее природных ресурсов от состояния экономики и осознания обществом важности этих проблем.

Источники угроз в экологической сфере:

- развитие топливно-энергетических отраслей промышленности;
- неразвитость законодательной основы природоохранной деятельности;
- отсутствие или ограниченное использования природосберегающих технологий;
- низкая экологическая культура
- использование территории России для 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.

Важнейшие задачи обеспечения ИБ в РФ

- реализация конституционных прав и свобод граждан РФ в сфере информационной деятельности;
- совершенствование и защита отечественной информационной инфраструктуры, интеграция России в мировое информационное пространство;

– противодействие угрозе развязывания противоборства в информационной сфере.

Основа системы обеспечения национальной безопасности РФ составляют органы, силы и средства обеспечения национальной безопасности, осуществляющие меры политического, правового, организационного, экономического, военного и иного характера, направленные на обеспечение безопасности личности, общества и государства.

Полномочия органов и сил обеспечения национальной безопасности РФ, их состав, принципы и порядок действий определяются соответствующими законодательными актами РФ.

3. ВЛИЯНИЕ ПРОЦЕССОВ ИНФОРМАТИЗАЦИИ ОБЩЕСТВА НА СОСТАВЛЯЮЩИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ.

По мере развития и усложнения средств, методов и форм автоматизации процессов обработки информации, повышается зависимость общества от степени безопасности используемых им информационных технологий, от которых зависит благополучие, а иногда и жизнь многих людей.

Актуальность и важность проблемы обеспечения безопасности информационных технологий обусловлены такими причинами, как:

– увеличение вычислительной мощности компьютеров при одновременном упрощении их эксплуатации;
– увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и других средств автоматизации;
– сосредоточение в единых базах данных информации различного назначения и различной принадлежности;

- высокие темпы роста парка персональных компьютеров, находящихся в эксплуатации в самых разных сферах деятельности;
- расширение круга пользователей, имеющих непосредственный доступ к вычислительным ресурсам и массивам данных;
- развитие программных средств, не удовлетворяющих даже минимальным требованиям безопасности;
- распространение сетевых технологий и объединение локальных сетей в глобальные;
- развитие глобальной сети Интернет, практически не препятствующей нарушениям безопасности систем обработки информации во всем мире.

К основным понятиям в области обеспечения ИБ относятся «информация», «информационная сфера», «информационная безопасность».

Системная задача обеспечения информационной безопасности, с одной стороны, и конкретные задачи технической, юридической и других подсистем, с другой - имеют разные предметы действий. Поэтому система информационной безопасности есть не простая сумма различных (правовых, организационных, технических) компонентов. Требуется системный и комплексный подходы.

Формирование системы, обеспечивающей информационную безопасность объекта, требует обычно решения ряда задач, связанных с формализованной информацией - информацией в форме документов или обменных сигналов технических систем.

В этих случаях вполне применимы методы математической теории информации и удается сформировать весьма точные значения параметров, характеризующих защищенность системы.

Однако для полной оценки защищенности эти параметры приходится сопоставлять с оценками для не поддающейся непосредственному доступу информации воздействия.

Например, можно достаточно достоверно оценить вероятность восстановления отдельного слова в перехваченном речевом сообщении (допустим 5 или 12 %). После этого возникает вопрос, какая вероятность допустима.

Получить такую оценку можно только экспертным путем. Попытки применить здесь методы теории информации создают некоторое наукообразие, но, по сути, неэффективны, так как результат полностью определяется исходными допущениями, формируемыми фактически произвольно.

Информационная сфера – это совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Она активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности РФ. Национальная безопасность РФ существенно зависит от обеспечения ИБ, и в ходе технического прогресса эта зависимость будет возрастать.

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

Государственная политика обеспечения ИБ РФ основывается на следующих основных принципах:

- соблюдении Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного

права при осуществлении деятельности по обеспечению ИБ РФ;

- открытости в реализации функций федеральных органов государственной власти, органов государственной власти субъектов РФ и общественных объединений, предусматривающей информирование общества об их деятельности с учетом ограничений, установленных законодательством РФ;
- правовое равенство всех участников процесса информационного взаимодействия, вне зависимости от их статуса (политического, социального и экономического), основывающемся на конституционном праве граждан на свободный поиск, получение, передачу, производство и распространение информации любым законным способом;
- - приоритетное развитии отечественных современных информационных и телекоммуникационных технологий, производство технических и программных средств, способных обеспечить совершенствование национальных телекоммуникационных сетей, их подключение к глобальным информационным сетям в целях соблюдения жизненно важных интересов РФ.

Национальные интересы в информационной сфере.

Доктрина ИБ РФ дает две классификации национальных интересов в информационной сфере:

классификация по принадлежности интересов;
классификация по важности интересов

В соответствии с *первой классификацией* национальные интересы -это совокупность интересов личности, интересов общества и интересов государства.

Интересы личности:

- Реализация конституционных прав на доступ к информации;

- Использование информации в интересах осуществления не запрещённой законом деятельности;
- Физическое, духовное и интеллектуальное развитие;
- Защита информации, обеспечивающей личную безопасность.

Интересы общества

- Обеспечение интересов личности в информационной сфере;
- Упрочение демократии, создание правового, социального государства;
- Достижение и поддержание общественного согласия;
- Духовное обновление России.

Интересы государства

- Гармоничное развитие российской информационной инфраструктуры;
- Реализация конституционных прав гражданина в области получение информации и пользования ею;
- Незыблемость конституционного строя, суверенитета и территориальной целостности России;
- Политическая, экономическая и социальная стабильность;
- Обеспечение законности и поддержание правопорядка;
- Развитие равноправного и взаимовыгодного международного сотрудничесства

Вторая классификация национальных интересов в информационной сфере связана с оценкой их важности. В рамках этой классификации выделяют четыре основные составляющие национальных интересов РФ в информационной сфере:

1. 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.

2. Информационное обеспечение государственной политики РФ, связанное с доведением до российской и международной общественности достоверной информации о государственной политике РФ, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

3. Развитие 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.

4. Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Угрозы национальным интересам РФ в информационной сфере подразделяются на следующие виды:

1. угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России:

- принятие федеральными органами государственной власти нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

- создание монополий на формирование, получение и распространение информации в РФ, в том числе с использованием телекоммуникационных систем;
- противодействие, в том числе со стороны криминальных структур, реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;
- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации;
- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание;
- неисполнение федеральными органами государственной власти, органами государственной власти субъектов РФ, органами местного самоуправления, организациями и гражданами требований федерального законодательства, регулирующего отношения в информационной сфере;
- ограничение доступа граждан к открытым информационным ресурсам федеральных органов гос. власти, к открытым архивным материалам, к другой открытой социально значимой информации;
- дезорганизация и разрушение системы накопления и сохранения культурных ценностей, включая архивы;
- нарушение конституционных прав и свобод человека и гражданина в области массовой информации;
- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;

- девальвация духовных ценностей, пропаганда образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе;
- снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов для внедрения и использования новейших технологий, в том числе информационных;
- манипулирование информацией (дезинформация, сокрытие или искажение информации).

2. Угрозы информационному обеспечению государственной политики РФ.

- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
- блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;
- низкая эффективность информационного обеспечения государственной политики РФ вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики;
- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

3. Угрозы развитию отечественной индустрии информации, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, обеспечению накопления, сохранности и использования отечественных информационных ресурсов.

- противодействие доступу РФ к информационным технологиям, равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг;
- закупка органами государственной власти импортных средств информатизации, телекоммуникации и связи при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;
- вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;
- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- утечка информации по техническим каналам;
- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов

государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;
- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

4. угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;
- несанкционированный доступ к информации, находящейся в банках и базах данных;
- нарушение законных ограничений на распространение информации.

4. ИСТОЧНИКИ УГРОЗ ИБ РФ. ГОСУДАРСТВЕННАЯ ИНФОРМАЦИОННАЯ ПОЛИТИКА РФ. ИНФОРМАЦИОННЫЕ РЕСУРСЫ СОВРЕМЕННОГО ОБЩЕСТВА

Источники угроз ИБ РФ подразделяются на внешние и внутренние.

К ***внешним*** относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов РФ в информационной сфере;
- ущемление интересов России в мировом информационном пространстве

- вытеснение РФ с внешнего и внутреннего информационных рынков;
- деятельность международных террористических организаций;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- увеличение технологического отрыва иностранных государств и их противодействие созданию конкурентоспособных российских информационных технологий;
- деятельность технических и иных средств (видов) разведки иностранных государств;
- разработка рядом государств концепций информационных войн.

К ***внутренним*** источникам относятся:

- критическое состояние отечественных отраслей промышленности;
- неблагоприятная криминогенная обстановка:
- сращивание государственных и криминальных структур в информационной сфере;
- получение криминальными структурами доступа к конфиденциальной информации;
- усиление влияния организованной преступности на жизнь общества;
- снижение степени защищенности законных интересов граждан, общества и государства в информационной сфере;
- ошибки при формировании и реализации единой государственной политики в области обеспечения ИБ;
- ошибки нормативно-правовой базы, в информационной сфере, недостаточная правоприменительная практика;
- неразвитость институтов гражданского общества и недостаточный государственный. контроль за развитием информационного рынка;

- недостаточное финансирование мероприятий по обеспечению информационной безопасности РФ;
- недостаточная экономическая мощь государства;
- снижение эффективности образования и воспитания, отсутствие квалифицированных кадров в области обеспечения ИБ;
- пассивность органов государственной власти, в информировании общества о своей деятельности, в принимаемых решениях, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов РФ и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

5. ГОСУДАРСТВЕННАЯ ИНФОРМАЦИОННАЯ ПОЛИТИКА РФ. ОСНОВНЫЕ ПОЛОЖЕНИЯ.

Государственная политика обеспечения ИБ РФ определяет основные направления деятельности органов государственной власти в этой области, их обязанности по защите интересов РФ в информационной сфере в рамках их деятельности и базируется на соблюдении баланса интересов личности, общества и государства в информационной сфере.

Государство в процессе реализации своих функций по обеспечению информационной безопасности РФ реализует следующие функции:

1. проводит анализ и прогнозирование угроз ИБ РФ, разрабатывает меры по ее обеспечению;
2. организует работу законодательных (представительных) и исполнительных органов государственной власти РФ по реализации комплекса мер, направленных на предотвращениеугроз информационной безопасности РФ;

3. поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;
4. контролирует разработку, создание, развитие использование, экспорт и импорт средств защиты информации посредством их сертификации и лицензирования деятельности в области защиты информации;
5. принимает меры по защите внутреннего рынка от проникновения на него некачественных средств информатизации и информационных продуктов;
6. способствует предоставлению физическим и юридическим лицам доступа к мировым информационным ресурсам, глобальным информационным сетям;
7. формулирует и реализует государственную информационную политику России;
8. организует разработку федеральной программы обеспечения информационной безопасности РФ, объединяющей усилия государственных и негосударственных организаций в данной области;
9. способствует вхождению России в мировое информационное сообщество на условиях равноправного партнерства.

Мероприятия по реализации государственной. политики обеспечения ИБ.

1. разработка и внедрение правовых норм, регулирующих отношения в информационной сфере, а также подготовка концепции правового обеспечения информационной безопасности РФ;
2. разработка и реализация механизмов повышения эффективности государственного руководства деятельностью государственных средств массовой

информации, осуществления государственной информационной политики;

3. создание федеральных программ, для формирования общедоступных архивов информационных ресурсов органов гос. власти, повышение правовой культуры и компьютерной грамотности граждан, развитие инфраструктуры единого информационного пространства России, комплексное противодействие угрозам информационной войны и т.д.
4. развитие системы подготовки кадров в области обеспечения ИБ РФ;
5. гармонизация отечественных стандартов в области информатизации и обеспечения ИБ АСУ, информационных и телекоммуникационных систем общего и специального назначения.

Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации:

Президент РФ, Совет Федерации Федерального Собрания РФ, Государственная Дума Федерального Собрания РФ, Правительство РФ, Совет Безопасности РФ, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом РФ и Правительством РФ, органы исполнительной власти субъектов РФ, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с законодательством РФ участие в решении задач обеспечения информационной безопасности РФ.

6. ИНФОРМАЦИОННЫЕ РЕСУРСЫ СОВРЕМЕННОГО ОБЩЕСТВА.

Информационные ресурсы - вся накопленная информация об окружающей нас действительности, как на материальных носителях так и в любой другой форме, обеспечивающей ее передачу между потребителями для решения разных задач.

Ресурс это информация, в том числе и недостоверная, т.е.:

1) представленная сомнительными фактами;
2) ложными положениями;
3) неэффективными подходами;
4) устаревшая информация;
5) несопоставимые данные;
6) информация, потерявшая конкретность в результате субъективных толкований в процессе частных "теоретических" построений;
7) заведомая "дезинформация».

Учет фактора "дезинформирования" (возможности поступления к пользователю недостоверной и устаревшей информации) требует включения в процессы информационной деятельности специальных процедур оценки информации на достоверность.

Без выявления недостоверной и устаревшей информации, накапливаемой в информационных ресурсах, есть угроза принятия неэффективных, а в ряде случаев и ошибочных решений, наносящих существенный ущерб.

Недостоверная и устаревшая информация не должна уничтожаться. Она должна локализовываться, и на ее основе необходимо строить системные фильтры для контроля информационных ресурсов любого уровня (организаций, объединений, национальных и международных).

При этом сама недостоверная информация должна непрерывно переоцениваться, уточняться и одновременно должны подвергаться переоценке решения, принятые ранее на основании такой информации.

Классы информационных ресурсов.

В зависимости от носителей информации информационные ресурсы делятся на 5 основных классов:

1) документы всех видов, на любых видах носителей;
2) персонал (память людей), обладающий знаниями и квалификацией в различных областях науки и техники;
3) организационные единицы - научные, производственные, управленческие и др. организации, располагающие кадровыми, техническими, производственными, финансовыми и прочими возможностями для решения определенного круга проблем и задач;
4) промышленные образцы (любые материальные объекты, созданные в процессе производства), рецептуры и технологии, программные продукты, которые являются овеществленным результатом научной и производственной деятельности людей;
5) научный инструментарий (в том числе автоматизированные системы научных исследований, автоматизированные рабочие места научных работников и проектировщиков, экспертные системы и базы знаний).

7. ИНФОРМАЦИОННОЕ ПРОТИВОБОРСТВО.

Информационное противоборство – соперничество социальных систем в информационно-психологической сфере по поводу влияния на те или иные сферы социальных отношений и установления контроля над источниками стратегических ресурсов, в результате которого одни участники соперничества получают преимущества, необходимые им для дальнейшего развития, а другие их утрачивают.

В современном многополярном мире информационное противоборство является основным средством обеспечения геополитического баланса.

Цель информационного противоборства – обеспечение национальных интересов в информационно-психологической сфере, которое включает в себя:

- обеспечение геополитической и информационно-психологической безопасности государства;
- достижение военно-политического превосходства и безусловного лидерства в сфере международных отношений;
- обеспечение достижения целей национальной экономической, идеологической, культурной, информационно-психологической экспансии;
- обеспечение благоприятных условий для перехода собственной национальной системы социально-политических отношений на новый, более высокоразвитый и высокотехнологичный этап эволюционного развития;
- трансформация структуры экономического, политического, социально-культурного, информационно-психологического пространств в соответствии с собственными принципами формирования информационной картины мира.

Основные способы достижения целей в информационном противоборстве:

- информационно-психологическое превосходство (доминирование);
- асимметричный ответ на внешние воздействия более сильных субъектов информационного противоборства.

Основные способы достижения информационно-психологического превосходства:

- тайное управление деятельностью органов власти государства-конкурента, информационными (информационно-психологическими) процессами, определяющими облик системы общественных, политических, экономических, духовных отношений государства-соперника;
- информационно-психологическая агрессия;

– информационно-психологическая война.

Внешняя информационно-психологическая экспансия является одним из методов создания условий, необходимых для организации тайного управления деятельностью геополитического субъекта.

Информационная операция (война) - целенаправленные действия, предпринятые для достижения информационного превосходства путём нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и информационных систем

Составные части информационной войны

1) психологические операции - использование информации для воздействия на аргументацию солдат врага.

2) электронная война - не позволяет врагу получить точную информацию

3) дезинформация - предоставляет врагу ложную информацию о наших силах и намерениях

4) физическое разрушение - может быть частью информационной войны, если имеет целью воздействие на элементы информационных систем.

5) меры безопасности - стремятся избежать того, чтобы враг узнал о наших возможностях и намерениях.

6) прямые информационные атаки - прямое искажение информации без видимого изменения сущности, в которой она находится.

8. КЛАССИФИКАЦИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Существуют различные классификации угроз ИБ

В достаточно известной монографии Л. Дж. Хоффмана «Современные

методы защиты информации» были выделены 5 групп различных угроз:

1. хищение носителей,
2. запоминание или копирование информации,
3. несанкционированное подключение к аппаратуре,
4. несанкционированный доступ к ресурсам ЭВМ,
5. перехват побочных излучений и наводок.

Существует классификации угроз по источнику возможной опасности:

1. человек,
2. аппаратура,
3. программа.

К группе угроз, в реализации которых основную роль играет человек, отнесены: хищение носителей, чтение информации с экрана, чтение информации с распечаток.

К группе, где основным средством выступает **аппаратура:** подключение к устройствам, перехват излучений.

К группе, где основное средство – **программа:** несанкционированный программный доступ, программное дешифрование зашифрованных данных, программное копирование информации с носителей.

Аналогичный подход предлагается в *классификации* где выделено *три класса угроз:*

природные (стихийные бедствия, магнитные бури, радиоактивное излучение и наводки),

технические (отключение или колебания напряжения сети электропитания, отказы и сбои аппаратно-программных средств,

электромагнитные излучения и наводки, утечки через каналы связи),

созданные людьми, причем в последнем случае различают непреднамеренные и преднамеренные действия различных категорий лиц.

В **руководящем документе Гостехкомиссии России** [РД. Концепция защиты средств вычислительной техники в АС от НСД к информации, 1992] введено понятие **модели нарушителя** в автоматизированной системе обработки данных. В качестве такового рассматривается субъект, имеющий доступ к работе со штатными средствами АС. При этом в зависимости от возможностей, предоставляемых нарушителям штатными средствами, угрозы делятся на четыре уровня:

самый низкий – возможности запуска задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции обработки информации;

промежуточный 1 – дополнительно к предыдущему имеются возможности создания и запуска собственных программ с новыми функциями обработки информации;

промежуточный 2 – дополнительно к предыдущему предполагается наличие возможностей управления функционированием АС, т.е. воздействия на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования;

самый высокий – определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав системы собственных технических средств с новыми функциями обработки информации (в этом случае предполагается, что нарушитель является специалистом высшей квалификации, знает все об АС, в том числе и об используемых средствах защиты информации).

Согласно [**специальным требованиям и рекомендациям по технической защите конфиденциальной информации (СТР-К)** различают 4 уровня возможностей **внутреннего нарушителя**, которые увеличиваются от уровня к уровню.

первый уровень – возможность запуска программ из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации (пользователь АРМ, пользователь сети);

второй уровень – возможность создания и запуска собственных программ с новыми функциями по обработке информации (прикладной программист, разработчик программного обеспечения);

третий уровень – возможность получения управления функционированием системы, а также воздействия на базовое программное обеспечение, состав и конфигурацию оборудования (системный программист, администратор сервера (ЛВС), администратор

информационной системы (базы данных), разработчик);

четвертый уровень – определяется возможностью проектирования, установки и ремонта средств электронно-вычислительной техники, вплоть до включения в их состав собственных технических и программных средств с новыми функциями по обработке информации (администратор информационной системы, администратор сервера (ЛВС), администратор безопасности информации, разработчик системы, разработчик средств защиты информации, обслуживающий АС персонал).

Можно проводить классификацию:

- по отношению источника угрозы к АС (внешние и внутренние угрозы);

- по виду источника угрозы (физические – отражают физические действия на систему; **логические** – средства, при помощи которых человек получает доступ к логической информации системы; **коммуникационные** – относятся к

процессам передачи данных по линиям связи; **человеческие** – являются наиболее трудно контролируемыми и непосредственно связанными с физическими и логическими угрозами);

- по степени злого умысла (случайные и преднамеренные) и т.д.;

- по способам их воздействия.

Преднамеренные угрозы, подразделяют на **активные** (несанкционированная модификация данных или программ) и **пассивные** (несанкционированное копирование данных или программ).

Такая классификация предусматривает подразделение угроз на **информационные, программно-математические, физические и организационные.**

Информационные угрозы реализуются в виде:

- нарушения адресности и своевременности информационного обмена;
- противозаконного сбора и использования информации;
- осуществления несанкционированного доступа к информационным ресурсам и их противоправного использования;
- хищения информационных ресурсов из банков и баз данных;
- нарушения технологии обработки информации.

Программно-математические угрозы реализуются в виде:

- внедрения в аппаратные и программные изделия компонентов, реализующих функции, не описанные в документации на эти изделия;
- разработки и распространения программ, нарушающих нормальное функционирование информационных систем или их систем защиты информации.

Физические угрозы реализуются в виде:

- уничтожения, повреждения, радиоэлектронного подавления или разрушения средств и систем обработки информации, телекоммуникации и связи;
- уничтожения, повреждения, разрушения или хищения машинных и других носителей информации;
- хищения программных или аппаратных ключей и средств криптографической защиты информации;
- перехвата информации в технических каналах связи и телекоммуникационных системах;
- внедрения электронных устройств перехвата информации в технические средства связи и телекоммуникационные системы, а также в служебные помещения;
- перехвата, дешифрования и навязывания ложной информации в сетях передачи данных и линиях связи;
- воздействия на парольно-ключевые системы защиты средств обработки и передачи информации.

Организационные угрозы реализуются в виде:

- невыполнения требований законодательства в информационной сфере;
- противоправной закупки несовершенных или устаревших информационных технологий, средств информатизации, телекоммуникации и связи.

Учитывая важность вопроса классификации угроз безопасности информации и существование в этой области большого числа различных подходов, необходимо провести системный анализ данной проблемы.

9. СИСТЕМНАЯ КЛАССИФИКАЦИЙ И ОБЩИЙ АНАЛИЗ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Из предыдущего изложения следует, что к настоящему времени

известно большое количество разноплановых угроз безопасности

информации различного происхождения. Различными авторами предлагается целый ряд подходов к их классификации. При этом в качестве критериев деления множества угроз на классы используются виды порождаемых опасностей, степень злого умысла, источники проявления угроз и т.д. Все многообразие предлагаемых классификаций может быть сведено к некоторой системной классификации, приведенной в таблице 2.

Дадим краткий комментарий к использованным в таблице 2 параметрам классификации, их значениям и содержанию.

Системная классификация угроз безопасности информации

Параметры классификации	***Значения параметров***	***Содержание значения параметра (примеры)***
1 . Виды угроз. Целевая направленность	Физическая целостность	Уничтожение (искажение)
	Логическая структура	Искажение структуры
	Содержание	Несанкционированная модификация
	Конфиденциальность	Несанкционированное получение
	Право собственности	Присвоение чужого права
2.Природа происхождения	Случайная	Отказы, сбои, ошибки, стихийные бедствия, побочные влияния.
	Преднамеренная	Злоумышленные действия людей

3.Предпосылки появления	Объективные	Количественная и (или) качественная недостаточность элементов системы,
	Субъективные	Действия развед. органов иностранных государств, промышленный шпионаж, уголовные элементы, недобросовестные сотрудники, террористы и т.д.
Источники угроз	Люди	Посторонние лица, пользователи, персонал
	Технические устройства	Технические устройства, устройства регистрации, передачи, хранения, переработки, выдачи.
	Модели, алгоритмы, программы	Общего назначения, прикладные, вспомогательные
	Технологические схемы обработки	Ручные, интерактивные, внутримашинные, сетевые
	Внешняя среда	Состояние атмосферы, побочные шумы, побочные сигналы

1. Виды угроз. Данный параметр является основополагающим, определяющим целевую направленность защиты информации.

2. Происхождение угроз. В таблице выделено два значения данного параметра: случайное и преднамеренное.

Под случайным понимается такое происхождение угроз, которое обуславливается спонтанными и независящими от воли людей обстоятельствами, возникающими в АС в процессе ее функционирования.

Наиболее известными событиями данного плана являются отказы, сбои, ошибки, стихийные бедствия и побочные влияния. Сущность перечисленных событий (кроме стихийных бедствий, сущность которых ясна) определяется следующим образом:

отказ – нарушение работоспособности какого-либо элемента системы, приводящее к невозможности выполнения им основных своих функций;

сбой – временное нарушение работоспособности какого-либо элемента системы, следствием чего может быть неправильное выполнение им в этот момент своей функции;

ошибка – неправильное (разовое или систематическое) выполнение элементом одной или нескольких функций, происходящее вследствие специфического (постоянного или временного) его состояния;

побочное влияние – негативное воздействие на систему в целом или отдельные ее элементы, оказываемое какими-либо явлениями, происходящими внутри системы или во внешней среде.

Преднамеренное происхождение угрозы обуславливается злоумышленными действиями людей.

3. Предпосылки появления угроз. В таблице приведены две возможные разновидности предпосылок: **объективные** (количественная или качественная недостаточность элементов системы) и **субъективные** (деятельность разведорганов иностранных государств, промышленный шпионаж, деятельность уголовных элементов, действия недобросовестных сотрудников системы).

Перечисленные разновидности предпосылок интерпретируются следующим образом:

количественная недостаточность – физическая нехватка одного или нескольких элементов системы, вызывающая нарушения технологического процесса обработки данных и/или перегрузку имеющихся элементов;

качественная недостаточность – несовершенство конструкции (организации) элементов системы, в силу чего могут появляться возможности случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую информацию;

деятельность разведорганов иностранных государств – специально организуемая деятельность государственных органов, профессионально ориентированных на добывание необходимой информации всеми доступными способами и средствами.

промышленный шпионаж – негласная деятельность организации (ее представителей) по добыванию информации, специально охраняемой от несанкционированной ее утечки или хищения, с целью создания для себя благоприятных условий и получения максимальных выгод (недобросовестная конкуренция);

злоумышленные действия уголовных элементов – хищение информации или компьютерных программ в целях наживы;

действия недобросовестных сотрудников – хищение (копирование) или уничтожение информационных массивов и/или программ по эгоистическим или корыстным мотивам, а также в результате несоблюдения установленного порядка работы с информацией.

4. Источники угроз. Под источником угроз понимается непосредственный ее генератор или носитель. Таким источником могут быть люди, технические средства, модели (алгоритмы), программы, внешняя среда.

Модели угроз и нарушителей. Модели угроз и нарушителей должны быть основным инструментом

менеджмента организации при развертывании, поддержании и совершенствовании системы обеспечения ИБ организации.

Модель угроз ИБ включает описание источников угрозы, уязвимостей, используемых угрозами, методов и объектов нападений, пригодных для реализации угрозы, типов возможной потери (например, конфиденциальности, целостности, доступности активов), масштабов потенциального ущерба. Для источников угроз – людей – может быть разработана **модель нарушителя ИБ**, включающая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, и возможной мотивации их действий.

Степень детализации параметров моделей угроз и нарушителей ИБ может быть различна и определяется реальными потребностями для каждой организации в отдельности.

При анализе угроз ИБ необходимо исходить из того, что эти угрозы непосредственно влияют на операционные риски деятельности организации. Операционные риски сказываются на бизнес-процессах организации.

Наиболее эффективным способом **минимизации рисков** нарушения ИБ для собственника является разработка совокупности мероприятий, методов и средств, создаваемых и поддерживаемых для обеспечения требуемого уровня безопасности информационных активов в соответствии с политикой ИБ.

Классы угроз информационной безопасности в руководящих документах

Угрозы в методе CRAMM

Раскроем часто встречаемую в литературе абривиатуру CRAMM.

CRAMM – CCTA Risk Analysis & Managment Method (в свою очередь CCTA – Central Computer & Telecommunications Agency), UK). То есть это метод анализа и управления рисками

Центрального компьютерного и телекоммуникационного агентства Великобритании.

В переводе Симонова С. в работе [Анализ рисков, управление рисками http://www.jetinfo.ru/1999/1/1/article1.1.1999.html] представлены следующие классы угроз:

1. **Форс-мажорные угрозы:** пожар; затопление; природные катаклизмы; нехватка персонала.
2. **Организационные недостатки.**
3. **Человеческие ошибки:** ошибки при маршрутизации; ошибки пользователей.
4. **Технические неполадки:** неисправность оборудования и вычислительной техники т.д. сбои системного и сетевого ПО; прикладного ПО.
5. **Преднамеренные действия:** использование чужого идентификатора, несанкционированный доступ к приложению; внедрение вредоносного программного обеспечения, и т.д.

Тема угроз информационной безопасности в документах ФСТЭК России

При составлении перечней угроз информационной безопасности, как правило, используют какой-либо **принцип классификации** этих угроз. В связи с этим явно или неявно используется та или иная модель угроз, представляющая собой их определенное формальное описание. Можно указать следующие элементы моделей, отражающие существенные особенности угроз**:**

- **источник (или агент) угрозы;**
- **метод реализации угрозы;**
- **используемая уязвимость информационно-технологической среды (системы) (ИТС);**
- **информационные активы, подверженные угрозе;**
- **вид воздействия на ИТС;**
- **нарушаемое свойство безопасности ИТС.**

Для практического применения удобно использовать классификацию угроз по различным признакам. В основу классификации обычно кладется какой-либо из вышеприведенных элементов.

Угрозы информационной безопасности и политика безопасности организации, это важные аспекты, учитываемые при формировании целей и требований информационной безопасности и выборе мер безопасности.

Для иллюстрации значения вышеприведенных элементов модели угроз рассмотрим примеры содержания некоторых из них.

Нарушаемое свойство безопасности. Реализация той или иной угрозы информационной безопасности организации может иметь последствием:

- нарушение конфиденциальности информации;
- нарушение целостности информации;
- нарушение (частичное или полное) работоспособности ИТС (нарушение доступности).

Используемая уязвимость системы. Реализация угроз, ведущих к нарушению прав доступа и/или конфиденциальности информации, может происходить:

- с использованием доступа субъекта системы (пользователя, процесса) к объекту (файлу данных, каналу связи и т.д.);
- с использованием скрытых каналов передачи информации.

Вид воздействия на ИТС. По этому критерию различают **активное** и **пассивное** воздействие.

Активное воздействие всегда связано с выполнением пользователем каких-либо действий, выходящих за рамки его обязанностей и нарушающих существующую политику безопасности.

Это может быть доступ к определенным наборам данных, программам, вскрытие пароля и т.д. Активное воздействие ведет к изменению состояния системы и может осуществляться либо с использованием доступа (например, к наборам данных), либо

как с использованием доступа, так и с использованием скрытых каналов.

Пассивное воздействие осуществляется путем наблюдения пользователем каких-либо побочных эффектов (от работы программы, например) и их анализе. Примером пассивного воздействия может служить прослушивание линии связи между двумя узлами сети. Пассивное воздействие всегда связано только с нарушением конфиденциальности информации в ИТС, так как при нем никаких действий с объектами и субъектами не производится. Пассивное воздействие не ведет к изменению состояния системы.

Способ воздействия на объект атаки (при активном воздействии).

- Непосредственное воздействие на объект атаки (в том числе с использованием привилегий), например, непосредственный доступ к набору данных, программе, службе, каналу связи и т.д., воспользовавшись какой-либо ошибкой.
- Воздействие на систему разрешений (в том числе захват привилегий).
- Опосредованное воздействие (через других пользователей), например, «маскарад».

Актив информационной инфраструктуры, подверженный угрозе (объект атаки).

Одной из самых главных составляющих нарушения функционирования информационно-телекоммуникационной системы (ИТС) является объект атаки, то есть компонент ИТС, который подвергается воздействию со стороны злоумышленника. Определение объекта атаки позволяет принять меры по ликвидации последствий нарушения, восстановлению этого компонента, установке контроля по предупреждению повторных нарушений и т.д. Воздействию могут подвергаться:

- **ИТС в целом**

– **объекты ИТС:** данные или программы, устройства системы, каналы передачи данных, процессы.

Причина появления используемой ошибки защиты.

Реализация любой угрозы возможна только в том случае, если в данной конкретной системе есть какая-либо ошибка или брешь защиты. Такая ошибка может быть обусловлена одной из следующих причин.

1. Неадекватность политики безопасности реальной ИТС.
2. Ошибки административного управления, под которыми понимается некорректная реализация или поддержка принятой политики безопасности в данной ИТС.
3. Ошибки в алгоритмах программ, в связях между ними и т.д., которые возникают на этапе проектирования и благодаря которым программы можно использовать совсем не так, как описано в документации.
4. Ошибки реализации алгоритмов программ (ошибки кодирования), связей между ними и т.д., которые возникают на этапе реализации или отладки и которые также могут служить источником недокументированных свойств.

Способ воздействия на ИТС: в интерактивном режиме или в пакетном режиме.

Используемые средства атаки. Для воздействия на систему злоумышленник может использовать стандартное программное обеспечение или специально разработанные программы.

Состояние объекта атаки. Объект атаки может находиться в одном из трех состояний: хранения информации; передачи информации; обработки информации.

Перечень угроз для объектов критических сегментов информационной инфраструктуры:

Операторы зомби-сетей (Bot-network operators); Криминальные группы; Иностранные разведывательные органы; Хакеры (Hackers); Создатели шпионского/злонамеренного ПО;

Фишеры (Phishers); Спамеры (Spammers); (Spyware/malware); Террористы

Инсайдеры (Insiders)

Перечень различные типов кибератак

Отказ в обслуживании, DOS-атака (Denial of service); Вирусы; Средства эксплуатации уязвимости (Exploit tools); Логические бомбы; Фишинг (Phishing); Снифферы (Sniffer); Троянские кони; Распределенный отказ в обслуживании, DDOS-атака (Distributed denial of service); Компьютерные черви; Поиск на местности доступной беспроводной сети (War driving); Сканирование дозвоном (War dialing).

Здесь единого принципа классификации не усматривается; наряду с результатом воздействия на систему (например, отказ в обслуживании) приведены методы реализации атак (логические бомбы, вирусы).

Множество угроз, которые надо рассматривать при анализе критически важных информационных инфраструктур, динамически меняется. Эти изменения определяются многими причинами, среди которых основную роль играет появление новых технологий и повышение зависимости от них.

В настоящее время предложен ряд перечней угроз. В качестве примера можно привести перечень угроз, содержащийся в германском стандарте по информационной безопасности **«Руководство по базовой защите информационных технологий» (BSI IT baseline protection manual).** Этот перечень, возможно, является наиболее полным из существующих. Все угрозы в каталоге угроз [Catalogues of Threats 2004] разбиты на 5 следующих групп.

1. Угрозы в связи с форс-мажорными обстоятельствами.
2. Угрозы на организационном уровне.
3. Угрозы, связанные с ошибками людей.
4. Угрозы, связанные с неисправностями техники.
5. Угрозы, вызванные злонамеренными действиями.

Всего 370 угроз.

10. КАНАЛЫ НЕСАНКЦИОНИРОВАННОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ (КНПИ).

КНПИ – это физический канал от источника защищаемой информации к злоумышленнику, по которому возможна утечка охраняемых сведений.

Классифицируем все возможные каналы несанкционированного

получения информации (КНПИ) по двум критериям:

- необходимости доступа (физического или логического) к элементам АС для реализации того или иного КНПИ
- зависимости появления КНПИ от состояния АС.

По первому критерию КНПИ могут быть разделены на **не требующие доступа**, т.е. позволяющие получать необходимую информацию дистанционно (например, путем визуального наблюдения через окна помещений АС), и **требующие доступа** в помещения АС.

В свою очередь, КНПИ, воспользоваться которыми можно только получив доступ в помещения АС, делятся на:

- **не оставляющие следы** в АС (например, визуальный просмотр изображений на экранах мониторов или документов на бумажных носителях)
- **оставляющие те или иные следы** (например, хищение документов или машинных носителей информации).

По второму критерию КНПИ делятся на:

- **постоянно существующие** независимо от состояния АС (например, похищать носители информации можно независимо от того, в рабочем состоянии находятся средства АС или нет);
- **существующие только в рабочем состоянии** АС (например, побочные электромагнитные излучения и наводки).

КНПИ 1-го класса – каналы, проявляющиеся безотносительно к обработке информации и без доступа

злоумышленника к элементам системы. Сюда может быть отнесено:

- **подслушивание разговоров**,
- **провоцирование на разговоры** лиц, имеющих отношение к АС,
- **использование злоумышленником визуальных, оптических и акустических средств.**

Данный канал может проявиться и путем хищения носителей информации в момент их нахождения за пределами помещения, где расположена АС.

КНПИ 2-го класса – каналы, проявляющиеся в процессе обработки информации без доступа злоумышленника к элементам АС. Сюда могут быть отнесены:

- **электромагнитные излучения** различных устройств ЭВМ, аппаратуры и линий связи;
- **паразитные наводки** в цепях питания, телефонных сетях, системах теплоснабжения, вентиляции и канализации, шинах заземления;
- **подключение к информационно-вычислительной сети** генераторов помех и регистрирующей аппаратуры;
- **осмотр отходов производства,** попадающих за пределы контролируемой зоны.

КНПИ 3-го класса – каналы, проявляющиеся безотносительно к обработке информации с доступом злоумышленника к элементам АС, но без изменения последних. К ним относятся;

- **всевозможные виды копирования** носителей информации и документов;
- **хищение производственных отходов.**

КНПИ 4-го класса – каналы, проявляющиеся в процессе обработки информации с доступом злоумышленника к элементам АС, но без изменения последних. Сюда может быть отнесено;

- **запоминание и копирование** информации в процессе обработки;
- **использование программных ловушек**, недостатков языков программирования и операционных систем;
- **поражение программного обеспечения** вредоносными закладками,
- **маскировка** под зарегистрированного пользователя.

КНПИ 5-го класса – каналы, проявляющиеся безотносительно к обработке информации с доступом злоумышленника к элементам АС и с изменением последних. Среди этих каналов:

- **подмена и хищение носителей** информации и аппаратур;
- **включение в программы блоков** типа «троянский конь», «компьютерный червь» и т.п.,
- **чтение остаточной информации**, содержащейся в памяти, после выполнения санкционированных запросов.

КНПИ 6-го класса – каналы, проявляющиеся в процессе обработки информации с доступом злоумышленника к элементам АС и с изменением последних. Сюда может быть отнесено:

незаконное подключение к аппаратуре и линиям связи;

снятие информации на шинах питания различных элементов АС.

11. ОБЫЧНЫЕ УЯЗВИМОСТИ

В приведенных ниже списках даны примеры уязвимостей в различных сферах безопасности, включая примеры угроз, которые могут использовать эти уязвимости. Эти списки могут быть полезными во время оценки уязвимостей. Следует подчеркнуть, что в некоторых случаях эти уязвимости могут использоваться и другими угрозами.

1. Внешняя среда и инфраструктура

Отсутствие физической защиты здания, дверей и окон. Неадекватное или небрежное использование физического управления доступом к зданиям и помещениям. Нестабильная

электрическая сеть. Размещение в местности, предрасположенной к наводнениям.

2. Аппаратные средства

Отсутствие программ периодической замены. Чувствительность к колебаниям напряжения. Чувствительность к колебаниям температуры. Чувствительность к влажности, пыли, загрязнению. Чувствительность к электромагнитному излучению. Недостаточное техническое обслуживание/неправильная установка носителей данных. Отсутствие эффективного контроля изменений конфигурации.

3. Программные средства

Нечеткие или неполные спецификации для разработчиков. Отсутствующее или недостаточное тестирование программных средств. Сложный пользовательский интерфейс. Отсутствие механизмов идентификации и аутентификаци. Отсутствие резервных копий и т.д.

4. Система связи

Незащищенные линии связи. Плохая разводка кабелей. Отсутствие идентификации и аутентификации отправителя и получателя. Передача паролей в незашифрованном виде. Отсутствие подтверждения отправления или получения сообщения и т.д..

5. Документы

Незащищенное хранение. Неконтролируемое копирование.

6. Персонал

Отсутствие персонала. Безнадзорная работа внешнего персонала или персонала, занимающегося уборкой. Недостаточное обучение по безопасности. Отсутствие осознания безопасности. и т.д.

7. Процедурные

Отсутствие санкционирования средств обработки информации. Отсутствие формального процесса санкционирования общедоступной информации и процесса

проверки прав доступа (надзора). Отсутствующая или недостаточная политика «чистого стола и пустого экрана» и т.д.

8. Обычные уязвимости обработки бизнес-приложений

Неверная установка параметров; Применение прикладных программ к неверным данным с точки зрения времени; Неспособность создания административных отчетов; Неверные даты.

9. Общеприменимые уязвимости

Единичная точка сбоя; Неадекватное реагирование технического обслуживания; Неправильно разработанные, несоответствующим образом выбранные или плохо управляемые защитные меры.

12. СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Вопросы, связанные со стандартизацией в Российской Федерации, регулируются Федеральным законом «**О техническом регулировании».**

Статья 11 Закона определяет цели стандартизации.

Статья 13 Закона определяет виды документов в области стандартизации.

Статья 14 Закона определяет статус национального органа Российской Федерации по стандартизации и технических комитетов по стандартизации.

В соответствии с постановлениями Правительства РФ от 16 июня 2004 г. № 284 и от 17 июня 2004 г. № 294 функции федерального органа по техническому регулированию и национального органа по стандартизации осуществляет **Федеральное агентство по техническому регулированию и метрологии**. (Ростехрегулирование, ФАТР и М).

Официальным изданием является «Вестник технического регулирования», зарегистрированный под номером ПИ № 77-16464 от 22 сентября 2003 г.

Основополагающим государственным стандартом Российской Федерации в области защиты информации является ГОСТ Р 52069.0-2003 «Защита информации. Система стандартов. Основные положения» (принят постановлением Госстандарта РФ от 5 июня 2003 г. № 181-ст). Он устанавливает цель и задачи системы стандартов по защите информации, объекты стандартизации, структуру, состав и классификацию входящих в нее стандартов и правила их обозначения.

В зависимости от объекта стандартизации в области ЗИ и требований, предъявляемых к нему, устанавливают стандарты следующих видов: 1) основополагающие; 2) на продукцию; 3) на процессы; 4) на технологию, включая в том числе информационные технологии; 5) на услуги; 6) на методы контроля; 7) на документацию; 8) на термины и определения.

В соответствии с данным стандартом система стандартов по защите информации (ССЗИ) может включать в себя следующие нормативные документы: регламенты, стандарты, правила, нормы и рекомендации по стандартизации, общероссийские классификаторы технико-экономической информации, нормативно-технические документы (НТД) системы общих технических требований к вооружению и военной технике (ОТТ).

Стандарты по ЗИ подразделяют на следующие категории:

международные (ГОСТ ИСО); межгосударственные (ГОСТ); государственные стандарты Российской Федерации (ГОСТ Р); государственные стандарты Российской Федерации, оформленные на основе аутентичного текста международного стандарта (ГОСТ Р ИСО/МЭК); государственные военные стандарты Российской Федерации (ГОСТ РВ); стандарты отраслей, в том числе и на оборонную продукцию (ОСТ); стандарты предприятий.

Зарубежные стандарты в области информационной безопасности

Стандарты и спецификации можно условно разделить на два вида: 1) оценочные стандарты, направленные на классификацию информационных систем и средств защиты по требованиям безопасности; 2) технические спецификации, регламентирующие различные аспекты реализации средств защиты.

Стандарты и регулирование

Различают следующие три понятия: добровольные стандарты; регулирующие стандарты; регулятивное использование добровольных стандартов.

Добровольные стандарты разрабатываются организациями, производящими стандарты. Они являются добровольными в том смысле, что их существование не делает обязательным их применение.

Регулирующие стандарты разрабатываются государственными регулятивными управлениями для достижения определенной общественной цели, например, в области безопасности. Эти стандарты обладают регулятивной силой и должны выполняться производителями в контексте применения данных предписаний.

Регулятивное использование добровольных стандартов – относительно новое или, по меньшей мере, недавно ставшее превалирующим явление. Типичный пример этого – предписание, требующее от государственных организаций, чтобы они приобретали только продукт, соответствующий некоторому набору добровольных стандартов.

Первым документом, получившим статус стандарта, были Критерии безопасности компьютерных систем Министерства обороны США - «Оранжевая книга». В данном документе впервые нормативно определены такие понятия, как «политика безопасности», вычислительная база защиты или ядро защиты (TCB, Trusted Computing Base) и т.д.

Согласно «Оранжевой книге» безопасная компьютерная система – это система, поддерживающая управление доступом к обрабатываемой в образом авторизованные пользователи или процессы, действующие от их имени, получают возможность читать, писать, создавать и удалять информацию.

Европейские критерии безопасности информационных технологий

Вслед за выходом «Оранжевой книги» страны Европы разработали согласованные «**Критерии безопасности информационных технологий»** (Information Technology Security Evaluation Criteria, далее – Европейские критерии).

Европейские критерии рассматривают следующие задачи средств информационной безопасности: защита информации от несанкционированного доступа с целью обеспечения ее **конфиденциальности;**

- обеспечение **целостности** информации посредством защиты от ее несанкционированной модификации или уничтожения; обеспечение **доступности** компьютерных систем с помощью противодействия угрозам отказа в обслуживании.

Американские Федеральные критерии безопасности информационных технологий

Федеральные критерии безопасности информационных технологий (Federal Criteria for Information Technology Security) разрабатывались как одна из составляющих Американского федерального стандарта по обработке информации (Federal Information Processing Standart), призванного заменить «Оранжевую книгу». Создание Федеральных критериев безопасности информационных технологий преследовало следующие цели: 1.) Определение универсального и открытого для дальнейшего развития **базового набора требований безопасности.** 2). Совершенствование существующих требований и критериев безопасности. 3). Приведение в соответствие принятых в разных странах требований и критериев безопасности информационных технологий. 4).

Нормативное закрепление основополагающих принципов информационной безопасности.

Общие критерии безопасности информационных технологий

Общие критерии безопасности информационных технологий (Common Criteria for Information Technology Security Evaluation, далее – Общие критерии) являются результатом совместных усилий авторов Европейских критериев безопасности информационных технологий, американских Федеральных критериев безопасности информационных технологий и Канадских критериев безопасности компьютерных систем, направленных на объединение основных положений этих документов и создание единого международного стандарта безопасности информационных технологий.

ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»

ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» относится к разновидности стандартов, оформленных на основе аутентичного текста. Основой для него стал международный стандарт ISO/IEC 15408-99 «Общие критерии безопасности информационных технологий».

Общие критерии состоят из 3-х частей: 1. Введение и общая модель.

2. Функциональные требования безопасности. 3. Требования доверия к безопасности.

Часть 1 стандарта включает методологию оценки безопасности ИТ, определяет виды требований безопасности (функциональные и доверия), основные конструкции (профиль защиты, задание по безопасности) представления требований безопасности в интересах трех категорий пользователей:

потребителей, разработчиков и оценщиков продуктов и систем ИТ.

Часть 2 стандарта включает универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам.

Часть 3 стандарта включает систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям. В этой же части содержится описание оценочных уровней доверия, определяющих шкалу требований, которые позволяют с возрастающей степенью полноты и строгости провести оценку проектной, тестовой и эксплуатационной документации, правильности функционирования комплекса средств безопасности, оценку уязвимостей продукта или системы ИТ, стойкости механизмов защиты и сделать заключение об уровне безопасности объекта оценки.

Стандарт не содержит критериев оценки безопасности, касающихся административных мер безопасности (организационные меры, управление персоналом, физическая защита и процедурный контроль), непосредственно не относящихся к мерам безопасности ИТ.

Руководящие документы Гостехкомиссии (ФСТЭК) России

В качестве стратегического направления Гостехкомиссия России выбрала ориентацию на «Общие критерии».

Рассмотрим два важных Руководящих документа – Классификацию автоматизированных систем (АС) по уровню защищенности от несанкционированного доступа (НСД) и аналогичную Классификацию межсетевых экранов (МЭ).

Согласно первому из них, 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 (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Основным критерием классификации МЭ служит протокольный уровень (в соответствии с эталонной семиуровневой моделью), на котором осуществляется фильтрация информации. Чем выше уровень, тем больше информации на нем доступно и, следовательно, тем более тонкую и надежную фильтрацию можно реализовать.

Значительное внимание в РД уделено собственной безопасности служб обеспечения защиты и вопросам согласованного администрирования распределенных конфигураций.

Рекомендации X.800

Технические спецификации X.800 появились немногим позднее «Оранжевой книги», но весьма полно и глубоко трактующей вопросы информационной безопасности распределенных систем.

Рекомендации X.800 – документ довольно обширный. Остановимся на специфических сетевых функциях (сервисах) безопасности, а также на необходимых для их реализации защитных механизмах.

13. СЕРВИСЫ БЕЗОПАСНОСТИ

Выделяют следующие **сервисы безопасно**сти и исполняемые ими роли:

Аутентификация. Данный сервис обеспечивает проверку подлинности партнеров по общению и проверку подлинности источника данных. **Аутентификация партнеров по общению** используется при установлении соединения и, быть может, периодически во время сеанса. Она служит для

предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной).

Управление доступом. Обеспечивает защиту от несанкционированного использования ресурсов, доступных по сети.

Конфиденциальность данных. Обеспечивает защиту от несанкционированного получения информации. **Конфиденциальность трафика** (это защита информации, которую можно получить, анализируя сетевые потоки данных).

Целостность данных подразделяется на подвиды в зависимости от того, какой тип общения используют партнеры – с установлением соединения или без него, защищаются все данные или только отдельные поля, обеспечивается ли восстановление в случае нарушения целостности.

Неотказуемость (невозможность отказаться от совершенных действий) обеспечивает два вида услуг: неотказуемость с подтверждением подлинности источника данных и неотказуемость с подтверждением доставки. Побочным продуктом неотказуемости является аутентификация источника данных.

Сетевые механизмы безопасности

Для реализации сервисов (функций) безопасности могут использоваться следующие механизмы и их комбинации: **шифрование**; **электронная цифровая подпись; механизмы управления доступо**м. Могут располагаться на любой из участвующих в общении сторон или в промежуточной точке;

• **механизмы контроля целостности данных**. В рекомендациях X.800 различаются два аспекта целостности: целостность отдельного сообщения или поля информации и целостность потока сообщений или полей информации. Для проверки целостности потока сообщений (то есть для защиты от кражи, переупорядочивания, дублирования и вставки

сообщений) используются порядковые номера, временные штампы, криптографическое связывание или иные аналогичные приемы;

• **механизмы аутентификации.** Согласно рекомендациям X.800, аутентификация может достигаться за счет использования паролей, личных карточек или иных устройств аналогичного назначения, криптографических методов, устройств измерения и анализа биометрических характеристик;

• **механизмы дополнения трафика;**

• **механизмы управления маршрутизацией.** Маршруты могут выбираться статически или динамически. Оконечная система, зафиксировав неоднократные атаки на определенном маршруте, может отказаться от его использования. На выбор маршрута способна повлиять метка безопасности, ассоциированная с передаваемыми данными;

• **механизмы нотаризации** служат для заверения таких коммуникационных характеристик, как целостность, время, личности отправителя и получателей. Заверение обеспечивается надежной третьей стороной, обладающей достаточной информацией. Обычно нотаризация опирается на механизм электронной подписи.

Администрирование средств безопасности

Администрирование средств безопасности включает в себя распространение информации, необходимой для работы сервисов и механизмов безопасности, а также сбор и анализ информации об их функционировании. Примерами могут служить распространение криптографических ключей, установка значений параметров защиты, ведение регистрационного журнала и т.п.

Согласно рекомендациям X.800, усилия администратора средств безопасности должны распределяться по трем направлениям: администрирование информационной системы в

целом; администрирование сервисов безопасности; администрирование механизмов безопасности.

Администрирование сервисов безопасности включает в себя

Определение защищаемых объектов, выработку правил подбора механизмов безопасности (при наличии альтернатив), комбинирование механизмов для реализации сервисов, взаимодействие с другими администраторами для обеспечения согласованной работы.

Обязанности администратора механизмов безопасности определяются перечнем задействованных механизмов.

Типичный список таков: • управление ключами (генерация и распределение); • управление шифрованием (установка и синхронизация криптографических параметров).

С различными стандартами в области информационной безопасности можно ознакомится в [1].

14. МЕРЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Защитные меры– это действия, процедуры и механизмы, способные обеспечить безопасность от возникновения угрозы, уменьшить уязвимость, ограничить воздействие инцидента в системе безопасности, обнаружить инциденты и облегчить восстановление информации (активов).

Эффективная безопасность обычно требует комбинации различных защитных мер для обеспечения заданных уровней безопасности при защите активов.

Порядок выбора защитных мер важен для правильного планирования и реализации программы ИБ.

Защитная мера может выполнять много функций безопасности, и, наоборот, одна функция безопасности может потребовать нескольких защитных мер. Защитные выполняют одну или несколько из следующих функций: предотвращение; сдерживание; обнаружение; ограничение; исправление; восстановление; мониторинг; осведомление.

Меры обеспечения ИБ (**меры контроля, защитные меры**) имеют сложную структуру и состоят из **организационных** и **программно-технических и криптографических мер** на верхнем уровне.

В свою очередь, организационные меры включают **законодательные, административные и процедурные меры** обеспечения ИБ.

Законодательные меры - это законы, стандарты, регламенты и другие нормативные документы.

Основой **административных мер**, является политика безопасности.

Процедурные, то есть реализуемые людьми, **меры** безопасности включают меры по: управлению персоналом; физической защите; поддержке работоспособности; реагированию на нарушения режима безопасности; планированию восстановительных работ.

Идентификация мер защиты важна и на этапе оценки рисков. В процессе идентификации мер защиты должна быть проведена проверка, что эти средства работают корректно.

Описание мер по обеспечению ИБ, приведенное ниже, выполнено в нотациях стандарта ГОСТ Р ИСО/МЭК 27001 и ISO/IEC 17799:2005 с указанием цели и описанием требований.

Стандарты ГОСТ Р ИСО/МЭК 27001 и ISO/IEC 17799:2005 выделяют следующие области контроля: политика безопасности; управление активами (ресурсами); безопасность кадровых ресурсов (персонала); физическая безопасность и безопасность от воздействия окружающей среды; управление средствами связи и функционированием; контроль доступа; приобретение, разработка и обслуживание информационных систем; управление инцидентами с информационной безопасностью; управление непрерывностью бизнес-процессов; соответствие различным требованиям.

Ориентировочно весь объем мероприятий (в денежном исчислении) по охране и защите информации можно разделить в следующем соотношении:

1. Правовые меры (законы, ведомственные акты, инструкции) – 5%.

2. Физические меры (ограда по периметру, служба охраны, разграничение полномочий и др.) – 15%.

3. Технические меры (различные технические и программные средства защиты) – 25–30%.

4. Административные меры (разработка политики в области безопасности, процедур ее внедрения, кадровая политика, обучение персонала, контроль и др.) – 50%.

Выбор средств контроля (мер защиты)

Средства контроля выбираются в соответствии с вопросами безопасности, идентифицированными в результате оценки риска, принимая в расчет угрозы и вид рассматриваемого информационного процесса или системы.

Выбор средств контроля всегда включает баланс **операционных** (нетехнических) и **технических** средств контроля.

Операционные средства контроля включают те, которые обеспечивают **физическую, кадровую и административную безопасность**.

Физические средства контроля безопасности включают прочность внутренних стен строения, дверные замки с кодовым набором, противопожарные системы и охрану.

Кадровая безопасность охватывает проверки, связанные с набором персонала (особенно лиц, занимающих ответственные посты), мониторинг персонала и программы повышения осознания безопасности.

Административная (процедурная) безопасность включает надежное документирование операционных процедур, процедуры разработки и одобрения приложений, а также процедуры менеджмента инцидентов информационной

безопасности. В связи этим важно, чтобы для каждой системы разрабатывались соответствующие **планы и стратегия** обеспечения непрерывности процессов, включая планирование действий в чрезвычайных ситуациях/восстановление после сбоев.

Техническая безопасность охватывает **аппаратную и программную защиту**, а также **средства контроля системы связи**. Эти средства контроля выбираются в соответствии с рисками для обеспечения функциональных возможностей безопасности и доверия.

Функциональные возможности будут, например, охватывать идентификацию и аутентификацию, требования логического контроля доступа, потребности контрольного журнала/журнала безопасности, обеспечение безопасности с помощью обратного звонка, аутентификацию сообщений, шифрование и т.д. Требования доверия документируют необходимый уровень доверия к функциям безопасности и, следовательно, объем и вид проверок, тестирования безопасности и т.д., необходимых для подтверждения этого уровня.

При выборе средств контроля для реализации следует рассматривать ряд факторов, включая:

- виды выполняемых функций: предотвращение, сдерживание, обнаружение, восстановление, исправление, мониторинг, информированность;
- относительную стойкость средств контроля;
- капитальные, операционные и эксплуатационные расходы на средства контроля;
- помощь, предоставляемую пользователям для выполнения их функций;
- простоту использования средства контроля для пользователя.

Идентификация вида системы информационно-коммуникационных технологий (ИКТ).

Для оценки существующей или планируемой системы ИКТ рассматриваемая система должна быть сравнена со следующими компонентами и должны быть идентифицированы компоненты, представляющие систему. В последующих пунктах предлагаются средства контроля для каждого из перечисленных ниже компонентов. Компоненты для выбора включают:

- автономную рабочую станцию;
- рабочую станцию (клиент без коллективно используемых ресурсов), подсоединенную к сети;
- сервер или рабочую станцию с коллективно используемыми ресурсами, подсоединенную к сети.

Идентификация физических условий/условий внешней среды

включает идентификацию физической инфраструктуры, поддерживающей существующую и планируемую систему ИКТ, а также соответствующих существующих и/или планируемых средств контроля. Поскольку все средства контроля должны быть совместимы с физической средой, эта оценка очень важна для успешного выбора.

При рассмотрении инфраструктуры могут быть полезны следующие

вопросы.

Периметр и здание:

- Где расположено здание ? Сколько у здания арендаторов и кто они? Где расположены значимые/критичные сферы?

Управление доступом: - Кто имеет доступ к зданию? - Существует ли система физического контроля доступа? Насколько прочна конструкция здания, двери окна и т.д. и какая защита им обеспечивается? Охраняется ли здание, происходит ли это в течение всех суток или только в рабочее время? Оснащено ли здание и/или помещения, в которых расположено критичное оборудование ИКТ, охранной сигнализацией?

Защита на местах: - Как защищается помещение (помещения), содержащее систему ИКТ? - Какие системы обнаружения возгорания, пожарной сигнализации и ликвидации пожара установлены и где? - Какие системы обнаружения утечки воды/жидкости, сигнализации и ликвидации установлены и где? Существуют ли поддерживающие коммунальные услуги типа водопроводно-канализационной сети, системы бесперебойного питания, кондиционирования воздуха (для контроля температуры и влажности)?

Выбор средств контроля в соответствии с проблемами и угрозами безопасности включает 2 этапа

1. **Определение и оценка проблем безопасности.** Должны учитываться требования конфиденциальности, целостности, доступности, учетности, подлинности и надежности. Мощность и количество выбранных средств контроля должны соответствовать оцененным проблемам безопасности.
2. **Для** каждой проблемы безопасности **составляется список типичных угроз** и для каждой угрозы предлагаются средства контроля в соответствии с рассматриваемой системой ИКТ.

Оценка проблем безопасности

Проблемы безопасности могут включать: потерю конфиденциальности; потерю целостности; потерю доступности; потерю учетности; потерю подлинности; потерю надежности.

Проблемы безопасности оцениваются путем рассмотрения того, причинят ли последствия сбоя или нарушения безопасности серьезный ущерб, незначительный ущерб или нулевой ущерб рассматриваемого объекта. Оценка должна проводиться отдельно для каждого актива, так как проблемы безопасности для различных активов могут быть разными.

В случае если все возможные потери конфиденциальности, целостности, доступности, учетности,

подлинности и надежности идентифицированы как, вероятно, причиняющие незначительный ущерб, то достаточную безопасность рассматриваемой системы ИКТ должен обеспечить **высокоуровневый** или **базовый подход**. В случае если любая из этих потерь идентифицирована как, вероятно, причиняющая серьезный ущерб, то нужно оценить, следует ли выбирать средства контроля дополнительно к тем, которые предлагаются ниже.

Потеря конфиденциальности

Рассмотреть последствия потери конфиденциальности (намеренной или ненамеренной) проверяемого актива. Например, потеря конфиденциальности может приводить: к утрате общественного доверия или ухудшению общественного имиджа; правовой ответственности, включая ту, которая может проистекать из нарушения законодательства о защите данных; - неблагоприятному влиянию на политику организации; - созданию угрозы личной безопасности; финансовым потерям.

В соответствии с ответами на приведенные выше вопросы должно быть принято решение, будут ли последствия, которые могут вытекать из потери конфиденциальности, серьезными, незначительными или нулевыми. Это решение должно быть задокументировано.

Потеря целостности.

Рассмотреть последствия потери целостности (намеренной или ненамеренной) проверяемого актива. Например, потеря целостности может приводить к: - неверным принимаемым решениям; мошенничеству; нарушению деловых функций; утрате общественного доверия или ухудшению общественного имиджа; финансовым потерям; правовой ответственности, включая ту, которая может проистекать из нарушения законодательства о защите данных.

В соответствии с ответами на приведенные выше вопросы должно быть принято решение, будут ли неблагоприятные последствия, которые могут вытекать из

потери целостности, серьезными, незначительными или нулевыми. Это решение должно быть задокументировано.

Потеря доступности

Рассмотреть последствия кратковременной потери доступности приложений или информации, т.е. какие деловые функции в случае их прерывания приведут к невыполнению времени реагирования или времени выполнения. Должна быть также рассмотрена крайняя форма потери доступности, необратимая потеря данных и/или физическое разрушение аппаратных или программных средств. Например, потеря доступности критических приложений или информации может приводить к: неверным принимаемым решениям; неспособности выполнения критических задач; утрате общественного доверия или ухудшению общественного имиджа; финансовым потерям; правовой ответственности, включая ту, которая может проистекать из нарушения законодательства о защите данных и из невыполнения договорных предельных сроков; значительным расходам на восстановление.

Потеря учетности

Рассмотреть последствия потери учетности пользователей системы или объектов (например, программных средств), действующих от имени пользователя. Кроме того, это рассмотрение должно включать автоматически генерируемые сообщения, которые могут приводить к действию. Например, потеря учетности может приводить к: манипулированию системой пользователями; мошенничеству; промышленному шпионажу; неотслеживаемым действиям; ложным обвинениям; правовой ответственности, включая ту, которая может проистекать из нарушения законодательства о защите данных.

Потеря подлинности

Рассмотреть последствия потери подлинности данных и сообщений, независимо от того, используются ли они людьми или системами. Это особенно важно в распределенных системах, где принятые решения распространяются среди

большого сообщества или где используется справочная информация. Например, потеря подлинности может приводить: - к мошенничеству; - использованию правомерного процесса с недействительными данными, приводящими к вводящему в заблуждение результату; - манипулированию организацией посторонними лицами; - промышленному шпионажу; - ложным обвинениям; - правовой ответственности, включая ту, которая может проистекать из нарушения законодательства о защите данных.

Потеря надежности

Рассмотреть последствия потери надежности систем. Кроме того, важно рассмотреть функциональные возможности, являющиеся подхарактеристикой надежности. Например, потеря надежности может приводить: - к мошенничеству; - потерянной доле на рынке; - отсутствию мотивации у персонала; - ненадежным поставщикам; - потери доверия клиентов; - правовой ответственности, включая ту, которая может проистекать из нарушения законодательства о защите данных.

Средства контроля конфиденциальности

Ниже перечислены виды угроз, которые могут ставить в опасность конфиденциальность и предлагаемые средства контроля для защиты от этих угроз.

Подслушивание является одним из способов получения доступа к значимой информации, например, путем подключения к линии или прослушивания телефонных разговоров.

Средства контроля:

Физические средства контроля - помещения, стены, строения и т. д. должны исключать подслушивание или делать его трудновыполнимым, также мерой защиты является добавление помех.

Политика информационной безопасности - наличие строгих правил, касающихся того, когда, где и каким способом должен происходить обмен значимой информацией.

Защита конфиденциальности данных - шифрование сообщения перед обменом сообщениями.

Электромагнитное излучение может использоваться нарушителем для приобретения знаний об информации, обрабатываемой системой ИКТ.

- Физические средства контроля: облицовка комнат, стен и т.д.; не позволяющая электромагнитному излучению проходить через облицовку.
- Защита конфиденциальности данных применима только пока информация зашифрована, а не для обрабатываемой, выводимой на экран или распечатываемой информации.
- Использование оборудования информационно-коммуникационных технологий с низким излучением. Может быть применено оборудование со встроенной защитой.

Вредоносное программное обеспечение может приводить к потере конфиденциальности, например, посредством перехвата и раскрытия паролей.

Средства контроля : Защита от вредоносного программного обеспечения; Менеджмент инцидентов ИБ.

Своевременное сообщение о необычном инциденте может ограничивать ущерб, в случае атак со стороны вредоносного программного обеспечения. Обнаружение вторжения может использоваться для обнаружения попыток проникновения в систему или сеть.

Имитация личности пользователя может быть использована, чтобы обойти аутентификацию и все сервисы и функции безопасности, связанные с этим. Это может приводить к проблемам конфиденциальности, когда такая имитация дает возможность доступа к значимой информации.

Средства контроля:

- Идентификация и аутентификация..
- Логический контроль доступа и аудит. Средства логического контроля не могут отличить законного

пользователя от незаконного, но можно уменьшить сферу влияния. Проверка и анализ контрольных журналов могут обнаруживать несанкционированную деятельность.

- Защита от вредоносного ПО. Т.К. одним из способов получения паролей является введение вредоносного программного обеспечения
- Сетевой менеджмент.
- Защита конфиденциальности данных. Если приведенный выше вид защиты невозможен или недостаточен, может быть обеспечена дополнительная защита, использующая шифрование хранимых значимых данных.

Неправильная маршрутизация/изменение маршрутизации сообщений – это умышленное или случайное неверное направление сообщений, тогда как изменение маршрутизации может происходить как с хорошими, так и с плохими целями. Изменение маршрутизации может, например, осуществляться для поддержки сохранности доступности. Неправильная маршрутизация и изменение маршрутизации сообщений могут приводить к потере конфиденциальности, если они делают возможным несанкционированный доступ к этим сообщениям.

Средства контроля

- Сетевой менеджмент
- Защита конфиденциальности данных. Чтобы избежать несанкционированного доступа, сообщения могут шифроваться.

Сбой программы - может подвергать опасности конфиденциальность, если это программное средство обеспечивает защиту конфиденциальности, например, программные средства управления доступом или шифрования, или если сбой программы создает дыру, например, в операционной системе.

Средства контроля:

– Менеджмент инцидентов. При неправильной работе программы, об этом сообщается ответственному лицу, чтобы как можно скорее могли быть приняты меры.
– Операционные вопросы. Некоторые сбои программ можно избежать путем тщательного тестирования программного средства перед его использованием и посредством контроля изменений программных средств.

Хищение подвергает опасности конфиденциальность, если похищенный компонент информационно-коммуникационных технологий содержит значимую информацию, к которой может получить доступ похититель.

Средства контроля:

– - Физические средства контроля. Физическая защита, затрудняющая доступ к строению, сфере или помещению, содержащим оборудование ИКТ, или специальные средства контроля против хищения.
– Кадровые. Должны существовать средства контроля для персонала (контроль внешнего персонала, соглашения об обеспечении конфиденциальности и т.д.), затрудняющие хищение.
– Защита конфиденциальности данных. Это средство контроля должно быть реализовано, если существует возможность хищения оборудования ИКТ, содержащего значимую информацию.
– Средства контроля носителей данных. Любой носитель данных, содержащий значимую информацию, должен быть защищен от хищения.

Несанкционированный доступ к компьютерам, данным, сервисам и приложениям может быть угрозой, если возможен доступ к любому значимому материалу.

Средства контроля:

– Идентификация и аутентификация. Соответствующие средства контроля идентификации и аутентификации должны применяться в сочетании с логическим контролем

доступа для предотвращения несанкционированного доступа.

- Логический контроль доступа и аудит. Должны использоваться механизмы управления доступом для обеспечения логического контроля доступа. Проверка и анализ контрольных журналов могут обнаруживать несанкционированную деятельность лиц, имеющих права доступа к системе.
- Сетевое разделение для затруднения несанкционированного доступа,.
- Физический контроль доступа.
- Средства контроля носителей данных. Если значимые данные хранятся на другом носителе, должны присутствовать средства контроля носителей данных для защиты носителей от несанкционированного доступа.
- Защита конфиденциальности данных. Если по некоторым причинам приведенный выше вид защиты невозможен или недостаточен, может быть обеспечена дополнительная защита, использующая шифрование значимых данных.

Несанкционированный доступ к носителям данных

Несанкционированный доступ к носителям данных и их использование могут подвергать опасности конфиденциальность, если на этих носителях хранится любой конфиденциальный материал.

Средства контроля:

- Операционные вопросы. Могут быть применены средства контроля носителей данных для обеспечения, например, физической защиты и учетности носителей данных
- Физическая безопасность. Соответствующая защита комнат (прочные стены и окна, а также физический контроль доступа) и принадлежности защиты могут обеспечить защиту от несанкционированного доступа.
- Защита конфиденциальности данных. Дополнительная защита хранящегося значимого материала может быть

достигнута путем шифрования материала. Необходима хорошая система менеджмента ключей, позволяющая надежное применение шифрования.

Средства контроля целостности

Ниже перечислены виды угроз, которые могут подвергать опасности целостность, вместе с предлагаемыми средствами контроля для защиты от этих угроз. Если это уместно для выбора средств контроля, то должны приниматься в расчет вид и характеристики системы ИКТ.

Ухудшение состояния носителей данных угрожает целостности всего, что хранится на этих носителях

Средства контроля:

- верификация целостности носителей данных,
- создание резервных копий.
- Защита целостности данных (могут использоваться криптографические средства).

Ошибка технического обслуживания подвергают целостность информации опасности

Средства контроля :

- Правильное техническое обслуживание.
- - Резервные копии.
- - Защита целостности данных.

Вредоносное программное обеспечение

Средства контроля:

- Защита от вредоносного программного обеспечения.
- Менеджмент инцидентов.

Имитация личности пользователя

Средства контроля:

- Идентификация и аутентификация.
- Логический контроль доступа и аудит.
- Защита от вредоносного программного обеспечения,
- Сетевой менеджмент.

При необходимости обеспечивают дополнительную защиту, использующую криптографические средства, подобные цифровым подписям.

Неправильная маршрутизация/изменение маршрутизации сообщений

Средства контроля

- Сетевой менеджмент
- Защита целостности данных. Могут быть использованы хэш-функции и цифровые подписи.

Неотказуемостъ

Должны быть применены средства контроля неотказуемости, когда важно иметь подтверждение того, что сообщение было послано и/или получено и что сеть передала сообщение. В качестве основы неотказуемости (целостности данных и неотказуемости) существуют специальные криптографические средства контроля.

Сбой программы может разрушить целостность данных и информации, которые обрабатываются с помощью этого ПО.

Средства контроля:

- Сообщение о неправильном срабатывании программы.
- Операционные вопросы.
- Резервные копии.
- Защита целостности данных при помощи криптографических средств.

Нарушения подачи (электроэнергии, кондиционирования воздуха)

Могут вызывать проблемы целостности, если из-за них происходят другие сбои. Например, нарушение подачи может приводить к аппаратным сбоям, техническим повреждениям или проблемам с носителями данных.

Средства контроля

- Контроль за энергоснабжением и кондиционированием воздуха, защита от скачков напряжения.
- Резервные копии.

Техническое повреждение

Могут разрушать целостность информации, хранящейся или обрабатываемой в этой сети.

Средства контроля :

- Операционные вопросы. Менеджмент изменений и конфигурации, менеджмент возможностей должны использоваться, чтобы избежать повреждений любой системы ИКТ или сети. Для обеспечения безотказной работы системы или сети используется документирование и техническое обслуживание.
- Сетевой менеджмент.
- Энергоснабжение и кондиционирование воздуха.
- Резервные копии.

Ошибки передачи могут разрушать целостность передаваемой информации.

Средства контроля:

- Тщательное планирование при прокладке кабелей.
- Сетевой менеджмент.
- Защита целостности данных. Для защиты от случайных ошибок передачи могут использоваться контрольные суммы или циклические избыточные коды в протоколах связи. Криптографические средства могут использоваться для защиты целостности передаваемых данных в случае умышленных атак.

Несанкционированный доступ к компьютерам, данным, сервисам и приложениям

Средства контроля:

- Идентификация и аутентификация.
- Логический контроль доступа и аудит.
- Сетевое разделение.
- Физический контроль доступа.
- Средства контроля носителей данных

– Целостность данных. Для защиты целостности хранящейся или передаваемой информации могут использоваться криптографические средства.

Использование несанкционированных программ и данных

Средства контроля:

– Обучение и повышение осознания безопасности.
– Резервные копии.
– Идентификация и аутентификация.
– Логический контроль доступа и аудит.
– Защита от вредоносного программного обеспечения.

Несанкционированный доступ к носителям

Средства контроля:

– Операционные вопросы.
– Физическая безопасность.
– Целостность данных. Для защиты целостности информации, хранящейся на носителях данных, могут использоваться криптографические средства.

Ошибки пользователей

Средства контроля:

– Обучение и повышение осознания безопасности.
– Резервные копии.

Средства контроля доступности

Ниже перечислены виды угроз, которые могут подвергать опасности доступность, вместе с предлагаемыми средствами контроля для защиты от этих угроз.

Следует отметить, что большинство из обсуждающихся средств контроля обеспечивает более «общую» защиту, т.е. они не направлены на конкретные угрозы, а обеспечивают защиту путем поддержки общего эффективного менеджмента информационной безопасности. Поэтому они не перечисляются здесь в деталях, но их эффект не следует недооценивать и они должны реализовываться для обеспечения общей эффективной защиты.

Разрушительная атака

Средства контроля

- Дисциплинарный процесс. Все служащие должны сознавать последствия в случае разрушения ими информации (намеренно или ненамеренно).
- Средства контроля носителей данных. Все носители данных должны быть соответствующим образом защищены от несанкционированного доступа, используя физическую защиту и учетность.
- Резервные копии.
- Физическая защита.
- Идентификация и аутентификация.
- Логический контроль доступа и аудит.

Ухудшение состояния носителей данных

Средства контроля.

- Средства контроля носителей данных.
- Резервные копии.

Отказ оборудования и услуг связи

Средства контроля:

- Избыточность и резервные копии. Избыточная реализация компонентов услуг связи может быть использована для снижения вероятности отказа услуг связи. В зависимости от максимально приемлемого времени простоя резервное оборудование тоже может быть использовано для удовлетворения требований. В любом случае должна быть сделана резервная копия данных конфигурации и топологии, чтобы обеспечить доступность в случае чрезвычайной ситуации.
- Сетевой менеджмент.
- Тщательное планирование при прокладке кабелей может помочь избежать повреждения; если есть подозрение, что линия может быть повреждена, она должна быть внимательно проверена.

– Неотказуемость. Если нужно подтверждение сетевой доставки, отправки или получения сообщения, должна применяться неотказуемость – тогда сбой связи или пропавшая информация могут быть легко обнаружены.

Пожар, затопление

Средства контроля:

– Физическая защита.
– Должен существовать план обеспечения непрерывности процессов и должны быть доступны резервные копии всей важной информации.

Ошибка технического обслуживания

Средства контроля :

– Техническое обслуживание.
– Резервные копии.

Вредоносное программное обеспечение

Средства контроля:

– Защита от вредоносного программного обеспечения.
– Менеджмент инцидентов.

Имитация личности пользователя

Средства контроля:

– Идентификация и аутентификация.
– Логический контроль доступа и аудит.
– Защита от вредоносного программного обеспечения.
– Сетевой менеджмент.
– Резервное копирование данных.

Неправильная маршрутизация/изменение маршрутизации сообщений

– Сетевой менеджмент.
– Неотказуемость.

Злоупотребление ресурсами может приводить к недоступности информации или услуг.

Средства контроля

- Кадровые. Персонал должен сознавать последствия злоупотребления ресурсами; в случае необходимости должны применяться дисциплинарные процессы.
- Операционные вопросы. Использование системы должно подвергаться мониторингу для обнаружения несанкционированной деятельности, а для сведения к минимуму возможностей злоупотребления привилегиями должно применяться разделение обязанностей.
- Идентификация и аутентификация.
- Логический контроль доступа и аудит.
- Сетевой менеджмент.

Природные бедствия

Средства контроля:

- Защита от природных бедствий.
- План обеспечения деловой непрерывности.

Сбой программы

Средства контроля :

- Сообщение о неправильном срабатывании программы.
- Операционные вопросы.
- Резервные копии.

Нарушения подачи (электроэнергии, кондиционирования воздуха)

Средства контроля:

- Контроль за энергоснабжением и кондиционированием воздуха.
- Резервные копии.

Техническое повреждение

- Средства контроля:
- Операционные вопросы.
- Сетевой менеджмент.
- План обеспечения непрерывности бизнеса.

Хищение

Средства контроля:

- Физические средства контроля.
- Кадровые.
- Средства контроля носителей данных.

Перегрузка трафика

Средства контроля:

- Избыточность и резервные копии. Избыточная реализация компонентов служб связи может быть использована для снижения вероятности перегрузки трафика. В зависимости от максимально приемлемого времени простоя резервное оборудование тоже может быть использовано для удовлетворения требований.
- Сетевой менеджмент..

Ошибки передачи

Средства контроля:

- Прокладка кабелей.
- Сетевой менеджмент

Несанкционированный доступ к компьютерам, данным, сервисам и приложениям

Средства контроля:

- Идентификация и аутентификация.
- Логический контроль доступа и аудит.
- Сетевое разделение.
- Физический контроль доступа.
- Средства контроля носителей данных

Использование несанкционированных программ и данных

Средства контроля:

- Обучение и повышение осознания безопасности.
- Резервные копии.
- Идентификация и аутентификация
- Логический контроль доступа и аудит.
- Защита от вредоносного программного обеспечения.

Несанкционированный доступ к носителям данных

Средства контроля:

- Операционные вопросы.
- Физическая безопасность.

Ошибки пользователей

- Обучение и повышение осознания безопасности.
- Резервные копии.

Средства контроля учетности, подлинности и надежности

Рамки учетности, подлинности и доступности широко различаются в разных сферах. Эти различия означают, что может применяться множество различных средств контроля. Поэтому ниже может быть дано лишь общее руководство.

Средства контроля, обсуждавшиеся выше, обеспечивают более «общую» защиту, т.е. они направлены на целый диапазон угроз и обеспечивают защиту путем поддержки общего эффективного менеджмента информационной безопасности. Поэтому они не перечисляются здесь, но их эффект не следует недооценивать, и они должны реализовываться для обеспечения общей эффективной защиты.

Учетностъ

Для обеспечения защиты учетности должны рассматриваться любые угрозы, которые могут приводить к предпринимаемым действиям, которые не могут быть приписаны конкретной сущности или субъекту.

Примерами таких угроз являются коллективное использование учетной записи, отсутствие прослеживаемости действий, имитация личности пользователя, сбой программы, несанкционированный доступ к компьютерам, данным, сервисам и приложениям и слабая аутентификация.

Существуют **два вида учетности**, которые следует рассматривать.

Один из них имеет дело с **идентификацией пользователя**, ответственного за определенные действия по отношению к информации и системам ИКТ.

Это могут обеспечивать контрольные журналы. Другой вид связан с **учетностью между пользователями** в системе. Услуги неотказуемости, разделенное знание или двойной контроль могут достигать этого.

Многие средства контроля могут использоваться для осуществления учетности или могут способствовать ее осуществлению. Могут быть применимы средства контроля, простирающиеся от таких вещей, как политики безопасности, повышение осознания безопасности, логический контроль доступа и аудит, до одноразовых паролей и средств контроля носителей данных. Реализация политики в отношения владения информацией является необходимым условием учетности. Выбор определенных средств контроля будет зависеть от конкретного использования учетности в рамках данной сферы.

Подлинность

Уверенность в подлинности может быть снижена любой угрозой, которая может приводить к неуверенности человека, системы или процесса в том, что объект является таким, как подразумевается.

Некоторые примеры, которые могут приводить к возникновению такой ситуации, включают не контролируемые изменения данных, не проверяемый источник данных, не поддерживаемый источник данных.

Многие средства контроля могут использоваться для обеспечения подлинности или могут способствовать ее обеспечению. Могут быть применимы средства контроля, простирающиеся от использования данных с помеченной ссылкой, логического контроля доступа и аудита до использования цифровых подписей. Выбор определенных средств контроля будет зависеть от конкретного использования подлинности в рамках данной сферы.

Надежность

Любая угроза, которая может приводить к несоответствующему поведению систем или процессов, будет

давать в результате снижение надежности. Некоторыми примерами таких угроз являются несоответствующее функционирование системы и ненадежные поставщики. Потеря надежности может приводить к плохому обслуживанию клиентов или утрате доверия клиентов. Многие средства контроля могут использоваться для обеспечения надежности или могут способствовать ее обеспечению. Могут быть применимы средства контроля, простирающиеся от таких вещей, как планы обеспечения деловой непрерывности, введение избыточности в физическую архитектуру и техническое обслуживание системы до идентификации и аутентификации и логического контроля доступа и аудита. Выбор определенных средств контроля будет зависеть конкретного использования надежности в рамках данной сферы.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Основные понятия и задачи информационной безопасности.
2. Политика информационной безопасности.
3. В чём состоят национальные интересы РФ?
4. В чем состоят интересы личности , общества и государства
5. Национальные интересы во внутриполитической сфере - это?
6. Национальные интересы в социальной сфере – это?
7. Национальные интересы в духовной сфере - это?
8. Национальные интересы в международной сфере – это?
9. Национальные интересы в информационной сфере - это?
10. Национальные интересы в военной сфере – это?
11. Национальные интересы в пограничной сфере - это?
12. Национальные интересы в экологической сфере это ?
13. Назовите Причины возникновения внутренних и внешних угроз национальной безопасности? Каковы их последствия?
14. Перечислите угрозы национальной безопасности России в социальной сфере..
15. Перечислите угрозы в международной сфере
16. Перечислите угрозы национальной безопасности РФ в информационной сфере.
17. Перечислите угрозы в военной сфере.
18. Перечислите угрозы национальной безопасности и интересам РФ в пограничной сфере.
19. Перечислите угрозы в экологической сфере.
20. Каковы важнейшие задачи обеспечения ИБ в РФ.
21. Каковы причины проблем обеспечения безопасности информационных технологий

22. На каких принципах основывается Государственная политика обеспечения ИБ РФ
23. Перечислите национальные интересы в информационной сфере.
24. Перечислите интересы личности общества и государства в информационной сфере.
25. Каковы угрозы национальным интересам РФ в информационной сфере
26. Назовите источники угроз ИБ РФ.
27. В чем состоит государственная информационная политика РФ. Основные положения.
28. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации - это
29. Информационные ресурсы современного общества - это
30. Информационное противоборство – это?
31. Какую цель преследует информационное противоборство?
32. Каковы основные способы достижения целей в информационном противоборстве?
33. Что такое информационная операция (война)?
34. Какие классификации угроз информационной безопасности вам известны?
35. Дать понятие модели нарушителя
36. Каковы возможностей внутреннего нарушителя?
37. Преднамеренные угрозы – это
38. Как реализуются информационные угрозы?
39. Как реализуются физические угрозы?
40. Как реализуются организационные угрозы?
41. Какова системная классификация угроз безопасности информации?
42. Какие составляющие должны присутствовать в модели угроз и нарушителей?

43. Какие каналы несанкционированного получения информации вам известны?
44. На какие классы подразделяются угрозы информационной безопасности согласно различным документам по обеспечению ИБ?
45. Перечислите угрозы для объектов критических сегментов информационной инфраструктуры.
46. Перечислите различные типы кибератак
47. Что такое уязвимости? Какие уязвимости вам известны?
48. Каким законом регулируются вопросы, связанные со стандартизацией в Российской Федерации?
49. Каким органом осуществляет техническое регулирование и по стандартизации?
50. Основополагающим государственным стандартом Российской Федерации в области защиты информации является…
51. На какие категории подразделяют стандарты по ЗИ?
52. В чём состоят зарубежные стандарты в области информационной безопасности со
53. В чем состоят Европейские критерии безопасности информационных технологий
54. В чём состоят Американские Федеральные критерии безопасности информационных технологий
55. В чем состоят Общие критерии безопасности информационных технологий.
56. В чём состоят руководящие документы Гостехкомиссии (ФСТЭК) России.
57. Назовите сервисы безопасности? Дать характеристику каждому.
58. Из каких составляющих складываются меры обеспечения ИБ ?
59. Какие существуют средства контроля конфиденциальности?
60. Какие существуют средства контроля целостности?

61. Какие существуют средства контроля доступности?
62. Какие существуют средства контроля учетности, подлинности и надежности?

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Варфоломеев А.А. Основы информационной безопасности: Учеб. пособие. – М.: РУДН, 2008. – 412 с.: ил.
2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. Учебное пособие для вузов, М.: Горячая линия – Телеком, 2006.- 544 с.
3. Семкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учеб. пособие. – М.: Гелиос АРВ, 2005.- 192 с.

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК