Домашняя работа:  
 **Информационная инфраструктура (ПО ГОСТ Р 53114-2008)** — это совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам.

**Документ (ПО ГОСТ Р 7.0.8-2013)** — это зафиксированная на носителе информация с реквизитами, позволяющими ее идентифицировать.

**Автоматизированная система (ПО ГОСТ 34.003-90) (AC)** — это система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций

**Информационные активы (information asset)** — информационные ресурсы или средства обработки информации организации - ГОСТ Р ИСО/ТО 13569-2007

Перехвату информации предшествует созданная намеренно утечка информации.

Сведения, которые важны для перехватчика:

* Работающие на рынке услуг
* Обладающие большим массивом персональных данных
* Использующие в своей работе ноу-хау

Таким образом, информация в настоящее время является соседством достижения определенных целей, которые могут использовать злоумышленники для получения какого-либо преимущества.

Информация может утекать по разным способам утечки информации

* Визуальные способы
* Акустические способы
* Электромагнитный способ
* Акустоэлектрический способ
* Материальный способ – анализ предметов, документов, отходов деятельности компании

Визуально-оптические средства – уменьшить можно по-разному: шторки, маленькие углы обзора, светоотражающая краска

Мы защищаем только осязаемые объекты информатизации.

Домашняя работа:

**Защита программных средств** - организационные, правовые, технические и технологические меры, направленные на предотвращение возможных несанкционированных действий по отношению к программным средствам и устранение последствий этих действий (ГОСТ Р 51188-98)

**Профилактика** - систематические действия эксплуатационного персонала, цель которых - выявить и устранить неблагоприятные изменения в свойствах и характеристиках используемых программных средств, в частности проверить эксплуатируемые, хранимые и (или) вновь полученные программные средства на наличие компьютерных вирусов. (ГОСТ Р 51188-98)

**Вакцинирование** - обработка файлов, дисков, каталогов, проводимая с применением специальных программ, создающих условия, подобные тем, которые создаются определенным компьютерным вирусом, и затрудняющих повторное его появление. (ГОСТ Р 51188-98)

**Компьютерный вирус** - программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам. (ГОСТ Р 51188-98)

# Компьютерные вирусы. Средства защиты

Компьютерный вирус можно назвать саморепродуцирующийся программой. Программа, попав в систему, наносит большой вред ПО.

В 20 веке был представлен класс саморепродуцирующихся программ, который походил на биологический вирус. Это был 1984. Это программа, обладающая способностью репродукции и способностью выполнять какие-либо вычисления. Особенность компьютерных вирусов такова, что она саморепродуцируются в другую программу только в том случае, если по отличительным признакам эта программа еще не содержит копии вируса.

Зараженная программа запускает копию вируса и тем самым порождает процесс его распространения. По утверждению Докутра Ковена компьютерный вирус определяется, как программа, которая может заражать другие программы, модифицируя их посредством

Стадии существования вируса

* Спячка
* Распространение в вычислительной системе – это обязательная для любой программы
* Запуск – программируемое событие параметров запуска
* Нарушение работы программ или данных или другие отрицательные действия – прописываются как зависимые или независимые

Д/З

**Биометрическая характеристика (biometric characteristic):** Измеряемая физическая характеристика или индивидуальный поведенческий признак, при помощи которого можно идентифицировать или верифицировать предъявляемую идентификационную информацию зарегистрированного пользователя –ГОСТ Р ИСО/МЭК 24713-2-2011

**Требования к соответствию (ПО ГОСТ Р 29109-1-2012)** – это требование, установленное в базовом стандарте, устанавливающее необходимое условие в краткой и точно выраженной форме.

Комплект для проведения испытаний на соответствие (ПО ГОСТ Р 29109-1-2012)- это программное обеспечение, применяемое для автоматизации однотипных испытаний на соответствие.

**Испытания уровня 1(ПО ГОСТ Р 29109-1-2012)** – это метод испытания на соответствие, при котором осуществляют побайтовый и поэлементный контроль соответствия спецификации записи для обмена биометрическими данными, определенной в базовом стандарте, на основе как присутствующих полей, так и диапазонов значений этих полей.

# Российское законодательство во области ИБ.

Входит конституция, уголовный кодекс, административный кодекс, закон об информатизации и информации №149 ФЗ. Данный закон дал основные понятия (информационная система, информация и т.д.). Также данный закон говорит о том что документ подтвержденный электронной подписью является юридически сильным. Чтобы признать юридическую силу документа необходимо наличие программно-технических средств, обеспечивающих идентификацию подписей.

Закон №99 ФЗ Дает такие понятия как: лицензия, лицензирование, лицензированный вид деятельности и другие. Закон устанавливает перечень видов деятельности на осуществление которых требуется лицензия. К этим относиться: распространение услуг в области шифрования и разработки, производство шифровальных средств и другие виды. ВСТЕК регулирует все что связанно с лицензии, все что связанно с шифрованием регулирует ФСБ.

Важную роль играет закон об участие в международном информационном обмене. Он также позиционирует основное средство защиты, имеющее лицензию и сертификат. Говорит о том, что защита конфиденциальной информации распространяется на деятельность распространяется на деятельность осуществляемой юридическими и физическими лицами обладающими лицензию на данный вид деятельности.

# Стандарты и спецификация

Д/з риски:

**Сравнительная оценка рисков**

Сравнительная оценка риска (ГОСТ Р 51897-2011) – это процесс сравнения результатов анализа риска с критериями риска для определения приемлемости риска.

Сравнительная оценка риска включает в себя сопоставление уровня риска с критериями риска, установленными при определении области применения менеджмента риска, для определения типа риска и его значимости.

Сравнительная оценка риска использует информацию о риске, полученную при анализе риска. Ре- зультаты сравнительной оценки риска используют для принятия решений о будущих действиях. Этические, юридические, финансовые и другие вопросы, а также восприятие риска организацией могут повлиять на принятие решения.

Принимаемые решения могут касаться таких вопросов как: - необходимость обработки риска;  
- приоритеты обработки риска;  
- необходимость выполнения действий;  
- выбор способа обработки риска.

Характер принимаемых решений и используемые критерии при принятии решений ранее установлены при определении области применения, однако на данном этапе они должны быть повторно и более подроб- но рассмотрены с точки зрения уже полученных данных об идентифицированных опасностях и риске.

Наиболее простая структура для определения критериев риска — это установление одного уровня, разделяющего опасности и риск, требующие обработки, от тех, которые подобных действий не требуют. Применение такой структуры приводит к простым и понятным результатам, однако не отражает неопреде- ленность, присущую оценке риска и установленному пограничному уровню риска.

Решение о необходимости и способах обработки риска зависит от затрат и преимуществ принятия риска и улучшения управления риском.

В соответствии с общим подходом следует разделить риск на три группы.

a) Высшая группа, в которой уровень риска является недопустимым, безотносительно преимуществ принятия риска и доходов, получаемых от деятельности организации, обработка риска является необходи- мой независимо от затрат.

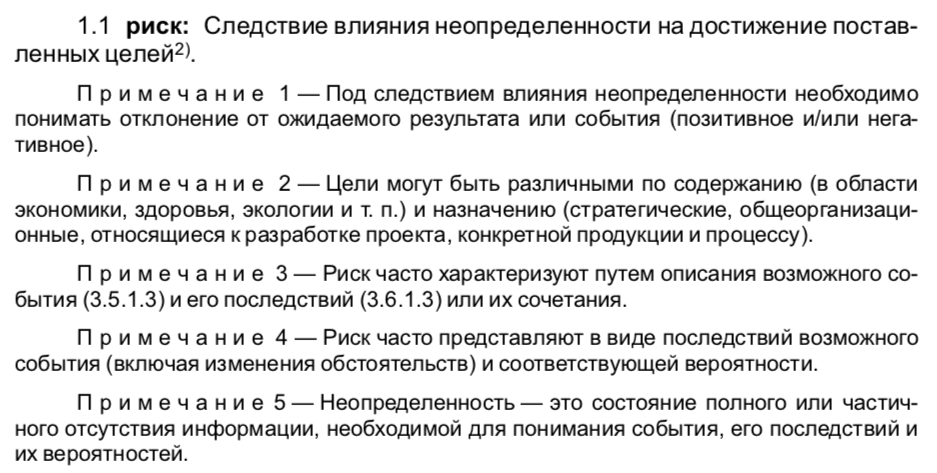
b) Средняя группа («серая» область), для которой затраты и преимущества принятия риска следует учитывать, а возможности соотносить с последствиями.

c) Низшая группа, в которой уровень риска незначителен или настолько мал, что необходимость в обработке риска отсутствует.

Для отнесения риска к низшей группе, используемой в сфере безопасности (в системе критериев ALARP1) — «Низкий, насколько реально возможно»), применяют следующий подход.

Для отнесения риска к низшей группе («Низкий, насколько реально возможно» в системе критериев ALARP1) ), используемой в сфере безопасности, применяют следующий подход: для низкого риска в средней группе устанавливают скользящую шкалу, в которой затраты и преимущества могут быть непосредственно сопоставлены, а возможный вред от событий с высоким риском следует снижать до тех пор, пока стоимость дальнейшего снижения риска не превысит полученные преимущества.

**ГОСТ Р ИСО/МЭК 31010 — 2011**

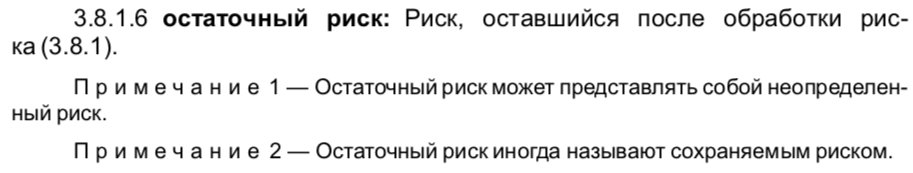
**Предпочтительный риск**: тип риска и его уровень, к которому организация стремится или готова поддержать

**ГОСТ Р 51897-2011**

**Исключение риска** (англ: risk avoidance, фр: refus du risque) — решение об исключении угрозы появления опасной ситуации или действий, связанных с возможностью ее возникновения.

**ГОСТ Р 51897-2011**

**Остаточный риск**



**ГОСТ Р 51897—2011**

Стандарты бывают двух видов: Оценочные стандарты – определяют классификацию информационных систем и средств защиты – регламентируют основы реализации средств защиты.

# Административный уровень информационной безопасности

Д/з

**Отчетность о риске** (англ: risk reporting, фр: rapport sur les risque) — форма обмена информацией о риске, предусматривающая информирование соответствующих внутренних и внешних причастных сторон путем предоставления информации о текущем состоянии риска и менеджменте риска.

**ГОСТ Р 51897-2011**

**Устойчивость организации** (ГОСТ Р 51897-2011) – это способность организации к адаптации в сложной и изменчивой окружающей среде.

**Обработка риска (воздействие на риск**): Процесс модификации (изменения) риска.

Примечание 1 - Обработка риска может потребовать:

- избежание риска путем принятия решения не начинать (не продолжать) действия, порождающего риск;

- удаление источника риска;

- изменение оценки вероятности наступления события;

- изменение оценки последствий;

- разделение риска с другими заинтересованными сторонами (включая контракты и финансирование рисков);

- поддержка ранее принятого информированного решения о риске.

Примечание 2 - Обработка рисков, связанных с негативными последствиями, иногда рассматривается как "смягчение риска", "устранение риска", "предотвращение риска", "уменьшение риска".

Примечание 3 - Обработка риска может привести к новому риску или модифицировать существующий риск.

**ГОСТ Р 56275-2014**

Административный уровень информационной безопасности – действия общего характера, выполняемые в организации. Основные действия направлены на обеспечение политики безопасности, выражающейся в деятельности, направленной на защиту информационных активов. Каждой компании необходимо проводить мероприятия по обучению персонала с соблюдением режима безопасности, поддержание режима безопасности и обеспечению мероприятий финансовыми ресурсами.

В политику безопасности входит комплект организационно-распределительных решений, выраженных в документационном выражении, обеспечивающий поддержание внутреннего порядка информационной безопасности.

В применении к домашнему заданию:

Для снижения опасных последствий и событий, каждая компания принимает процессы по менеджменту риска и внедряет в деятельность компании менеджмент системы обеспечения информационной безопасности.

Т.е. лицо, которое причастно к управлению риском или его воздействию может быть как стороной являющейся жертвой риска, так и стороной управления риском.

Принятие решения о качестве риска и его состояний выполняется на уровне руководства компании.

**Д/з**

**Анализ средств и целей** – это процесс решения задачи, когда на каждом шаге производится поиск операций, которые максимально сокращают разность между текущим состоянием и известным целевым состоянием.

**ГОСТ 33707-2016**

**Аудит безопасности автоматизированной информационной системы** – это проверка реализованных в автоматизированной информационной системе процедур обеспечения безопасности с целью оценки их эффективности и корректности, а также разработки предложений по их совершенствованию.

**ГОСТ 33707-2016**

**Альтернативное планирование** - это планирование, в котором в разрабатываемый план включаются альтернативные действия процесса решения задачи.

**ГОСТ 33707-2016**

**Буферизация входных и выходных потоков** – это использование вспомогательной памяти в качестве буферной памяти для уменьшения задержек обработки, при передаче данных между периферийным устройством и процессорами вычислительной машины.

**ГОСТ 33707-2016**

# Реагирование на нарушение безопасности информации (системной безопасности)

В каждой организации существует политика безопасности. Один из разделов политики информационной безопасности должен включать перечень мероприятий по обнаружению и устранению нарушений режима информационной безопасности. Необходимо для реализации заданных мероприятий составлять внутренний документ планирования мероприятий обнаружения и нейтрализации нарушений информационной безопасности.

Цели процессов реакции на нарушения:

1. Быстрая локализация инцидентов, следовательно, уменьшение наступающих последствий
2. Обнаружение нарушителя
3. Создание порядка предупреждения повторных нарушений

Для организации действий:

1. Необходима постоянная доступность специалиста, который в любой момент дня и ночи может сделать план для дальнейшей работы с проблемами. Данная процедура очень похожа на порядок действий при пожаре.

Существуют сети из двух сегментов. Каждый сегмент администрируется своим администратором. Один из сегментов заразился вирусом. В данной ситуации необходимо приятие быстрых мер.

После немедленного прекращения всей работы, необходимо запустить процедуру лечения на обоих сегментах сети.

Требования по локализации инцидента могут вступать в конфликт с процедурой по выявлению нарушителя. Чтоб конфликтов не было, необходимо расставить приоритеты. Статистика говорит о том, что выявление нарушителя более сложная задача, чем локализация инцидента.

Для предотвращения повторных нарушений необходимо проводить работу по анализу условий и параметров инцидента накапливают статистические сведения о ситуации и формировать базу данных инцидента.

**Восстановление**

Каждая организация в политике безопасности имеет критически важные функции, выполнение которых должно обеспечиваться в любых условиях. В связи с тем, что от серьёзных нарушений не застрахована не одна организация, необходимо организовывать планирование восстановительных работы что позволит организации быть готовой к всевозможным авариям и нарушениям, уменьшить ущерб и сохранить работоспособность.

Д/з

**Исключение нарушения защиты** – это исключение, возникающее при попытке доступа программы к защищенной области запоминающего устройства.

**ГОСТ 33707-2016**

**Конфигурация системы обработки информации** – это совокупность процессов информационной системы и способов взаимосвязи этих процессов.

**ГОСТ 33707-2016**

**Автоматическая обработка данных** – это обработка данных, выполняемая автоматически, без участия человека. Техническим средством обработки может быть ЭВМ или иные устройства, машины.

**ГОСТ 33707-2016**

**Информационная модель предметной области** – это модель, описывающая общие понятия и связи между ними для данной предметной области.

**ГОСТ Р 56843-2015**

**Д/з**

Что необходимо при использовании менеджмента инцидента.

Какие мероприятия включает в себя работа на этапе улучшения безопасности?

Что такое улучшение безопасности?

Улучшение безопасности  – это структурный процесс обнаружения, оповещения, оценки и менеджмента инцидентов и событий ИБ, позволяет быстро идентифицировать любое событие или инцидент ИБ и реагировать на них, тем самым улучшая общую безопасность за счет быстрого определения и реализации правильного решения, а также обеспечивая средства предотвращения подобных инцидентов ИБ в будущем.

**ГОСТ Р 18044-2007**

Менеджмент инцидентов – это процесс, включающий в себя не только технические средства, но также персонал, и, следовательно, этот процесс должен поддерживаться лицами, соответствующим образом обученными для работы в организации и осведомленными в вопросах безопасности информации.

**ГОСТ Р 18044-2007**

При использовании системы менеджмента инцидентов ИБ необходимо осуществить следующие процессы:

- обнаружение и оповещение о возникновении событий ИБ (человеком или автоматическими средствами);

- сбор информации, связанной с событиями ИБ, и оценка этой информации с целью определения, какие события можно отнести к категории инцидентов ИБ;

- реагирование на инциденты ИБ:

- немедленно, в реальном или почти реальном масштабе времени;

- если инциденты ИБ находятся под контролем, выполнить менее срочные действия (например, способствующие полному восстановлению после катастрофы);

- если инциденты ИБ не находятся под контролем, то выполнить "антикризисные" действия (например, вызвать пожарную команду/подразделение или инициировать выполнение плана непрерывности бизнеса);

- сообщить о наличии инцидентов ИБ и любые относящиеся к ним подробности персоналу своей организации, а также персоналу сторонних организаций (что может включить в себя, по мере необходимости, распространение подробностей инцидента с целью дальнейшей оценки и (или) принятия решений);

- правовую экспертизу;

- надлежащую регистрацию всех действий и решений для последующего анализа;

- разрешение проблемы инцидентов.

**ГОСТ Р 18044-2007**

Необходимо подчеркнуть, что процессы менеджмента инцидентов ИБ являются итеративными, с постоянным внесением улучшений с течением времени в ряд элементов ИБ. Эти улучшения предлагаются на основе данных об инцидентах ИБ и реагировании на них, а также данных о динамике тенденций. Этап "Улучшение" включает в себя:

- пересмотр имеющихся результатов анализа рисков ИБ и анализ менеджмента организации;

- улучшение системы менеджмента инцидентов ИБ и ее документации;

- инициирование улучшений в области безопасности, включая внедрение новых и (или) обновленных защитных мер ИБ.

# Стандарты и спецификации

Этот стандарт является основным стандартом, охватившим различные вопросы и определяющим инструменты оценки безопасности информационных систем.

Часть 1 – Введение и общая модель

Часть 2 – функциональные компоненты безопасности

Часть 3 – компоненты доверия безопасности

Общие критерии содержат основные виды требований, предъявляемые функциям безопасности, требование доверия, они соответствуют пассивным началам предъявляемым технологиям.

Необходимо проверять выполнение их для конкретного объекта. Исходя из этапов жизненного цикла можно выделить этапы оценки:

* определение назначения, применения и требование безопасности.
* работы по проектированию систем.
* Этап испытаний и сертификации.
* Проведение внедрения и эксплуатации.

Необходимо минимизировать ущерб устраняя слабые места объекта оценки. Для того чтобы выполнить структурирование в пространстве, в общих критериях существует иерархия, сначала определяется класс, далее семейство, затем компонент и уже самый минимальный – элемент.

В этой иерархии больший элемент представляет классы, таким образом имея библиотеки классы, могут формироваться 2 вида нормативного документа.

Формируется 2 вида документа. Требования к определенным решениям, продукту, выполнение которых обеспечивает достижение целей.

Все классы подразделяются на группы, которые отличаются особенностями обработки информации.

# Законодательный уровень ИБ

В деле обеспечения информационной безопасности успех может принести только комплексный подход. Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

* законодательного;
* административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
* процедурного (меры безопасности, ориентированные на людей);
* программно-технического.

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это наказывается обществом.

Различают две группы мер на законодательном уровне:

* меры, направленные на создание и поддержание в обществе негативного отношения к нарушениям и нарушителям информационной безопасности
* направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности.

Самое важное и трудное на законодательном уровне - создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

Д/з

**Управляющая программа** - Системная программа, реализующая набор функций управления, в который включают управление ресурсами и взаимодействие с внешней средой системы обработки информации, восстановление работы системы после проявления неисправностей в технических средствах.

**ГОСТ 19781-90**

**Программа обслуживания** - Программа, предназначенная для оказания услуг общего характера пользователям и обслуживающему персоналу системы обработки информации.

**ГОСТ 19781-90**

**Драйвер** - Программа, предназначенная для управления работой периферийных устройств, обычно в мини- и микроЭВМ.

**ГОСТ 19781-90**

**Макроопределения** - Программа, под управлением которой макрогенератор порождает макрорасширения макрокоманд

**ГОСТ 19781-90**

# Компьютерное преступление. Криминалистика.

Компьютерные преступления могут быть разделены на несколько групп:

* Преступления, которые направлены против технических средств
* Преступления, которые используют технические средства
* Преступления, когда компьютер используется в качестве запоминающего устройства – формируется место хранения – директория для фиксации списка украденных номеров, паролей или других файлов

Основная проблема киберпреступлений заключается в их расследовании. Противоправные действия может длиться очень быстро (несколько милсек), а подготовка к выполнению незаконного действия может быть от месяца до нескольких лет. Сбор фактов, имеющих отношение к компьютерному преступлению и важных для расследования, также может длиться достаточно долгое время. Возможность неполучения таких фактов тоже существует. Причины:

* Преступник профессионально скрывает следы.
* Потерпевший не хочет возбуждать уголовное дело.

Современных подход к обучению компьютерных технологий, стремительный рост компьютерных технологий – все это говорит о повышенной опасности реализации компьютерных преступлений.

Компьютерное преступление – это деяние, совершаемое лицами без права на то с целью получения информации на коммерческое использование. За совершение компьютерных преступлений предусматривается уголовная ответственность (гл. 28 УК РФ)

Д/з

Разработка системы менеджмента информационной безопасности (СМИБ)

Внедрение и обеспечение функционирования СМИБ

Проведение мониторинга и анализа

Поддержка и улучшение СМИБ – что за действия?

**ГОСТ Р ИСО/МЭК 27001-2006**

**4.2.1 Разработка системы менеджмента информационной безопасности**  
  
Организация должна осуществить следующее:

a) определить область и границы действия СМИБ с учетом характеристик бизнеса, организации, ее размещения, активов и технологий, в том числе детали и обоснование любых исключений из области ее действия (см. 1.2);

b) определить политику СМИБ на основе характеристик бизнеса, организации, ее размещения, активов и технологий, которая:

1) содержит концепцию, включающую в себя цели, основные направления и принципы действий в сфере ИБ;

2) принимает во внимание требования бизнеса, нормативно-правовые требования, а также договорные обязательства по обеспечению безопасности;

3) согласуется со стратегическим содержанием менеджмента рисков организации, в рамках которого будет разрабатываться и поддерживаться СМИБ;

4) устанавливает критерии оценки рисков [см. 4.2.1, перечисление с)];

5) утверждается руководством организации.  
  
**Примечание** - Для целей настоящего стандарта политика СМИБ имеет приоритет перед политикой ИБ. Эти политики могут быть изложены в одном документе;

c) определить подход к оценке риска в организации, для чего необходимо:

1) определить методологию оценки риска, подходящую для СМИБ, которая должна соответствовать требованиям обеспечения деятельности организации и нормативно-правовым требованиям информационной безопасности;

2) разработать критерии принятия риска и определить приемлемые уровни риска [см. 5.1, перечисление f)].  
  
Выбранная методология оценки риска должна обеспечивать сравнимые и воспроизводимые результаты.  
  
Примечание - Имеются различные методологии оценки риска. Примеры таких методологий даны в ИСО/МЭК ТО 13335-3:1998 "Руководство по управлению безопасностью информационных технологий. Часть 3. Методы управления безопасностью информационных технологий" [7];

d) идентифицировать риски, для чего необходимо:

1) идентифицировать активы в пределах области функционирования СМИБ и определить владельцев\* этих активов;  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
\* Здесь и далее термин "владелец" определяет лицо или организацию, которые имеют утвержденные руководством обязательства по контролю за производством, разработкой, поддержкой, использованием и безопасностью активов. Термин "владелец" не означает, что лицо действительно имеет какие-либо права собственности на актив.

2) идентифицировать угрозы этим активам;

3) идентифицировать уязвимости активов, которые могут быть использованы угрозами;

4) идентифицировать последствия воздействия на активы в результате возможной утраты конфиденциальности, целостности и доступности активов;

e) проанализировать и оценить риски, для чего необходимо:

1) оценить ущерб для деятельности организации, который может быть нанесен в результате сбоя обеспечения безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности или доступности активов;

2) оценить реальную вероятность сбоя обеспечения безопасности с учетом превалирующих угроз, уязвимостей и их последствий, связанных с этими активами, а также с учетом применяемых мер управления безопасностью;

3) оценить уровни рисков;

4) определить, являются ли риски приемлемыми или требуют обработки с использованием критериев допустимости рисков, установленных в 4.2.1, перечисление с);

f) определить и оценить различные варианты обработки рисков.  
  
Возможные действия:

1) применение подходящих мер управления;

2) сознательное и объективное принятие рисков при условии, что они полностью соответствуют требованиям политики и критериям организации в отношении принятия рисков [см. 4.2.1, перечисление, с), 2)];

3) избежание рисков;

4) передача соответствующих деловых рисков сторонним организациям, например страховщикам или поставщикам;

g) выбрать цели и меры управления для обработки рисков.  
  
Цели и меры управления должны быть выбраны и реализованы так, чтобы удовлетворять требованиям, определенным в процессе оценки и обработки рисков. Этот выбор должен учитывать критерии принятия рисков [см. 4.2.1, перечисление с), 2)], а также нормативно-правовые требования и договорные обязательства.  
  
Цели и меры управления должны быть выбраны согласно приложению А как часть процесса оценки и обработки рисков и соответствовать требованиям этого процесса.

Перечень целей и мер управления, приведенный в приложении А, не является исчерпывающим, а потому могут быть выбраны дополнительные цели и меры управления.  
  
Примечание - Приложение А содержит подробный перечень целей и мер управления, обычно используемых в организациях. Рекомендуется использовать этот перечень в качестве исходных данных, позволяющих выбрать рациональный вариант мер управления и контроля;

h) получить утверждение руководством предполагаемых остаточных рисков;

i) получить разрешение руководства на внедрение и эксплуатацию СМИБ;

j) подготовить Положение о применимости, которое включает в себя следующее:

1) цели и меры управления, выбранные в 4.2.1, перечисление g), и обоснование этого выбора;

2) цели и меры управления, реализованные в настоящее время [см. 4.2.1, перечисление е), 2)];

3) перечень исключенных целей и мер управления, указанных в приложении А, и процедуру обоснования их исключения.  
  
Примечание - Положение о применимости содержит итоговые решения, касающиеся обработки рисков. Обоснование исключений предусматривает перекрестную проверку, позволяющую определить, что ни одна мера управления не была случайно упущена.

**ГОСТ Р ИСО/МЭК 27001-2006**

**4.2.2 Внедрение и функционирование системы менеджмента информационной безопасности**  
  
Организация должна выполнить следующее:

a) разработать план обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении менеджмента рисков ИБ (см. раздел 5);

b) реализовать план обработки рисков для достижения намеченных целей управления, включающий в себя вопросы финансирования, а также распределение функций и обязанностей;

c) внедрить меры управления, выбранные согласно 4.2.1, перечисление g), для достижения целей управления;

d) определить способ измерения результативности выбранных мер управления или их групп и использования этих измерений для оценки результативности управления с целью получить сравнимые и воспроизводимые данные [см. 4.2.3, перечисление с)].  
  
Примечание - Измерение результативности мер управления позволяет руководителям и персоналу определить, в какой степени меры управления способствуют достижению намеченных целей управления;

e) реализовать программы по обучению и повышению квалификации сотрудников (см. 5.2.2);

f) управлять работой СМИБ;

g) управлять ресурсами СМИБ (см. 5.2);

h) внедрить процедуры и другие меры управления, обеспечивающие быстрое обнаружение событий ИБ и реагирование на инциденты, связанные с ИБ [см. 4.2.3, перечисление а)].

**ГОСТ Р ИСО/МЭК 27001-2006**

**4.2.3 Проведение мониторинга и анализа системы менеджмента информационной безопасности**  
  
Организация должна осуществлять следующее:

a) выполнять процедуры мониторинга и анализа, а также использовать другие меры управления в следующих целях:

1) своевременно обнаруживать ошибки в результатах обработки;

2) своевременно выявлять удавшиеся и неудавшиеся попытки нарушения и инциденты ИБ;

3) предоставлять руководству информацию для принятия решений о ходе выполнения функций по обеспечению ИБ, осуществляемых как ответственными лицами, так и информационными технологиями;

4) способствовать обнаружению событий ИБ и, таким образом, предотвращать инциденты ИБ путем применения средств индикации;

5) определять, являются ли эффективными действия, предпринимаемые для устранения нарушения безопасности;

b) проводить регулярный анализ результативности СМИБ (включая проверку ее соответствия политике и целям СМИБ и анализ мер управления безопасностью) с учетом результатов аудиторских проверок ИБ, ее инцидентов, результатов измерений эффективности СМИБ, а также предложений и другой информации от всех заинтересованных сторон;

c) измерять результативность мер управления для проверки соответствия требованиям ИБ;

d) пересматривать оценки рисков через установленные периоды времени, анализировать остаточные риски и установленные приемлемые уровни рисков, учитывая изменения:

1) в организации;

2) в технологиях;

3) в целях деятельности и процессах;

4) в выявленных угрозах;

5) в результативности реализованных мер управления;

6) во внешних условиях, например, изменения нормативно-правовых требований, требований договорных обязательств, а также изменения в социальной структуре общества;

е) проводить внутренние аудиты СМИБ через установленные периоды времени (см. раздел 6).  
  
Примечание - Внутренние аудиты, иногда называемые аудитами первой стороны, проводятся самой организацией (или внешней организацией от ее имени) для собственных целей;

f) регулярно проводить руководством организации анализ СМИБ в целях подтверждения адекватности ее функционирования и определения направлений совершенствования (см. 7.1);

g) обновлять планы ИБ с учетом результатов анализа и мониторинга;

h) регистрировать действия и события, способные повлиять на результативность или функционирование СМИБ, в соответствии с 4.3.3.

**ГОСТ Р ИСО/МЭК 27001-2006**

**4.2.4 Поддержка и улучшение системы менеджмента информационной безопасности**  
  
Организация должна регулярно осуществлять следующее:

a) выявлять возможности улучшения СМИБ;

b) предпринимать необходимые корректирующие и предупреждающие действия, использовать на практике опыт по обеспечению ИБ, полученный как в собственной организации, так и в других организациях;

c) передавать подробную информацию о действиях по улучшению СМИБ всем заинтересованным сторонам, при этом степень ее детализации должна соответствовать обстоятельствам и, при необходимости, согласовывать дальнейшие действия;

d) обеспечивать внедрение улучшений СМИБ для достижения запланированных целей.

**ГОСТ Р ИСО/МЭК 27001-2006**

# Пресечение разглашения конфиденциальной информации

Пресечение и разглашение конфиденциальной информации – комплекс мероприятий исключающих разглашение защищаемых сведений их владельцами.

Ошибки в обмене информации. Тем самым представляя возможности. лояльность служащих, которые поддаться подкупу конкурентов, ужесточение дисциплины приводит к утечки данных. Такой подход высокотехнологичных отраслей.

Стратегия предприятий, результаты исследований, списки клиентов, торговля. Список поданных заявок на патент. Разглашение – это умышленной или не осторожное действие сотрудников или должностных лиц. Оглашение информации, в следствии чего информацию получают лица не уполномоченные к ее просмотру.

Оглашение выражается в сообщении, передачи, пересылке, опубликовании или каких то потерь деловой и научной информации. При наличии определенных условий, нарушение правил обращения с конфиденциальными документами

Факторы разглашения информации:

* Недостаточные знания
* Непонимание важности тщательного их выполнения
* Слабый недостаточный контроль соблюдения правила работы конфиденциальных сведений
* Повышенная текучка кадров

Для основы защиты надо:

* Принцип минимализма допуска лиц к информации
* Принцип сохранения информации
* Строгое соответствие законодательству

# Концепция комплексной защиты информации

Стадии информации

Документальная – формализованное отображение информации на бумажных носителях и других носителях информации.

Электронная – информация находящейся в АИС с возможностью ее редактирования, модификации, сохранения.

Нахождение информации в информационной структуре.

Вопрос о защите информации наиболее актуален. Ее необходимо защищать от НСД информации, а также от несанкционированного вмешательства в процесс ее разработки.

Политика информации строится таким образом, что обеспечение защиты должно применяться ко всем компонентам информационной структуры. Для обеспечения комплексного подхода к вопросам безопасности необходимо внедрение в компанию комплексной системы защиты конфиденциальной информации (КСЗИ).

Методики организационно-техническими мероприятиями системы необходимо разрабатывать по 3 основным направлениям:

* Методологическое направление;
* Организационно-правовое направление;
* Техническое направление.

На методологическом направлении необходимо решение следующих вопросов:

1. Создание комплексной безопасности;
2. Обеспечение работы планирования комплексной системы защиты информации;
3. Разработка плана внедрения работ комплексной системы защиты информации;
4. Учитывать принципы построения комплексной системы;

Существует несколько принципов:

1. Принцип комплексности;
2. Работа системы должна быть непрерывной;
3. Принцип разумной достаточности.
4. Универсальности и гибкости
5. Защищенности системы от внешнего воздействия
6. Система должна быть понятна в использовании и т д

# Требования к системе защиты информации

Основное требование системы защиты заключается в необходимости идентификации всех технологий, программ и пользователей. Уровень идентификации должен быть не ниже уровня записи.

Необходимо применение следующих способов ограничений, а именно классификация доступа в соответствии с иерархией системы.

Полная идентификация информационных ресурсов и их классификация по важности и месту размещения.

Минимизация прав пользователей по доступу к информационным объектам. Все программные процедуры должны быть закреплены за конкретными пользователями. Система защиты должна обеспечивать идентификацию всех движений данных идентификации, всех действий пользователей и фиксировать все документально.

К характеристикам систем безопасности сформулированы общие требования:

* Требование к программному и аппаратному обеспечению
* Требование к архитектуре информационных систем
* Применению стратегии защиты
* Требование к затратам на поддержание ресурсов и поддержание работоспособностей мер защиты, а также программные затраты
* Требования к надежности системы защиты т.е. она должна надежно функционировать во всех режимах АИС и даже при воздействии внешних факторов (попытка взлома и т. д.)
* Требования к степени секретности - система защиты должна поддерживать несколько степеней секретности.
* Требования к уровню полномочий – система защиты должна поддерживать несколько уровней полномочий.
* Требования к продолжительности загрузки программного уровня
* Требования к процедуре подготовки средств защиты и продолжительности времени на включение информационной системы (должно быть минимальным)
* Система защиты должна реагировать на попытки несанкционированного доступа
* Должно быть рабочее место администратора.
* Система защиты должна иметь лицензии и сертификаты.

# Организационные требования

Они предусматривают реализацию административных и процедурных мер. На административном уровне необходимо выполнение требований

Контроль изменений в системе и ПО

Контроль за применением правил защиты

Мероприятия тестирования ПО

Ведение протокола действий доступа к системе

Организация систем резервного копирования

Подбор персонала, обладающим необходимыми компетенциями

Процедуры обучения обслуживающего персонала

Для обеспечения доступа к системе необходимо:

* Разработать инструкцию на установку ОС
* Должна быть разработана политика и методика восстановления системы при сбоях и отказах
* Определить объем выдаваемой информации по запросам.
* Разработать документ для ведения протоколов использования автоматизированных систем
* Разработать процедуру отчистки архивных хранилищ от вышедшей из хранения информации

# Требования к подсистемам защиты

Системы защиты принято делить на несколько подсистем:

* Управление доступом к ресурсам:

1. Должна обеспечивать идентификацию, аутентификацию и контроль, должна обеспечивать управление потоками данных (информации).
2. Должна выполнять функцию отчистки оперативной памяти и временной памяти.

* Регистрация и учет действий пользователей:

1. Должна выполнять регистрацию и учет доступа в систему, запуска программ, доступа к файлам
2. Учет выдачи документов
3. Регистрация выдачи полномочий
4. Учет носителей информации
5. Сигнализация о критических событиях

* Система криптографической защиты
* Подсистема обеспечения целостности

Перечень средств, реализующих функции системы:

* Должен быть перечень функций защиты
* Должен быть перечень основных характеристик системы

# Различие понятий аутентификации, идентификации и авторизации

**Авторизация** — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.

**Аутентификация** — процесс, в ходе которого на основании пароля, ключа или какой-либо иной информации, пользователь подтверждает, что является именно тем, за кого себя выдает.

**Идентификация** — процесс, в ходе которого выясняются права доступа, привилегии, свойства и характеристики пользователя на основании его имени, логина или какой-либо другой информации о нем.

# Перспективы комплексной защиты информации

**Комплексная защита информации** – система мер по хранению информации, шифрованию, мониторингу доступа к ним. Комплексная система защиты обеспечивает защиту информации от вирусных и хакерских атак, сохранность данных при физической утрате технических систем и информации. Безопасность доступа к информационным ресурсам и процедуры восстановления информационной системы в случае остановов и повреждений.

Основное положение комплексной защиты является обратная связь от компонентов концепции и ее основе. Т.е. к основе функционирования и организации функционирования ИС.

Содержание обратной связи – это условие, при выполнении которых создаются предпосылки для выполнения наиболее эффективного решения.

Условия можно разделить на 3 класса:

* Общие методологические – создают основу для повышения эффективности управления качеством. В этом классе выделяют 2 группы:

1. Условия по осознанию проблемы
2. Условия по наличию предполагаемых решений

* Организационные – предполагают реализацию четкой организации построения автоматизированной информационной системы, ее архитектурной структуры, а также технологий автоматизированной обработки. Этак группа условий также делится на подгруппы:

1. Структурно-функциональная однозначность устройств и компонентов АИС
2. Организационное единство процессии управления, обработки, передачи, хранения и изменения информации

* Конструктивные – предлагают учет требований защиты, применяемой в архитектуре системы и технологиях её функционирования. Делится на следующие подгруппы:

1. Концептуальная – это стандартизация на уровне концепций, принципов и правил организации рассматриваемого вида деятельности. Должна предусмотреть структуризацию концепции управления и комплексной защиты автоматизации обработки данных. Структуризация концепции необходимых ресурсов. Структуризация концепции должна осуществляться взаимоувязанно.
2. Структурирование компонентов АИС -одно из важнейших условий, при котором уделяется внимание структуризации математического, программного и информационного
3. Структурирование технологий обработки информации

Условия структурированности автоматической системы заключается в том, что любая система технологическая схема обработки информации представляется 3 участками:

* Линейный участок
* Ветвящийся участок
* Циклический

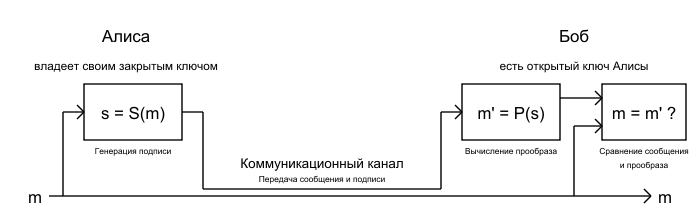
Пути реализации комплексной защиты необходимо:

* Создать разноплановые органы защиты и территориальные центры защиты
* Организовывать организационные-решения в области защиты и оказывать повседневную помощь территориальным и ведомственным центрам защиты.

Следующее важнейшее решение к вопросу о защите информации является создание регулярных систем сбора и накопления данных, относящийся к

Политика информационной безопасности: ГОСТ Р ИСО 17799

# Ключевые алгоритмы шифрования в ИБ

**Электронная подпись на основании алгоритма RSA**  
Поскольку цифровая подпись обеспечивает как аутентификацию автора сообщения, так и подтверждение целостности содержимого подписанного сообщения, она служит аналогом подписи, сделанной от руки в конце рукописного документа.

Важное свойство цифровой подписи заключается в том, что её может проверить каждый, кто имеет доступ к открытому ключу её автора. Один из участников обмена сообщениями после проверки подлинности цифровой подписи может передать подписанное сообщение ещё кому-то, кто тоже в состоянии проверить эту подпись.

**ГОСТ 28147-89** – описывает алгоритм криптопреобразования, блочный шифр с 256-битным ключом и 32 циклами (называемыми раундами) преобразования, оперирующий 64-битными блоками. Основа алгоритма шифра — сеть Фейстеля. Выделяют четыре режима работы: простой замены, гаммирование, гаммирование с обратной связью, режим выработки имитовставки.

**AES** - симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принят в качестве стандарта в США, все считают что он круче ГОСТа выше.

**DES** (англ. Data Encryption Standard) — алгоритм для симметричного шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт (FIPS 46-3).

Входными данными для блочного шифра служат:

* блок размером n бит;
* ключ размером k бит.

На выходе (после применения шифрующих преобразований) получается зашифрованный блок размером n бит, причём незначительные различия входных данных, как правило, приводят к существенному изменению результата.

**MD5** — 128-битный алгоритм хеширования. Предназначен для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности. Широко применялся для проверки целостности информации и хранения хешей паролей.

**SHA-1** – (Secure Hash Algorithm 1) — алгоритм криптографического хеширования. Алгоритм генерирует 160-битное хеш-значение, называемое также дайджестом сообщения. Используется во многих криптографических приложениях и протоколах. Принципы, положенные в основу SHA-1, аналогичны тем, которые использовались Рональдом Ривестом при проектировании MD4, который служит основной для MD5 соответственно.

**SHA-2** (Secure Hash Algorithm Version 2) — семейство криптографических алгоритмов — однонаправленных хеш-функций, включающее в себя алгоритмы SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256 и SHA-512/224.

**Хеш-функции** предназначены для создания «отпечатков» или «дайджестов» для сообщений произвольной длины. Применяются в различных приложениях или компонентах, связанных с защитой информации.

**XSS-атаки** (межсайтовый скриптинг) — тип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода (который будет выполнен на компьютере пользователя при открытии им этой страницы) и взаимодействии этого кода с веб-сервером злоумышленника. Является разновидностью атаки «внедрение кода».

Специфика подобных атак заключается в том, что вредоносный код может использовать авторизацию пользователя в веб-системе для получения к ней расширенного доступа или для получения авторотационных данных пользователя. Вредоносный код может быть вставлен в страницу как через уязвимость в веб-сервере, так и через уязвимость на компьютере пользователя.

Для термина используют сокращение «XSS», чтобы не было путаницы с каскадными таблицами стилей, использующими сокращение «CSS».