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.

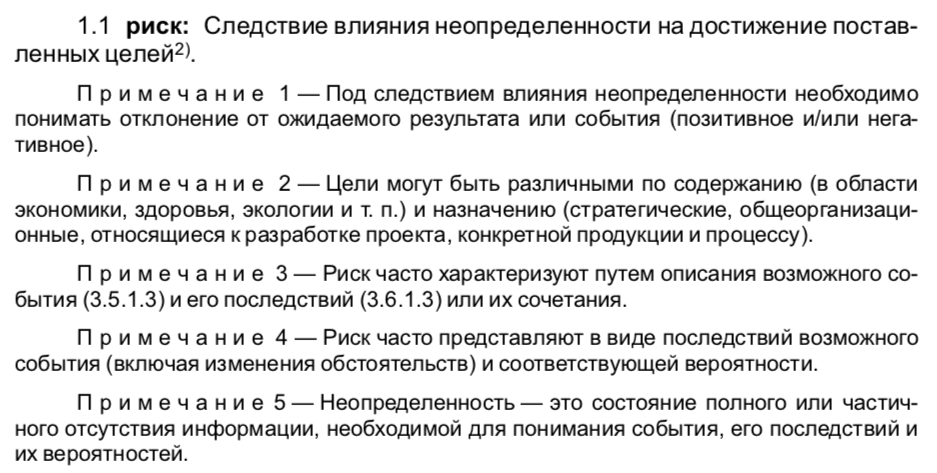
b) Средняя группа («серая» область), для которой затраты и преимущества принятия риска следует учитывать, а возможности соотносить с последствиями.

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**

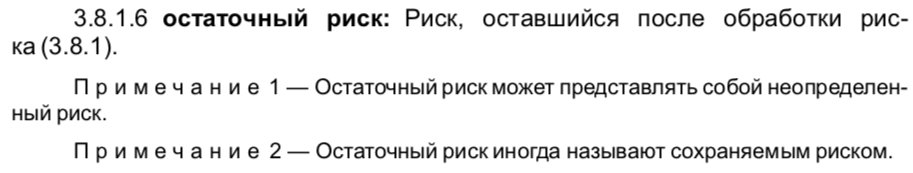
**Предпочтительный риск**: тип риска и его уровень, к которому организация стремится или готова поддержать

**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.

Д/з

Управляющие программы

Программа обслуживания

Драйвер

Макроопределения

# 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)