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**

Комплект для проведения испытаний на соответствие;a

Испытания уровня 1;

# 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

Риски

Сравнительная оценка рисков

Предпочтительный риск

Исключение риска

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