Задание к 1 ноября

- С сайта http://yury.name/cryptography/ изучить лекции 1,2 и 3.
- До 1 ноября написать эссе объемом от 2 до 8 страниц А4 и отправить по адресу pra@yandex.ru

ФЗ № 152 от 26 июля 2006

ФЕДЕРАЛЬНЫЙ ЗАКОН О ПЕРСОНАЛЬНЫХ ДАННЫХ

Область действия Закона

- Настоящим ФЗ регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти…, юридическими лицами и физическими лицами **с использованием средств автоматизации**, в том числе в информационно-телекоммуникационных сетях, **или без использования таких средств, если обработка** ПД без использования таких средств **соответствует характеру действий** (операций), совершаемых с ПД **с использованием средств автоматизации**, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск ПД, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях ПД, и (или) доступ к таким ПД.

Действие закона не распространяется

- обработке персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных;
- организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда Российской Федерации и других архивных документов в соответствии с законодательством об архивном деле в Российской Федерации;
- обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;
- предоставлении уполномоченными органами информации о деятельности судов в Российской Федерации в соответствии с Федеральным законом от 22 декабря 2008 года N 262-ФЗ "Об обеспечении доступа к информации о деятельности судов в Российской Федерации

Что такое Персональные данные

- персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

Классы

$X_{ПД}$ \ $X_{КПД}$	3	2	1
Категория 4	К4	К4	К4
Категория 3	К3	К3	К2
Категория 2	К3	К2	К1
Категория 1	К1	К1	К1

Категории ПД $\left(X_{ПД}\right)$

- категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
- категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;
- категория 4 - обезличенные и (или) общедоступные персональные данные.

Значения $X_{КПД}$

- 1 - в информационной системе одновременно обрабатываются персональные данные более чем 100.000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;
- 2 - в информационной системе одновременно обрабатываются персональные данные от 1000 до 100.000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;
- 3 - в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

Классы

$X_{ПД}$ \ $X_{КПД}$	3	2	1
Категория 4	К4	К4	К4
Категория 3	К3	К3	К2
Категория 2	К3	К2	К1
Категория 1	К1	К1	К1

Согласие субъекта

- Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе, за исключением случаев, предусмотренных частью 2 статьи 9. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных.

Согласие не требуется

1) обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

1.1) обработка персональных данных необходима в связи с реализацией международных договоров Российской Федерации о реадмиссии;

2) обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

3) обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

4) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5) обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

6) обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

Принцип минимальных привилегий

- каждая операция должна выполняться с наименьшим набором привилегий, требуемых для данной операции.

Принцип прозрачности

- СЗИ должна работать в фоновом режиме, быть незаметной и не мешать пользователям в основной работе, выполняя при этом все возложенные на нее функции.

Принцип превентивности

- последствия реализации угроз безопасности информации могут повлечь значительно большие финансовые, временные и материальные затрат по сравнению с затратами на создание комплексной системы защиты.

Принцип адекватности

- применяемые решения должны быть дифференцированы в зависимости от вероятности возникновения угроз безопасности, прогнозируемого ущерба от ее реализации, степени конфиденциальности информации и ее стоимости

Принцип системного подхода

- заключается во внесении комплексных мер по защите информации на стадии проектирования СЗИ, включая организационные и инженерно-технические мероприятия. Следует помнить оснащение средствами защиты изначально незащищенной АС является более дорогостоящим, чем оснащение средствами защиты проектируемой АС

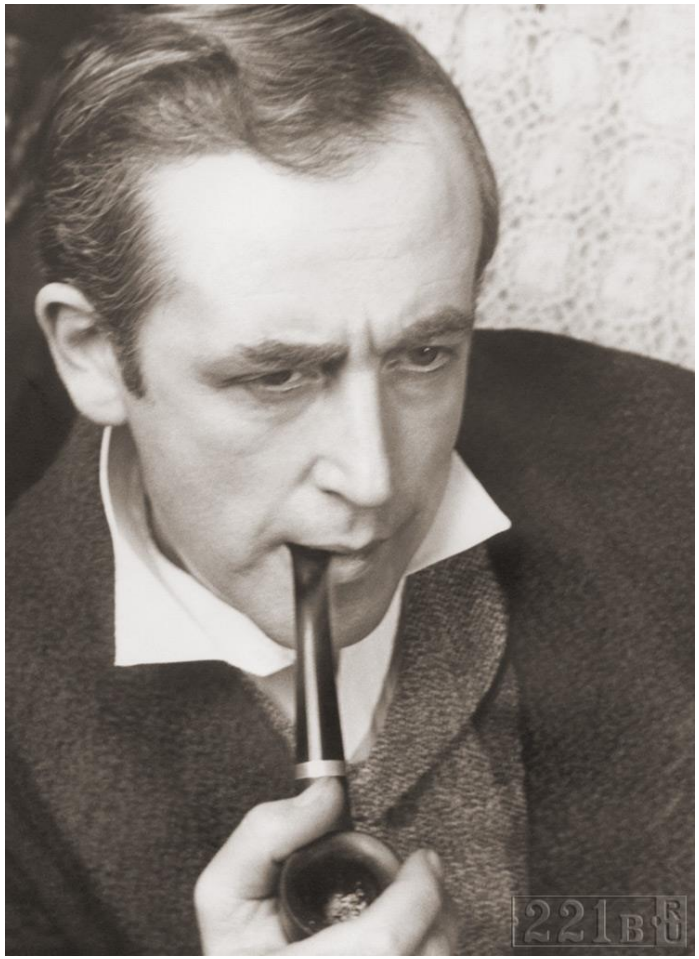
Принцип непрерывности защиты

- функционирование системы защиты не должно быть периодическим. Защитные мероприятия должны проводиться непрерывно и в объеме предусмотренном политикой безопасности

Принцип адаптивности

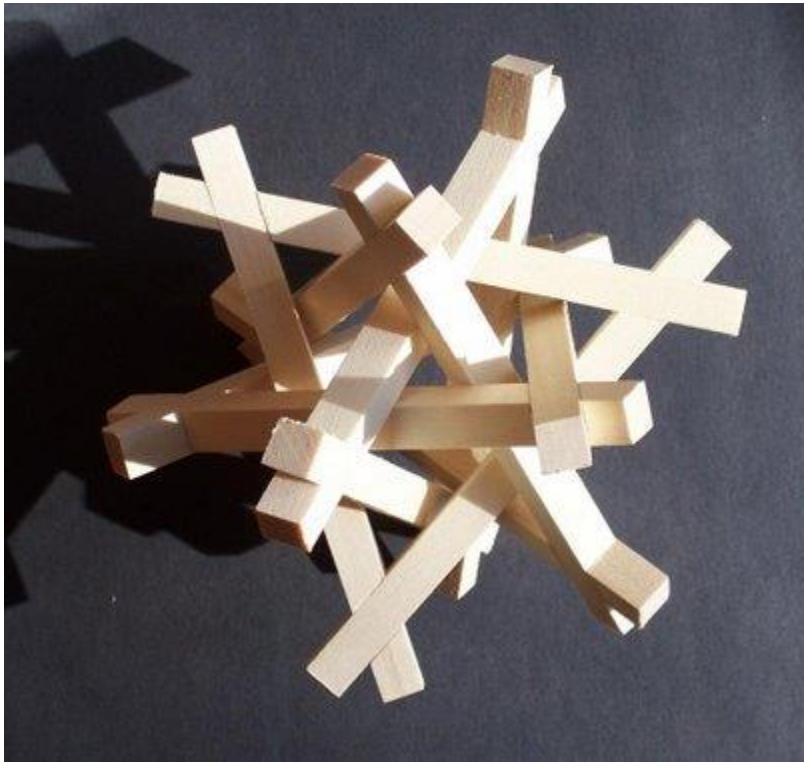
- система защиты должна строиться с учетом возможного изменения конфигурации АС, числа пользователей, степени конфиденциальности и ценности информации. Введение новых элементов АС не должно приводить к снижению достигнутого уровня защищенности

Принцип доказательности



- Результаты работы СЗИ не должны зависеть от субъекта.
- Используются:
  - Только известные формальные модели
  - Применение систем аутоинтефикации
  - Сертифицированных элементов
  - Требование сертификации СЗИ в целом

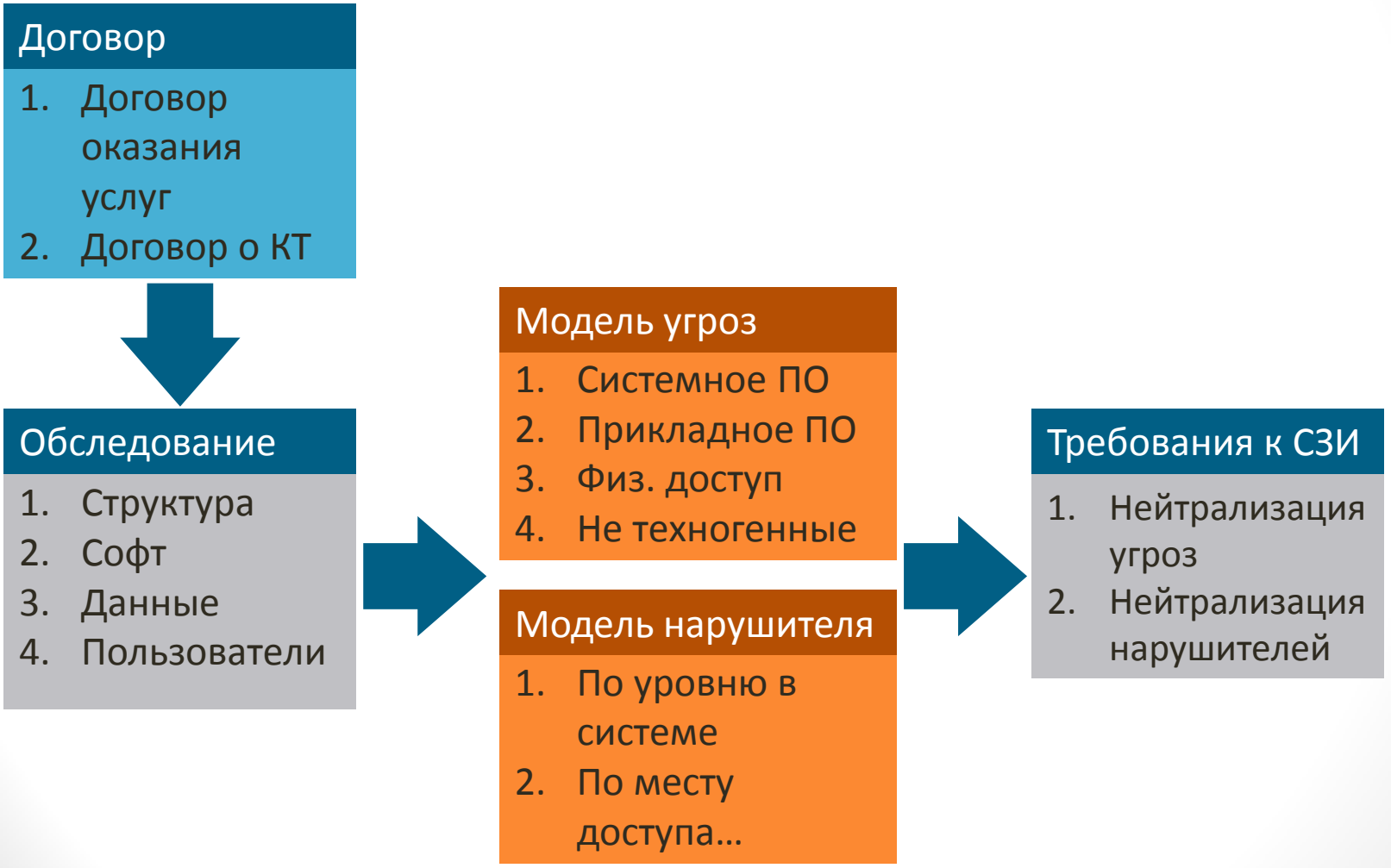
Принцип унификации решений



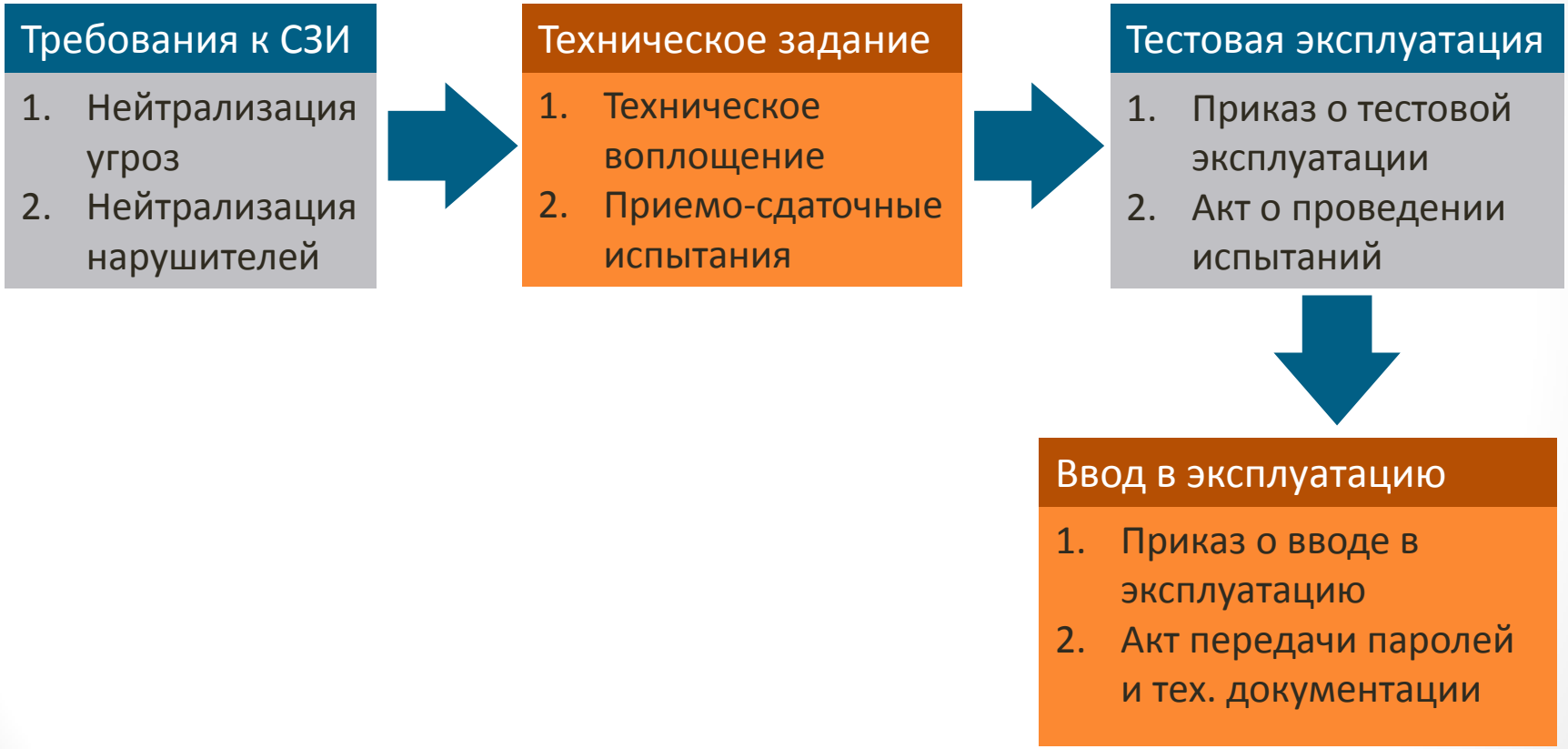
- Разрабатываемые решения должны быть единообразными в схожих ситуациях.
- Следствием принципа является использование:
  - Типовых проектов
  - Типовой классификации рисурсов
  - Типовых конфигурации

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Информационные потоки при создании СЗИ



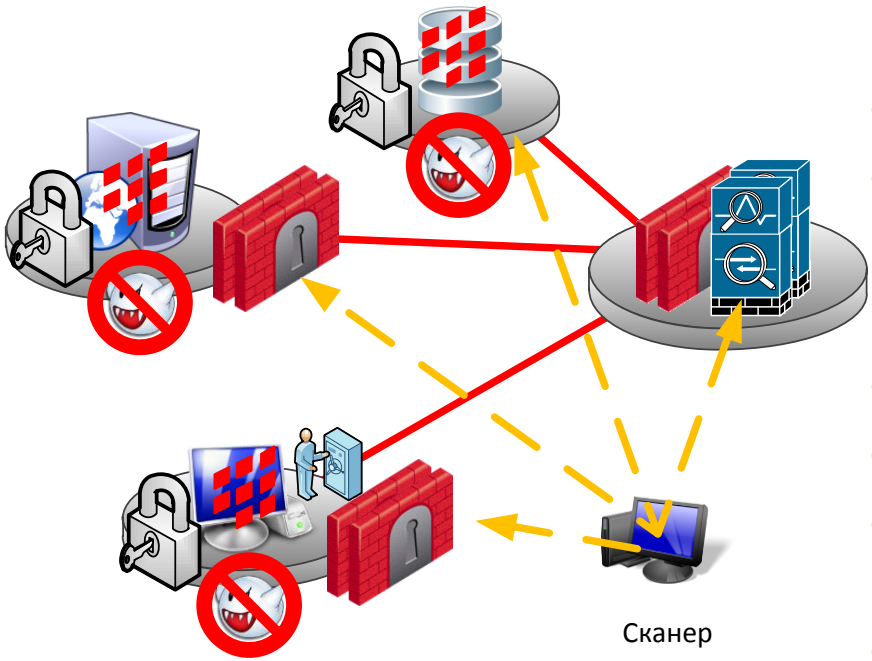
Информационные потоки при создании СЗИ



Структура СЗИ
(топологический анализ)

- Разделение потоков информации различных классов
- Выявление зон свободного доступа людей к активному сетевому оборудованию
- Выявление зон свободного доступа к линиям связи
- Выявление участков сети с радиоканалом

Элементы системы защиты информации



- Защита от НСД:
  - Авторизация;
  - Разграничение доступа.
- Антивирусная защита.
- Надежное хранилище
  - Контроль целостности
  - обеспечение конфиденциальности
- Подсистема управление траффиком.
- Подсистема резервного копирования
- Системы обнаружения (предотвращения) вторжений.
- Система анализа защищенности.
- Криптографическая подсистема.
- Подсистема регистрации событий.

Цена вопроса

Сертификация Windows

- Средства вычислительной техники. Защита от несанкционированного доступа к информации.
  - Показатели защищенности от несанкционированного доступа к информации“ по 5 классу защищенности,
  - могут использоваться при создании автоматизированных систем до класса защищенности 1Г включительно
  - при создании информационных систем персональных данных до 2 класса включительно.

Принципы классификации

- Составляется перечень типов ресурсов типы по тематике, функциональному назначению, сходности технологии обработки и т.п. признакам
- Для каждого типа ресурсов определяется степень важности по основным задачам СЗИ.
- Для каждого типа ресурсов с учетом значимости субъектов и уровней наносимого им ущерба устанавливается степень необходимой защищенности.

Типовая структура

- Активное сетевое оборудование на границе зон может реализовывать:
  - Трансляцию адресов;
  - Фильтрацию трафика;
  - IDS;