Лекция №2

Основные понятия

Замечания: Когда вы мне пишете письма, не отсылайте меня на небеса, никуда не посылайте дальше Макадана. В ваших письмах не должно быть никаких ссылок. Отправляйте только то, что вам пишут. В том случае, если речь идёт о результатах, мне на почту должно прийти чаще всего три файла: 1) исходный текст; 2) исполнимый модуль; 3) отчёт о проделанной работе в виде совокупности скриншотов. Если exe-файл не пропускает, то нужно: 1) либо менять почту; 2) либо заархивировать exe-файл в zip-архив (пароль на архив: **8491a9144f334061b3f139333f27a4b8bd3aea38** 🡨 не делай такой сложный).

Ответы на упражнения из предыдущей лекции:

1. Deep Purple, Маяковский, Зубович – какая связь? Ответ: Deep Purple – «Child in Time», Маяковский – «Что такое хорошо и что такое плохо?», Зубович – Статья с эпиграфом «Что такое хорошо и что такое плохо?»
2. Самая программистская песня Beatles: «When I’m 64»
3. Найти толкование на английском: было просто.

Толкование №201

Безопасность системы, создание, хранение и передача данных (безопасность информационной системы) рассматривается как состояние системы, при котором:  
1) система способна противостоять дестабилизирующему воздействию внутренних и внешних угроз

2) функционирование и сам факт наличия системы не создаёт угроз для внешней среды и элементам самой системы

Толкование №202

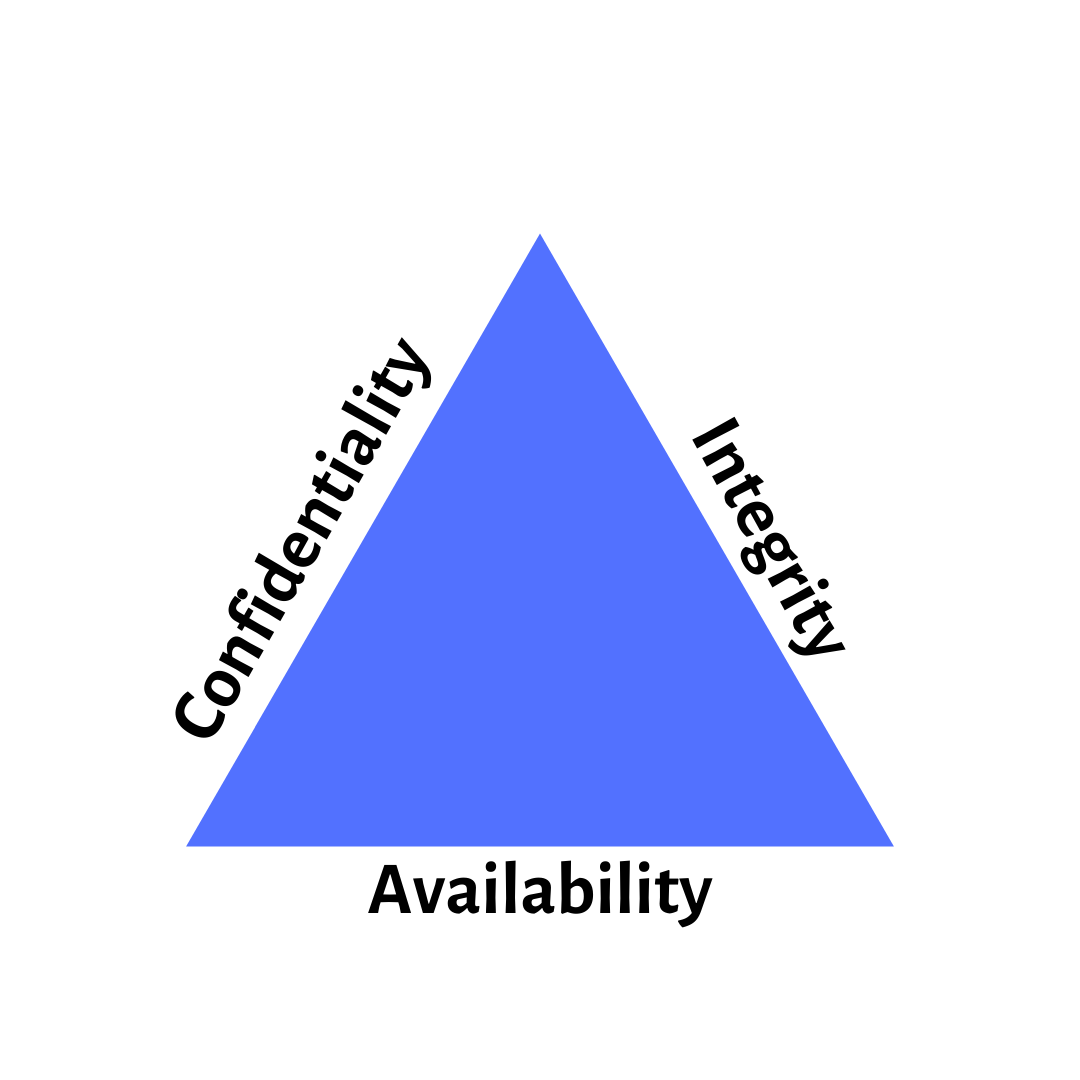
Традиционно безопасность системы обработки данных рассматривается как возможность системы обеспечить наличие и поддержание на должном уровне трёх базовых свойств защищаемых данных:

А) Свойство «целостности» - обеспечение того, что защищаемые данные могут быть созданы, изменены, переданы, удалены только законными пользователями, а также то, что они поддерживаются внепротиворечивом и актуальном состоянии.

Б) Доступность – обеспечение доступа к защищаемым данным для легальных пользователей.

В) Конфиденциальность – обеспечение того, что доступ к данным могу получить только легальные пользователи.

Обычно, говоря об этих свойствах на английском языке. В различных источниках, в том числе на помойке, рисуют такую картинку:



**Confidentiality** – When protected information be wanted to be able to restrict access to those who are allowed to see it. Everyone else should be disallowed from playing anything about its contents.

**Integrity** – Is ashured that the information being accessed had no been opened and truly represents what is intended.

**Availability** – means that information can be accessed and modified by anyone authorized to do so in appropriate time frame.

Толкование №203

Под защитой информации следует понимать комплекс мероприятий, направленных на обеспечение всех трёх аспектов информационной безопасности. И ресурсов, используемых для создания, хранения, обработки и передачи данных. Данное толкование взято из источника: Емельянова «Защита информации в информационном компьютере. Учебное пособие.» г. Москва, 2013.

Система называется безопасной, если она, используя соответствующие аппаратное и программное средства, административные установления управляет доступом к информации таким образом, что только должным образом авторизованные лица или действующие от их имени процессы получают права доступа к данным, права изменять, создавать, удалять и передавать данные.

Толкование №204

Под угрозой понимают возможность возникновения на каком-либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию, а именно:

А) Нарушение физической целостности;

Б) Несанкционированная модификация;

В) Несанкционированное получение;

Г) Несанкционированное размножение информации;

Угрозы бывают преднамеренными и непреднамеренными.

Далее будем говорить только о преднамеренных. А о непреднамеренные угрозы – это события/действия, которые совершаются по неосторожности, по незнанию или по невнимательности.

Преднамеренные угрозы – угрозы, связанные со злым умыслом преднамеренного разрушения системы с потерей или утечкой данных из системы.

Толкование №205

Реализация угрозы называется атакой.

Толкование №206

Существует большое количество подходов классификации угроз и соответствующих им атак.

Упражнение №201 (на почту до конца дня)

На странице 76 книги Емельянова (и другие) представлена таблица угроз безопасности. Необходимо используя программное средство Exel изобразить точно такую таблицу и прислать на почту этот exel-вский файл. При чём в файле должны присутствовать дата и время окончания рисования схемы.

Толкование №207

Основные угрозы можно рейтинговать по-разному. Есть большое количество организаций, которые составляют рейтинги угроз по их ущербу для физических и юридических лиц. Соответственно, на помойке можно найти различные варианты подобных рейтингов, например, по результатам 2019-ого года (т.е. в 2020-ом году) этот рейтинг был таким.

Для физических лиц

1-ое место: Несанкционированное использование информации о кредитной карте.

2-ое место: Мошенничество с личными данными с помощью так называемого «фишинга».

3-е место: Ущерб пользователям со смартфонов из-за не авторизованных приложений.

4-ое место: Запрос денег с помощью угроз или мошенничества с использованием электронной почты и так далее.

5-ое место: Клевета или обман в социальных сетях.

6-ое место: Интернет-мошенничество путём ложных оповещений.

7-ое место: Несанкционированное использование интернет-банкинга.

8-ое место: Несанкционированный вход в интернет-сервис.

9-ое место: Ущерб от вымогателей.

10-ое место: Неправильное управление какими-то устройствами IoT.

Угрозы юридическим лицам

1-ое место: Ущерб, нанесённый целевыми атаками.

2-ое место: Ущерб, нанесённый с деловой электронной почты.

3-е место: Ущерб от вымогателей.

4-ое место: Увеличение количества атак с использованием слабых мест в цепочке поставок.

5-ое место: Утечка информации из-за внутреннего мошенничества.

6-ое место: Отказ в обслуживании из-за соответствующих атак.

7-ое место: Кража личной информации из интернет-сервисов.

8-ое место: Ущерб от уязвимостей устройств IoT.

9-ое место: Увеличение злоупотреблений из-за раскрытия информации о противодействии уязвимостям.

10-ое место: Утечка информации из-за невнимательности.

Упражнение №202 (прислать до следующего вторника)

Найти во всемирной липкости информацию на английском языке (обязательно с картинками), соответствующую представленному рейтингу угроз для физических лиц и для юридических лиц. Желательно найти 2020-ый год.

Толкование №208

Основные направления борьбы с угрозами – с.83-87 Емельяновой (и других):

А) Стандартизация

Б) Правовое обеспечение, функционирование систем обработки данных

В) Организационное сопровождение в виде политик безопасности

Г) Программно-техническое направление, предполагающее разработку и создание программных и аппаратных средств защиты данных

Толкование №209

В рамках организационного сопровождения систем защиты данных могут быть использованы следующие средства борьбы с угрозами:

А) Управление доступом, идентификация, аутентификация, разграничение доступа, метки безопасности и так называемое «ролевое управление доступом»

Б) В рамках этого организационного управления: шифрование, копирование, перестановка, аналитическое преобразование, гаммирование, комбинирование, числовое и символьное сжатие/расширение.

В) Направление, предполагающее протоколирование и аудит.

Более подробно на с.125-178 книги Емельяновой (и других).

Толкование №210

Программно-техническое направление борьбы с угрозами, в первую очередь, ориентированно на противодействие программно-техническим угрозам безопасности организационных систем, при этом вредоносные воздействия в такой борьбе делятся на два основных вида:

А) Воздействие на данные (модификация, искажение, уничтожение)

Б) Воздействие непосредственно на систему обработки данных (вывод из строя, ложное действие, модификация функциональности и создание помех в работе)

Толкование №211

Программно-технические угрозы реализуются посредством создания так называемых mailware или badware.

Под badware понимается любой аппаратно реализованы элемент и(или) любое программное средство, которое: 1) во-первых действует обманным путем и приводит к обратимым или необратимым изменениям системы; 2) во-вторых приводит к потенциальным, нежелательным для системы результатам без понятного и доходчивого информировании пользователя системы и его согласия.

Толкование №212

Существуют различные способы классификации того, что называется badware, например, может быть сделана классификация по таким критериям, как:

1. По характеру воздействия
2. По способу реализации
3. По способу проникновения
4. По способности к саморазмножению

Толкование №213

По характеру вредоносного воздействия могут быть выделены следующие пункты системы:

1. Уничтожение или удаление данных программных средств
2. Вывод системы из строя
3. Вредоносное инициирование, выполнение функционала системы не к месту и не ко времени
4. Создание препятствия к выполнению функций системы

Толкование №214

По характеру проникновения могут быть выделены следующие пункты системы:

1. По средствам разработки программы
2. Неосознанное внесение изменений персоналом
3. Двунамеренные атаки
4. В процессе ремонта или обновлении оборудования; также при модификации программного обеспечения

Толкование №215

В самом общем случае разделы безопасности информационной системы могут быть разделены на внутренние и внешние.

Толкование №216

Программно-технические угрозы безопасности подробно рассмотрены на с.87-125 книги Емельяновой (и других).

Материал, который изложен на этих страницах, может быть основой так называемых бомб, ответов на первый вопрос экзаменационных билетов.