Лекция 2

Замечание №0

- необходимо слепо (тупо) следовать тому, что определено постановкой задачи. Необходимо всегда очень внимательно читать условие задачи, аккуратно записать то, что говорится и не делать того, чего нет в задании. Не воспринимать на свой лад то, о чём идёт речь, потому что очень часто слышу фразу “Я художник, я так вижу”.

Замечание №1 - в дальнейшем в своей жизни следовать следующим принципам:

Принцип 1.

Принцип так называемого “хорошего рассказывания”, который предполагает, если рассматривается какое-то понятие, или излагается какой-то материал, или даётся ответ на какой-либо вопрос, необходимо сначала на 1м шаге рассказать то, о чём будете говорить, 2й шаг - говорить то, что хотите сказать, 3й шаг - расскажи о чём рассказал

Принцип 2. Называется “разделяй и властвуй” - предполагает что для того, чтобы разобраться с каким-либо понятием, или разобраться с какими-либо врагами, необходимо сначала выбрать самого основного врага (или самое основное понятие).

Шаг 2 - разобраться с врагом, или понятием (значит, разложить его по полочкам, разложить на составляющиеа).

Шаг 3 - переход на 1й шаг

Принцип 3. Ограничение контекста.

Начиная с этой лекции и на последующих, отвечать на любой вопрос, который будет в начале лекции задаваться со слова “Если” и продолжать это “если” ограничением контекста.

Пример: на 2й вопрос “Что такое программа” - стоило ответить “Если речь идёт о компьютерной технике, о персональных вычислительных машинах, то программа - это …” Если дальше применять принцип “разделяй и властвуй” - то стоит говорить, что такое ВМ, что такое инструкция и тд. Если речь идёт о политической партии и ограничивать контекст обществом, то программа - это набор фраз, с помощью которых определяются цели и задачи политической партии

Принцип 4. Правило, или принцип “3х компасов”. Заключается в следующем: для того, чтобы установить истину, а именно, в каком направлении плыть, на корабле должно быть как минимум 3 компаса. Т.к. если 1 компас на корабле есть, если он сломается, то можно уплыть в неизвестном направлении. Если есть 2 компаса и 1 сломается, то с вероятностью 50/50 сломается и можно уплыть в неизвестном управлении и тд.

В рамках БИС

1 компас - средства массовой информации, а именно, слова преподавателя, слова одногруппника, информация из интернета, информация из книг.

2 компас - результаты, полученные не Вами, а результаты, полученные с помощью вычислительной техники (но только не с помощью ИИ)

3 компас - ваш здравый смысл

Толкование 7. Постулаты в области БИС

Постулат 1. Не существует абсолютных методов и средств защиты данных. Любая система защиты данных и программ может быть взломана и к ней может быть получен доступ.

Постулат 2. Построение системы для защиты данных необходимо тогда и только тогда, когда стоимость разработки и внедрение этой системы меньше стоимости вреда, который может быть нанесён заказчику системы из-за её отсутствия

Постулат 3. Тем, что нельзя измерить - невозможно управлять (связан с постулатом 2). Прежде, чем говорить о необходимости построения системы защиты данных, необходимо оценить стоимость этой системы

Постулат 4. Основной. Потребует от нас погружение в пучину низкоуровнего программирования. Чем ближе к аппаратному уровню уровень реализации систем защиты данных и программ, тем, при прочих равных условиях, более надёжно построенная система защиты данных.

Толкование 8. Безопасность системы создания, хранения и передачи данных рассматривается, как состояние, при котором

1) система способна противостоять дестабилизурующему воздействию внутренних и внешних угроз

2) функционирование и сам факт наличия системы не создаёт угроз для внешний среды и элементов самой системы

Толкование 9.

Традиционно, безопасность системы обработки данных, обеспечивается как поддержание 3х базовых свойств защищаемых данных

1) целостность (обеспечение того, что защищаемые данные могут быть создана, изменены, переданы, удалены только законными пользователями и того, что они поддерживаются в непротиворечивом и актуальном состоянии)

2) конфиденциальность - обеспечивает то, что доступ могут получить только легальные пользователи

3) доступность - обеспечение беспрепятственного доступа к защищаемым данным для легальных пользователей

Толкование 10.

Под защитой информации следует понимать комплекс мероприятий, направленных на обеспечение всех аспектов информационной безопасности, т.е. Целостности, доступности и конфиденциальности, а также ресурсов, используемых для создания, хранения, обработки и передачи данных.

На странице 47 книги “Защита информации в персональном компьютере”, учебное пособие, 1м из авторов которого, является автор по фамилии “Емельянова”, рассматриваются вопросы, которые вам придётся конспектировать при подготовке бомб для билетов на экзаменах. Поэтому, будьте бдительны, что чаще всего вам придётся брать инфу из этой книги

Система называется безопасной, если она использует соответственные аппаратные, программные средства, административные .., управляет доступом к информации так, что только должным образом авторизованные лица, или же действующие от их имени процессы, получают право доступа к данным. Т.е. Право создавать, изменять, управлять и передавать данные.

Толкование 11.

Под угрозой, будем понимать возможность возникновения на каком-либо этапе жизнедеятельности системы явление, или событие, следствием которого могут быть нежелательные воздействия на информацию (на данные и программы), а именно, нарушение физической целостности, несанкционированная модификация, несанкционированное получение и несанкционированное размножение данных и программ.

Угрозы бывают преднамеренными и непреднамеренными. Более подробно можно посмотреть на с. 75 ранее обозначенной книги. Под преднамеренными угрозами понимаются угрозы, связанные со злым умыслом преднамеренного физического разрушения системы, или с потерей, или утечкой данных из системы.

Толкование 12.

Реализация угрозы называется атакой.

Толкование 13.

Существует большое количество подходов, классификации угроз и соответствующих им атак. Например, угрозы безопасности, могут классифицироваться по цели угрозы, по принципу воздействия, по характеру воздействия, по способу воздействия, по объекту атаки, по состоянию объекта или средству атаки.

По причине ошибки.

Данная классификация взята со страницы 76 упомянутой книги.

Следующая лекция начнётся с вопроса: В том списке, который вы записали сейчас, через запятую, отсутствует 1 из подходов, который есть в книге на с. 76.

Вопрос будет такой, какой принцип классификации пропущен.

Толкование 14.

Существуют различные подхода к определению основны угроз информационной безопасности и их ранжированию по степени частоты возникновения, по степени нанесения ущерба и тд и тп

В разных странах и тд может быть разной. Например, существует такая классификация 10 угроз для физических лиц, которая была представлена в 1й из стран в 1м из прошедших

Вопрос 2, который будет на след лекции. Нужно будет указать страну и год, в котором эта классификация была представлена.

Эта классификация следующая: В скобочках записано, какое место занимала угроза в предшествующем году 10 основных угроз для физических лиц:

1. Несанкционированное использование платежей через смартфон (в прошлом году тоже 1е место)

2. Фальсификация персональных данных, путём фишинга (в прошлом году тоже 2е место)

3. Клевета, или розыгрыш в социальных сетях (7)

4. Выманивание денег методом запугивания, или мошенничества с использованием электронной почты (5)

5. Несанкционированное использование данных кредитной карты (3)

6. Несанкционированное использование интернет-банкинга (4)

7. Кража личной информации из сервисов в интернете (10)

8. Интернет мошенничество из-за поддельного предупреждения (9)

9. Ущерб пользователям смартфонов вредоносными приложениями (6)

10. Несанкционированный вход в сервисы в интернете (8)

Вопрос №2 на следующей лекции будет сформулирован таким образом: в какой стране и в каком году были выделены эти 10 основных угроз и в каком году

Подсказка: это Азия

Толкование 15. В настоящее время, на ряду с перечисленными выше угрозами, существует ещё одна угроза, которая называется кража конфиденциальной информации путём целевых атак

Выделяют 3 метода атаки:

11. Открытие прикрепленного файла, или ссылки в электронном письме, отправленном злоумышленником. Может заразить ваш компьютер вредоносным программным обеспечением

12. Подделка веб-сайта. Суть метода заключается в том, что подделывается веб-сайт. Причём, при доступе к этому поддельному веб-сайту осуществляется заражение того, кто лезет в этот неизвестный веб сайт соответствующим вирусом, или вредоносным ПО

13. Несанкционированный доступ, когда некоторые уязвимости используются для кражи информации и вторжении во внутренние сети, например, белгосуниверситет

Толкование 16.

Основные направления борьбы с угрозами,

1е направление: стандартизация в области защиты систем обработки данных. Правовое обеспечение функционирования систем обработки данных и соответствующих систем безопасности.

3, огранизационное сопровождение систем защиты данных в виде политик безопасности.

4) программно техническое направление борьбы с угрозами, предполагающее разработку и создание аппаратных и программных средств защиты данных

Толкование 17.

В рамках организационного направления борьбы с угрозами используется следующее

а) управление доступом, идентификация, аутентификация, разграничение доступа и ролевое управление доступом

б) криптографическое закрытие, шифрование, кодирование, гаммирование, смысловое и символьное сжатие и расширение

в) протоколирование и аудит

Толкование 18.

Программно-техническое направление борьбы с угрозами в первую очередь ориентировано на противодействие программно-техническим угрозам безопасности технических систем

При этом предполагается, что необходимо бороться с 2мя видами вредоносного воздействия:

1) воздействие на данные, когда они модифицируются, уничтожаются, или искажаются

2) воздействие на систему обработки данных, когда система может быть выведены из строя, либо модифицирована функциональность, либо созданы помехи в работе

Толкование 19. Программно-технические угрозы реализуются посредством создания так называемых нехороших изделий, malware/badware Под badware обычно понимают любой аппаратно реализованный элемент, или любое программное средство, которое

а) действует обманным путём и приводит к обратимым и необратимым изменениям в системе и приводят к потенциально нежелательным для системы результатам без понятного и доходчивого информирования пользователя системы о своём функционале, без согласия пользователя на использование этого средства

б)