**Основы информационной безопасности**

1. **Титульный слайд (название модуля, автор)**

Приветствие. Занятие «Основы информационной безопасности».

1. **Программа модуля**

Кратко – про что будет доклад. На практическом занятии: знакомство с библиотекой Pandas и ее использование для анализа базы данных угроз и уязвимостей ФСТЭК России.

1. **Что такое информация?**

Понятие информации можно определить как со стороны чистой математики (где это мера, обратная неопределенности), так и со стороны законодательства (в частности, определение из ФЗ-149 «Об информации, информационных технологиях и о защите информации».

На практике удобно использовать некий синтез определений, который отражает нематериальную природу информации (не зависит от формы представления), а также ее ценность для снижения неопределенности, которая еще и падает со временем.

Ссылки:

<http://www.consultant.ru/document/cons_doc_LAW_61798/>

1. **Среда обитания информации – информационная сфера**

Рассмотреть модель информационной сферы в изложении Доктрины обеспечения ИБ Российской Федерации 2000-го года.

Сделать акцент на том, что, когда мы говорим «информационная безопасность», мы говорим о безопасности информационной сферы в целом – не выделяя какой-то конкретной ее части.

Ссылки:

<https://base.garant.ru/182535/>

1. **Что такое безопасность?**

После перейти к понятию безопасность в наиболее широкой трактовке.

Акцентировать внимание, что свойство безопасности симметрично: как среда не должна навредить системе, так и наоборот.

1. **Пример информационной сферы**

Разобрать абстрактные понятия информационной сферы на жизненном примере: некоторое предприятие.

Обратить внимание, что даже в этом примере в границы информационной сферы попадают субъекты, не относящиеся к самому предприятию: это его контрагенты.

1. **Иерархия понятий**

Далее обсудить, что мы будем говорить в первую очередь о компьютерной безопасности.

Акцентировать внимание на отличии этого термина от термина «Информационная безопасность» - компьютерная безопасность сосредоточена только на информационной инфраструктуре и той информации, которая представлена носителями в информационной инфраструктуре.

При этом далее мы будем использовать термины ИБ и КБ в качестве синонимов.

Также здесь нужно обратить понятие на термин «компьютерная система», под которым мы будем понимать часть автоматизированной системы, включающей только средства автоматизации.

1. **Что такое компьютерная система с точки зрения КБ?**

Вновь вернемся к понятию компьютерной системы. Согласно введенному определению это набор инструментов для обработки информации и сама информация, которая может либо кратковременно попадать в систему, либо храниться в ней длительное время, что определяется процессами обработки информации.

Сама информация при этом обладает рядом свойств, называемых свойствами безопасности информации: конфиденциальность, целостность и доступность (пояснить по каждому свойству, что за ними скрывается). Это не исчерпывающий список свойств безопасности информации, но указанные 3 свойства наиболее часто рассматриваются в вопросах ИБ.

Нарушение состояния безопасности информации – это нарушение одного из свойств.

1. **Содержание**

Подвести краткий итог и анонсировать следующий блок.

1. **Составные части атаки**

Ввести несколько формальных определений, заодно упомянуть базовые стандарты в области ИБ:

ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»

ГОСТ Р 53113.1-2008 «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения».

1. **Составные части атаки**

Перейти к визуализации понятий.

Пояснить, что угрозы и источники угроз – это объективные свойства среды, которые никак не связаны с защищаемой компьютерной системой.

А вот уязвимость и актив – это базовые элементы (с точки зрения КБ) компьютерной системы.

1. **Отличие ущерба и потерь**

Ущерб выражается в терминах безопасности информации, т.е. нарушение свойства целостности, доступности или конфиденциальности.

А вот потеря – это уже некоторые негативные последствия за рамками компьютерной системы: реальные денежные потери, срыв планов производства, экологические бедствия, травмы и гибель людей.

Отметить, что атака, приводящая к потерям, может содержать множество шагов (реализаций различных угроз). Каждый такой шаг будет наносить ущерб активам КС, но потери возникнут только в конце цепочки атаки.

1. **Появление уязвимостей в системе**

Разобрать понятия и разные типы уязвимостей по ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем»

Также упомянуть понятие многофакторной уязвимости (сразу несколько вариантов) и сказать, что в вопросах ИБ предполагают, что уязвимости присутствуют всегда – вопрос лишь времени (вероятности) их обнаружения источником угрозы.

1. **Прочие важные понятия**

Проговорить прочие важные понятия, которые вводятся с помощью базовых понятий:

Риск – некая мера, объединяющая последствия реализации угрозы и вероятность их наступления.

Модель угроз – попытка описания возможных угроз системы и определение наиболее актуальных из них.

Сценарий атаки – описание действий источника угрозы по реализации угрозы (с использованием уязвимости и нанесением ущерба активу).

Понятие атаки – когда мы наблюдаем в реальности реализацию угрозы посредством уязвимости.

Инцидент – по сути, факт успешной атаки.

1. **Содержание**

Подвести краткий итог и анонсировать следующий блок.

1. **ровни обеспечения информационной безопасности**

4 уровня обеспечения ИБ: законодательство – создание правового поля, формирование отношения к сфере ИБ.

Административный – цели и ресурсы на обеспечение ИБ со стороны высшего руководства предприятием.

Процедурный – все процессы обеспечения ИБ, упомянуть афоризм Брюса Шнайера и акцентировать внимание на том, что состояние безопасности не является устойчивым – оно требует постоянной поддержки, поэтому нужна процедурная составляющая.

Программно-технический уровень – то, где сосредоточены все программно-аппаратные средства обеспечения ИБ.

1. **Законодательный уровень**

Рассматриваем каждый уровень чуть более подробно.

На законодательном уровне регулируются информационные отношения в информационной сфере (всех уровней – даже внутри организации мы ориентируемся на действующее законодательство и, например, не можем объявить коммерческой тайной информацию, для которой явно установлен запрет на отнесение к коммерческой тайне в одноименном законе).

Также отметить, что только на законодательном уровне может быть введено понятие компьютерного преступление, а без него невозможно полноценно обеспечить ИБ на любом уровне.

1. **Общая структура нормативно-правовых актов РФ**

Описать иерархию НПА Российской Федерации.

Напомнить понятие юридической силы и назначения отдельных видов НПА.

1. **Административный уровень**

Пояснить, что административный уровень – это придание «законности» мероприятий по обеспечение ИБ на отдельно взятом предприятии. Пояснить примером, что подразделения по обеспечению ИБ могут, например, накладывать запреты на определенные действия смежных подразделений и даже вышестоящего руководства. Чтобы у них была возможность это делать – нужно указание со стороны высшего руководства компании.

Кроме того, обеспечение ИБ – это затратное мероприятие, соответственно, руководство должна поставить цели и выделить средства для их достижения.

1. **Политика безопасности**

Основной документ, отражающий волю высшего руководства по вопросам ИБ – это политика [информационной] безопасности.

Акцентировать внимание, что политика – это свод принципов. Постановка целей и общих установок по их достижению (например, без физических наказаний в отношении сотрудников ☺ ). Политика ни в коем случае не должна быть подробной инструкцией. Хорошая политика занимает буквально несколько страниц будучи напечатанной.

1. **Процедурный уровень обеспечения ИБ**

Процедурный уровень – это процессы, которые позволяют достигать и сохранять свойство безопасности на длительных промежутках времени.

Для этого реализуется ряд процессов, которые делят по уровням их детализации и скорости протекания.

Стратегические процессы рассматривают вопросы ИБ верхнеуровнево и цикл их выполнения тоже длительный. Как правило, не менее года. Здесь мало связи с реальными компьютерными системами, вопросы в больше степени касаются персонала, документации и пр.

Тактические процессы реализуются в более быстром темпе, и они уже в большей степени связаны с защищаемой компьютерной системой. Сюда попадают различные манипуляции с компонентами компьютерной системы и системы защиты: обновление, изменение политик и пр.

1. **Программно-технический уровень, стратегии защиты**

Программно-технический уровень по большей части представлен средствами обеспечения ИБ, работающими в автоматическом режиме (в соответствии с заданной конфигурацией).

При этом программно-технические средства (ПТС) реализуют различные стратегии защиты:

* Превентивная – когда усилия направлены на то, чтобы не дать злоумышленнику использовать уязвимость и совершить за счет этого атаку. Обычно это достигается путем запрета выполнения каких-то действий в системе (например, ограничение допустимого сетевого трафика)
* Активная – на этой стадии злоумышленник уже реализует свою атаку и задача ПТС этой стадии: обнаружить признаки атаки и пресечь ее дальнейшее выполнение (напомнить, что реальная атака всегда будет представлена цепочкой, лишь в конце которой бизнесу наносятся потери)
* Реактивная – это стратегия, направленная на устранение последствий реализации атаки. Например, если актив был искажен или уничтожен – мы восстанавливаем его из резервной копии.

1. **Программно-технический уровень обеспечения ИБ**

Сам программно-технический уровень тесно связан с процедурным (акцентировать внимание на том, что один без другого бессмысленен).

Поэтому можно говорить о еще одном уровне процессов: оперативных процессах обеспечения ИБ. Большая часть из них реализуется автоматически с помощью ПТС обеспечения ИБ, но часть требует периодического участия человека.

1. **Содержание**

Подвести краткий итог и анонсировать следующий блок.

1. **Модель компьютерной системы**

Для решения любой задачи необходимо построение адекватной модели объекта из реального мира. Для компьютерной системы наиболее общей является модель, в которой система представлена набором состояний, а также преобразованием перехода (в общем случае W – не функция, так как КС может перейти в каждый момент времени во множество новых состояний, конкретизируется выбор состояния на основе дополнительных данных: действий пользователя, сигналов от других систем и пр.), меняющей состояние системы с течением времени.

1. **Модель безопасности компьютерной системы**

Для модели безопасности дополнительно вводятся еще два элемента модели:

Условие перехода – булева функция, определяющая допустимые значения для функции переходов W (отражение ограничений правил ИБ в реальной системе).

g – критерий безопасности, который умеет по текущему состоянию определять является оно безопасным или нет.

Все состояния, соответственно, делятся на 2 класса: безопасные и небезопасные.

Такая модель уже позволяет исследовать вопросы защищенности КС.

1. **Основная теорема безопасности**

Моделируя реальную систему всегда очень сложно описать множество состояний и функцию переходов, чтобы полученная модель не была переусложнена, но при этом решала свою задачу – позволяла делать какие-то предсказания относительно эволюции реальной системы.

В частности, моделирование безопасности КС производится с целью определения функции ограничений f и критерия g, таких, чтобы для данной модели системы не был бы возможен переход в небезопасное состояние.

Если при этом критерий g соответствует реальному критерию безопасности, то функция f будет соответствовать реальным правилам безопасности, реализация которых позволит сделать моделируемую систему абсолютно защищенной (конечно, пока мы остаемся в пределах упрощений модели).

Таким образом, цель моделирования безопасности – нахождение f,g и q0 таких, что, если в начальный момент времени (в состоянии q0) система находится в безопасном состоянии (т.е. g(q0) = 1) и переходит в новые состояния только с соблюдением правил безопасности (т.е. f(qt, qt+1) = истина), то она будет оставаться в безопасном состоянии в любой момент времени.

Можно дополнительно упомянуть частные примеры, например, модель Бела Лападулы, акцентировав внимание, что многое определяется понятием критерия безопасности.

1. **Содержание**

Подвести краткий итог и анонсировать следующий блок.

1. **Понятие субъекта**

Переходим к рассмотрению типовых «кирпичиков» для формальных моделей безопасности КС.

Субъект – это активная сущность системы. То, что меняет систему во времени. Без субъектов система была бы статична, информация в ней не менялась бы никогда.

Субъект – это аватар пользователя. Естественно, человек не может выполнять действия в КС напрямую, ему необходимы посредники в виде пакетов прикладного ПО. Чем субъект будет являться в реальной системе – зависит от этой системы. Далее мы посмотрим на несколько примеров.

1. **Понятие объекта**

Следующий фундаментальный компонент модели – объект. Объект – это пассивная сущность. Он выступает в роли хранилища информации. В КС манипуляция с информацией происходит посредством объектов. Сами объекты имеют некоторую структуру, определяемую конкретной КС, физическое воплощение объекта, как и субъекта, определяется типом конкретной моделируемой системы.

Важно, что информационное содержимое объекта меняется с течением времени.

1. **Поток и доступ**

Для того, чтобы описать изменения информации в объектах моделируемой КС, необходимо ввести 2 дополнительных понятия.

Для начала примем, что перенос информации в системе осуществляют только субъекты, а хранение информации может осуществляться только объектами. Т.е. субъект не может перенести информацию от себя к объекту – он будет инициировать перенос от одного объекта к другому. Если при этом необходимо моделировать ситуацию, когда у субъекта есть собственная память, мы просто предполагаем наличие дополнительного объекта, связанного с субъектом, в котором эта информация может хранится.

Перенос информации от одного объекта (источника) к другому (получателю) будем называть *потоком* информации. Также примем, что один из объектов может отсутствовать – это случай передачи информации из/в смежную систему.

Инициацию потока субъектом s от объекта oi к объекту oj будем называть доступом субъекта s к объекту oi и объекту oj.

Ссылки:

<https://elar.urfu.ru/bitstream/10995/1778/5/1335332_schoolbook.pdf>

Н.А. Гайдамакин, «Учебно-методический комплекс. Теоретические основы компьютерной безопасности», раздел 1.3.

**Примечание:** в упомянутом пособии рассматривается субъектно-объектная модель целостности КС, поэтому некоторые определения в ней отличаются от приведенных здесь. Мы рассматриваем более общий случай.

1. **Примеры**

Рассмотрим несколько примеров применения субъектно-объектной модели к реальным КС.

Процессор. В этом случае субъект – это текущий поток исполнения процессора, а объектами являются регистры процессора, ячейки памяти, порты ввода/вывода, программные прерывания и пр. Процессор при этом контролирует доступ субъекта – потока исполнения к этим ресурсам и, в зависимости от состояния служебных регистров, может блокировать большинство вариантов доступа.

Операционная система. Наиболее каноничный пример: в качестве субъектов выступают процессы (потоки, нити), действующие от имени пользователя ОС, объектами являются все объекты ОС: файлы, сокеты, сигналы, события, каналы и пр.

Переходя к более сложным и масштабным системам можно обратить внимание, что границы между субъектами и объектами размываются. В частности, если мы говорим о локальной вычислительной сети, то информационный обмен тут осуществляют сетевые сервисы (например, браузер и web-сервер), которые могут периодически меняться ролями, в зависимости от текущего направления информационного потока.

На совсем абстрактном уровне – облаке субъекты укрупняются до законченных сервисов (например, облачная система бухгалтерского учета), объектами доступа становятся элементы облачной инфраструктуры, обеспечивающие исполнение программного кода сервиса, хранение его данных и организацию информационных потоков между другими объектами.

1. **Содержание**

Подвести краткий итог и анонсировать следующий блок.

1. **От общего к частному**

Теперь попробуем перейти от общих задач ИБ к частным техническим задачам, решаемым в современных КС.

Для этого вновь пройдем с наиболее абстрактного уровня – информационной сферы в целом – до конкретного уровня информационной инфраструктуры (компьютерной системы).

Безопасность в информационной сфере в наиболее общем виде мы рассмотрели. Если же спуститься ниже – на уровень отдельного предприятия, то общая безопасность в информационной сфере превращается в безопасность бизнес-процессов. Именно от бизнес-процесса зависит и безопасность информации, и безопасность субъектов отношений.

Рассматривая безопасность бизнес-процесса с учетом определения термина «безопасность», приходим к выводу, что она достигается в случае четкой регламентированности процесса, когда каждый участник знает, что нужно делать, как нужно делать и выполняет это в соответствии с предписанием инструкции.

Соответственно, на самом нижнем уровне мы должны обеспечить взаимодействие субъектов и объектов отражающее регламент бизнес-процесса и роли его участников. Причем некорректные действия должны быть недоступны – тогда можно будет гарантировать безопасность на уровне бизнес-процесса.

1. **Проблема перехода**

Но, при переходе на уровень компьютерной системы, мы полностью видоизменяем объект, безопасность которого должна быть обеспечена.

Для примера рассматриваем примитивный процесс: Иванов составляет договоры и отправляет их на согласование Петрову.

С точки зрения компьютерной системы это один процесс формирует файл с договором, который затем преобразуется в электронное письмо и доставляется до почтовой программы.

1. **Проблема перехода**

И вот тут возникает проблема:

1. Отсутствует гарантия, что процесс, который создал файл с договором был действительно инициирован Ивановым (и весь сеанс работы с ним внешняя информация поступала от Иванова).
2. Далее в компьютерной системе идет пересылка контейнеров (файл, электронное письмо), но у нас абсолютно нет информации, что же внутри этих контейнеров – возможно, там совсем уже не договор, который должен был быть направлен Петрову
3. И, наконец, у нас нет гарантии, что почтовое приложение запущено Петровым и он получает из него информацию. Более того, зная техническую природу передачи данных, мы не можем гарантировать, что полученное [возможно] Петровым письмо, было получено только им. Не исключена ситуация, что это письмо было получено еще какими-то субъектами.

И вот из перечисленных проблем и можно сформировать основные задачи ИБ, решаемые в современных КС.

1. **Связь человека и субъекта КС**

Рассказать о понятиях идентификации и аутентификации. Хорошим источником информации является ГОСТ, ссылка на который приведена ниже.

Ссылки:

ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения.

1. **Связь человека и субъекта КС**

Также упомянуть о проблеме вредоносного ПО – которое формально действует от имени легитимного пользователя, но не в его интересах.

Основные методы борьбы с ним: контроль целостности (белый список) и обнаружение вредоносного ПО (черный список).

1. **Ограничение доступа**

На этапе доступа субъекта к объекту есть развитые в современных КС решения по авторизации, которые опираются на политику управления доступом. Тут также рекомендуется опираться на ГОСТ Р 58833-2020.

Ссылки:

ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Общие положения.

1. **Контроль информационных потоков**

Больше всего задач решается на этапе контроля информационных потоков. Так как потоков множество на разных уровнях архитектуры КС (внутри одного хоста, в масштабах локальной вычислительной сети, распределенной сети предприятия и даже всего мира – сети Интернет).

При этом задача решается в двух направлениях: не допустить входящего потока с опасной или вредной информацией (межсетевое экранирование, обнаружение вторжений, защита от нежелательной корреспонденции), а также не допустить исходящего потока критичной информации в сторону нелегитимного получателя (средства предотвращения утечек информации).

1. **Обеспечение конфиденциальной передачи**

При защите информационного потока от прослушивания (т.е. избегание ситуации, когда поток имеет несколько адресатов, часть из которых нелегитимна) также есть две стратегии:

1. Сокрытие самого факта передачи информации (стеганография)
2. Криптографическое преобразование передаваемой информации, чтобы нелегитимный получатель не мог извлечь из соответствующих контейнеров данных осмысленную информацию.
3. **Выявление инцидентов ИБ**

Но, как мы говорили ранее, помимо мер, направленных на противодействие реализации угрозы ИБ, нужно также обеспечить оперативное выявление признака реализации угрозы для последующей нейтрализации цепи атаки. Или, говоря в терминах модели, научиться выявлять переход в небезопасное состояние.

Основным методом для наблюдения за изменениями КС, важными с точки зрения ИБ, является регистрация и учет событий безопасности. При этом событие – это информация, на основе которой можно сделать вывод о том, в какое состояние перешла системы. Специальные средства автоматического анализа событий ИБ позволяют выявить по ним признаки инцидента (переход в небезопасное состояние).

1. **Если вовремя не выявили…**

И, если ничего не помогло, должны вступать в дело средства восстановления пострадавших от атаки активов.

Необходимо сделать ремарку, что восстановить нарушено свойство конфиденциальности невозможно – тут больше речь про целостность и доступность.

Если речь идет о целостности, то восстановить целостность актива поможет резервная копия. Если же речь о доступности – то современные отказоустойчивые архитектуры позволят максимально быстро восстановить нормальный режим функционирования актива.

1. **Содержание**

Подвести краткий итог и анонсировать следующий блок.

1. **Применение методов ИИ в ИБ**

Естественно, что для всех перечисленных задач актуально применение современных алгоритмов машинного обучения и искусственного интеллекта.

В частности: классификация позволяет определять пользователя, например, по его клавиатурному почерку (непрерывная аутентификация), классификация информации позволяет «заглянуть» внутрь контейнера и более осознано применять политики разграничения доступа, классификация сетевых узлов (по профилю их сетевой активности) позволяет выявить вредоносные сетевые узлы.

Также находят свое применение методы выявления аномалий: это и аномалии в потоке событий ИБ (что может говорить о признаках инцидента), и аномальное поведение пользователей и процессов (что может сигнализировать о внедрении вредоносного ПО) и аномалии в сетевой активности, что позволяет выявлять, кроме всего прочего, скрытые каналы утечки информации.

В последнее время также все чаще реальных операторов и диспетчеров заменяют программными алгоритмами, построенными на основе техник обучения в подкреплением – в вопросах ИБ также есть ряд задач, где нужна скорость реакции и принятия решений значительно выше возможностей человека. Например, при реагировании на обнаруженный инцидент ИБ.

1. **Примеры применения ИИ в ИБ**

Обратить внимание, что технологии при этом могут использовать не только во благо, но и во вред.

1. **Сбор информации (crawlers, scrappers)**

Озвучить варианты использования ИИ алгоритмов для обработки больших информационных массивов, которые представлены преимущественно на естественном языке.

Опять акцентировать внимание на том, что задачи очень схожи, несмотря на то, что в одном случае результат – это повышение защищенности, а в другом – совсем наоборот.

1. **Моделирование (генерация) информации**

Акцентировать внимание на генеративном ИИ. Эти технологии позволяют создавать сложные эмуляторы жертв для того, чтобы потом ловить на них нарушителей. Кроме того, генеративный ИИ может применяться для кодирования информации или как замена датчику случайных чисел.

1. **Анализ трафика**

Одна из самых популярных областей применения технологий ИИ – это анализ трафика. Количество и разнообразие трафика давно уже создало проблему понимания структуры и легитимности информационных потоков даже в небольших сетях передачи данных. При этом технологии ИИ могут решить многие задачи анализа трафика: автоматически строить правила глубокой инспекции пакетов, выявлять фрагменты атак или вредоносного кода в трафике, выявлять признаки ботнета в сети и пр. И опять все методы могут быть использованы и во вред – для сбора детальной информации об объекте атаки.

1. **Анализ и защита кода**

Тема безопасной разработки ПО крайне актуальна уже на протяжении последних 10 лет. Но в этой отрасли до сих пор множество проблем с выполнением стандартных процедур безопасной разработки. Технологии ИИ позволяют значительно снизить трудозатраты на различные виды проверок ПО, а где-то даже и автоматически корректировать написанный код, если он содержит ошибки и потенциальные уязвимости.

И снова злоумышленник может использовать инструмент во вред – то, что помогает найти слабые места в коде для их устранения, точно также поможет найти эти же места, но уже для использования их при проведении атаки.

1. **Поведенческий анализ**

Человек остается самым слабым звеном информационной системы, поэтому анализ поведения пользователя КС может говорить о многом. Как для нужд защиты, так и нападения.

1. **Базы знаний, Threat Intelligence**

Сфера ИБ долгое время оставалась и остается до сих пор не очень сильно автоматизированной сферой. По-прежнему множество ценной информации представлено только в человекочитаемом виде. И здесь также может помочь ИИ – методы анализа естественных языков позволяют в автоматическом режиме вобрать в систему обеспечения ИБ содержимое баз знаний.

Сделать переход на практическое занятие, где будет вестись работа с БДУ ФСТЭК России.

1. **Спасибо за внимание.**

Рекомендуемая литература:

1.