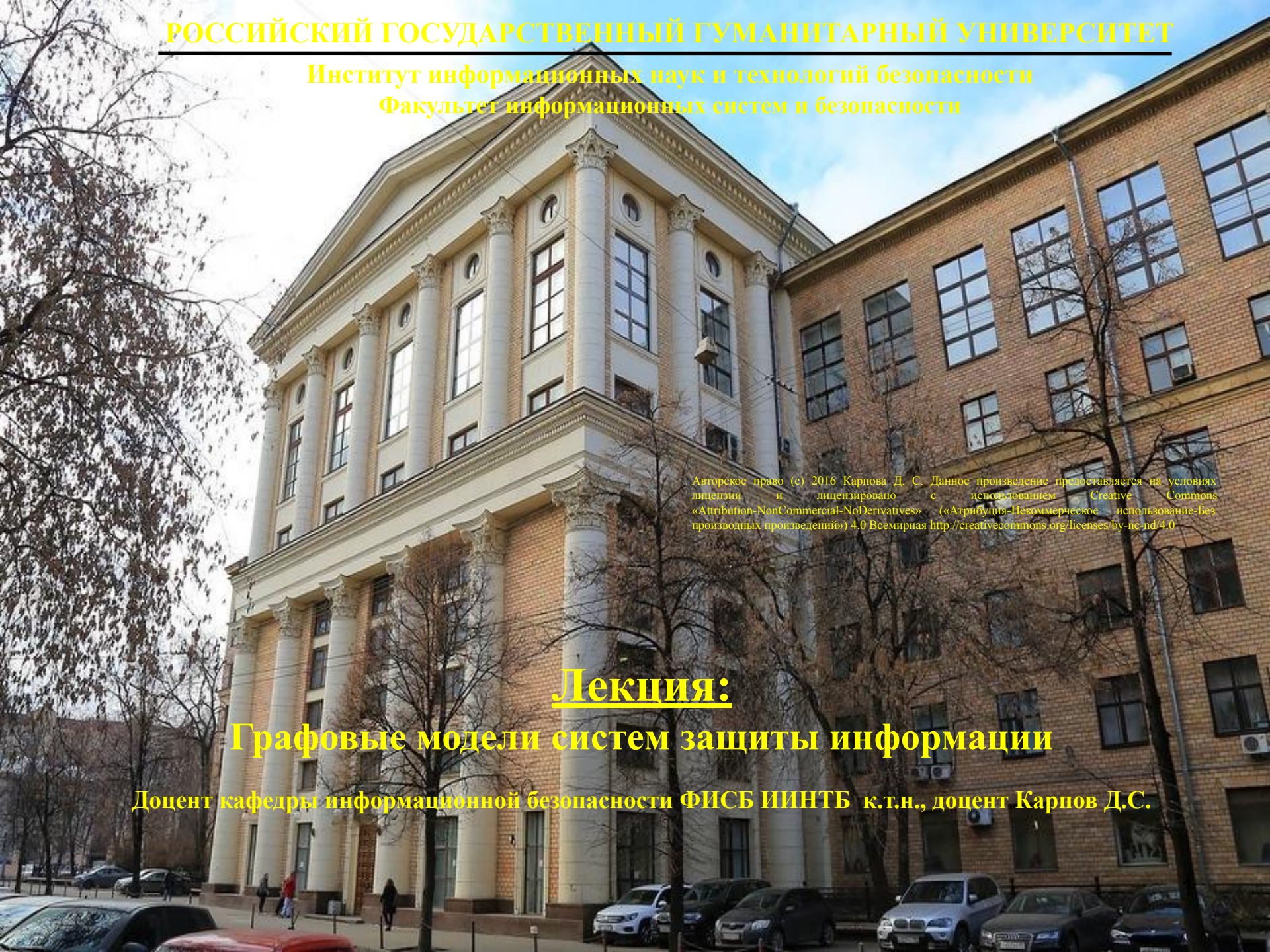
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ

Институт информационных наук и технологий безопасности

Факультет информационных систем и безопасности



Лекция:

Графовые модели систем защиты информации

Доцент кафедры информационной безопасности ФИСБ ИИНТБ к.т.н., доцент Карпов Д.С.

Учебные вопросы

1. Краткие сведения из теории графов
2. Графовые модели компьютерных атак
3. Риск-ориентированные графовые модели систем защиты информации

Актуальность теоретико-прикладных исследований в области защиты информации

Данные последних исследований в области информационной безопасности говорят о растущем внимании руководителей компаний в России и по всему миру к проблеме защиты информации.

Этот факт обусловлен увеличением числа инцидентов, связанных с потерей и разглашением информации или утратой контроля над ней.

Финансовые убытки крупных корпораций оцениваются миллионами долларов в год.

Кроме того, продолжает совершенствоваться нормативно-правовая база в области кибербезопасности.

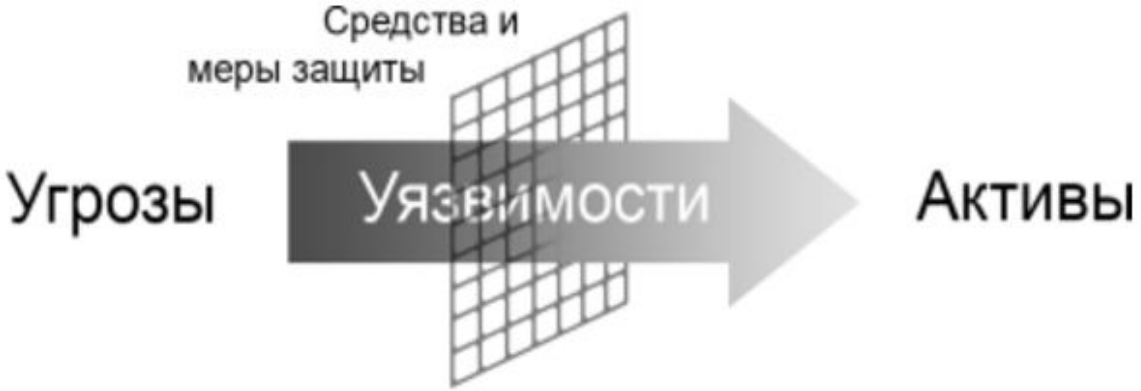
Последние изменения в законодательстве РФ призваны поддержать отечественных производителей средств защиты от киберугроз и обеспечить более высокую долю таких продуктов на российском рынке ИБ.

В этом свете **деятельность по проработке фундаментальных основ ИБ и проведение прикладных исследований являются актуальной задачей.**

Важнейшим направлением обеспечения ИБ является защита информации.

Предметная область «защита информации»

В упрощенном виде предметную область «защита информации» можно представить в виде следующей схемы, которая позволяет проследить связь угроз, уязвимостей и активов.



Актив - всё, что имеет ценность для организации.

Примечание.

Различают следующие виды активов: информация; программное обеспечение; технические средства (например, компьютер); услуги и сервисы; люди и их квалификация, навыки и опыт; нематериальные активы (например, репутация и имидж)

(ISO/IEC 27000:2009; ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология).

Все информационные активы предприятия подвержены рискам реализации угроз кибербезопасности посредством эксплуатации злоумышленниками некоторых известных уязвимостей. Для решения задачи снижения финансовых убытков от подобных инцидентов необходимы инвестиции в правильно отобранные процессы и технологии, обеспечивающие предупреждение и обнаружение рисков безопасности, защиту от их воздействия и реагирование на них. Следует понимать, что защита информации в общем случае сочетает применение технических средств и проведение организационных мероприятий

Терминология. Угрозы безопасности информации

Угроза безопасности информации (Information security threat) - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации

(ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения).

Источник угрозы безопасности информации (Information security threat source) - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации

(ГОСТ Р 50922-2006)

Угроза - возможная причина нежелательного инцидента, которая может нанести ущерб [информационной] системе или всей организации

(ISO/IEC 27000:2014).

Терминология. Уязвимости

Уязвимость - слабость актива или управления, эксплуатация которой приведёт к реализации одной или нескольких угроз (ISO/IEC 27000:2014).

Уязвимость - недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации (ГОСТ Р 56545-2015. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей)

Уязвимость - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации (Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утв. Зам. директора ФСТЭК России 15 февраля 2008 г.).

Уязвимость нулевого дня (Zero-day vulnerability) - уязвимость, которая становится известной до момента выпуска разработчиком программного обеспечения информационной системы мер защиты информации по ее устранению, исправлений ошибок или соответствующих обновлений (ФСТЭК России: методический документ от 11.02.2014 «Меры защиты информации в государственных информационных системах»).

Уязвимость программного обеспечения - ошибка в программном обеспечении, способная напрямую быть использована хакером для получения доступа к системе или сети
(Банк данных угроз безопасности информации ФСТЭК России).

Слабость программного обеспечения (Software weakness) - любая ошибка, допущенная в ходе реализации, написании, разработки или проектирования программного обеспечения (**дефект**, неисправность, «баг», уязвимость), которая, в случае оставления её неисправленной, может являться причиной уязвимости системы или сети для атак (Банк данных угроз безопасности информации ФСТЭК России).

Терминология. Уязвимости

Класс уязвимости - характеристика, уязвимости программного обеспечения, определяющая причину возникновения уязвимости.

В банке данных используются следующие классы уязвимостей:

уязвимость кода – уязвимость, появившаяся в результате разработки программного обеспечения без учета требований по безопасности информации;

уязвимость архитектуры – уязвимость, появившаяся в результате выбора, компоновки компонентов программного обеспечения, содержащих уязвимости;

уязвимость многофакторная – уязвимость, обусловленная наличием в программном обеспечении уязвимостей различных классов (Банк данных угроз безопасности информации ФСТЭК России).

Статус уязвимости - характеристика уязвимости, определяющая степень подтверждения факта существования уязвимости.

Значение поля «Статус уязвимости» принимает одно из следующих значений:

«Подтверждена производителем» – если наличие уязвимости было подтверждено производителем (разработчиком) программного обеспечения, в котором содержится уязвимость;

«Подтверждена в ходе исследований» – если наличие уязвимости было подтверждено исследователем (организацией), не являющимся производителем (разработчиком) программного обеспечения;

«Потенциальная уязвимость» – во всех остальных случаях (Банк данных угроз безопасности информации ФСТЭК России).

Степень опасности уязвимости (Vulnerability severity) - мера сравнительная величина, характеризующая подверженность информационной системы уязвимостям, использование которых может привести к нарушению свойств безопасности информации (Банк данных угроз безопасности информации ФСТЭК России).

Терминология. Атаки

Как показал мировой и отечественный опыт, атаки являются наиболее опасными угрозами (что обусловлено их тщательной подготовкой, скрытностью проведения, целенаправленным выбором объектов и целей атак). (Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации" (утв. ФСБ РФ 21.02.2008 N 149/54-144))

Атака [компьютерная] - попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к активу или его несанкционированного использования (ISO/IEC 27000:2014).

Компьютерная атака: Целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств (Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации), Р 50.1.056-2005 Техническая защита информации. Основные термины и определения).

Сетевая атака: Компьютерная атака с использованием протоколов межсетевого взаимодействия (Р 50.1.053-2005 Информационные технологии. Основные термины и определения в области технической защиты информации), Р 50.1.056-2005 Техническая защита информации. Основные термины и определения).

Атака и вторжение. Система обнаружения вторжений

Атака – действия, предпринимаемые злоумышленником, против компьютера (или сети) потенциальной жертвы.

Атака может быть:

- Безуспешной (неудачной);
- Успешной (удачной).

Успешную атаку называют вторжением.

Вторжение – несанкционированный вход в информационную систему в результате действий, нарушающих политику безопасности или обходящих систему защиты.

Политика информационной безопасности (организации); **политика ИБ (организации)**: Формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

Примечание - Политики должны содержать:

- предмет, основные цели и задачи политики безопасности;
- условия применения политики безопасности и возможные ограничения;
- описание позиции руководства организации в отношении выполнения политики безопасности и организации режима информационной безопасности организации в целом;
- права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности организации;
- порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности.

(ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения).

Средство обнаружения вторжений, средство обнаружения атак: Программное или программно-техническое средство, которое автоматизирует процесс контроля событий, протекающих в компьютерной системе или сети, а также самостоятельно анализирует эти события в поисках признаков инцидента информационной безопасности. (ГОСТ Р 53114-2008)

Система обнаружения вторжений – это программный или программно-аппаратный комплекс, предназначенный для выявления и по возможности предупреждения действий, угрожающих безопасности информационной системы.

Событие и инцидент ИБ. Является ли событие безопасности частью атаки?

Событие - возникновение или изменение определённого набора обстоятельств (ISO Guide 73:2009 (Банк данных угроз безопасности информации ФСТЭК России)).

Событие информационной безопасности (information security event): Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности (ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности)

Инцидент информационной безопасности (information security incident): Появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ (ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности).

SOC (Security Operation Center) – ситуационный центр информационной безопасности (центр мониторинга и реагирования на инциденты информационной безопасности).

Является ли событие безопасности является частью атаки?

Как только событие нарушает политику безопасности, оно сразу рассматривается как часть атаки.

Атака отличается от события безопасности тем, что в случае атаки злоумышленник пытается достичь некоторого результата, противоречащего политике безопасности.

Например, доступ пользователя к файлу или вход в систему — это событие безопасности. Однако, если этот доступ или вход осуществляется в нарушение прав доступа, то это уже атака.

Научное и прикладное значение моделирования систем защиты информации

В процессе проектирования сложных систем, таких как комплексные и интегрированные СЗИ информационных систем (ИС), в большинстве случаев прибегают к моделированию основных процессов, происходящих внутри системы и на стыке среда-система. Кроме того, **модели могут использоваться для проведения мониторинга и аудита безопасности на этапах эксплуатации и сопровождения ИС**.

Под моделированием здесь понимается математическое моделирование, позволяющее получить формальное описание системы и производить в дальнейшем количественные и качественные оценки ее показателей.

Выделим следующие теории, которые могут быть использованы при моделировании СЗИ:

- теории вероятностей и случайных процессов;
- теории графов, автоматов и сетей Петри;
- теория нечетких множеств;
- теории игр и конфликтов;
- теория катастроф;
- эволюционное моделирование;
- формально-эвристический подход;
- энтропийный подход.

Методы моделирования систем защиты информации

Отличия большинства моделей заключаются в том, какие параметры они используют в качестве входных, а какие — представляют в виде выходных после проведения расчетов.

Кроме того, **в последнее время широкое распространение получают методы моделирования, основанные на неформальной теории систем: методы структурирования, методы оценивания и методы поиска оптимальных решений.**

Методы структурирования являются развитием формального описания, распространяющимся на организационно-технические системы.

Использование этих методов позволяет представить архитектуру и процессы функционирования сложной системы в виде, удовлетворяющем следующим условиям:

1. полнота отражения основных элементов и их взаимосвязей;
2. простота организации элементов и их взаимосвязей;
3. гибкость — простота внесения изменений в структуру и т. д.

Методы оценивания позволяют определить значения характеристик системы, которые не могут быть измерены или получены с использованием аналитических выражений, либо в процессе статистического анализа, — вероятности реализации угроз, эффективность элемента системы защиты и др.

В основу таких методов положено экспертное оценивание — подход, заключающийся в привлечении специалистов в соответствующих областях знаний для получения значений некоторых характеристик.

Методы поиска оптимальных решений представляют собой обобщение большого количества самостоятельных, в большинстве своем математических теорий с целью решения задач оптимизации. В общем случае к этой группе можно также отнести методы неформального сведения сложной задачи к формальному описанию с последующим применением формальных подходов. Комбинирование методов этих трех групп позволяет расширить возможности применения формальных теорий для проведения полноценного моделирования систем защиты.

1. Краткие сведения из теории графов

Графовые модели систем защиты информации

Граф $G=[R, A]$ – это совокупность двух множеств: множества R точек , которые называются вершинами, и множества A ребер. Каждый элемент $a \in A$ есть упорядоченная пара (p_i, p_j) элементов множества R, вершины p_i и p_j называются концевыми точками или концами ребра a.

Граф называется конечным, если множества R и A конечны.

Это определение графа должно быть дополнено в одном важном отношении. В определении ребра можно принимать или не принимать во внимание порядок расположения двух его концов. Если этот порядок несущественен, т. е. если $(p_i, p_j) = (p_j, p_i)$, то говорят, что a есть неориентированное ребро; если же этот порядок существенен, то a называется ориентированным ребром (ориентированное ребро часто называется дугой). В последнем случае p_i называется также начальной вершиной, а p_j – конечной вершиной ребра a.

Граф называется неориентированным, если каждое его ребро неориентировано, и ориентированным, если ориентированы все его ребра. В ряде случаев естественно рассматривать смешанные графы, имеющие как ориентированные, так и неориентированные ребра.

Графовые модели систем защиты информации

Ребра, имеющие одинаковые концевые вершины, называются **параллельными**.

Ребро, концевые вершины которого совпадают, называется **петлей**. Она обычно считается неориентированной.

Вершина и ребро называются **инцидентными** друг другу, если вершина является для этого ребра концевой.

Вершина, не инцидентная никакому ребру, называется **изолированной**.

Граф, состоящий только из изолированных вершин, называется **нуль-графом**.

Две вершины, являющиеся концевыми для некоторого ребра называются **смежными вершинами**.

Два ребра, инцидентные одной и той же вершине, называются **смежными**.

Число ребер, инцидентных одной вершине p_i, будем обозначать через $\rho(p_i)$. Это число называется **локальной степенью или просто степенью графа в вершине** p_i.

В случае ориентированного графа G обозначим через $\rho(p_i)$ и $\rho^*(p_i)$ число ребер, соответственно выходящих из вершины p_i и входящих в p_i. Эти числа называются локальными степенями G в p_i.

Если все числа $\rho(p_i)$ (т. е. локальные степени G в p_i) конечны, то граф называется **локально-конечным**.

Вершина степени 1 называется **висячей**.

Вершина степени 0 называется **изолированной**.

Графовые модели систем защиты информации

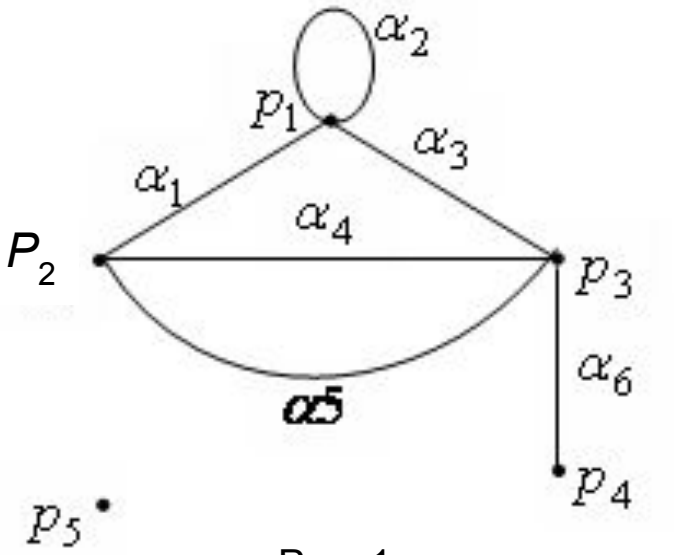


Рис. 1

На рис. 1:

a_4 и a_5 – параллельные ребра;

a_2 – петля;

вершина p_3 и ребро a_3 инцидентны друг другу;

p_1, p_2 – смежные вершины;

a_1 и a_4 – смежные ребра;

локальная степень вершины p_1 равна трем, p_4 – висячая вершина, p_5 – изолированная.

Графовые модели систем защиты информации

Граф *G* называется **полным**, если любые две его различные вершины соединены ребром и он не содержит параллельных ребер.

Дополнением графа *G* называется граф *G (надчерк.)* с теми же вершинами, что и граф *G* и содержащий только те ребра, которые нужно добавить к графу *G*, чтобы получился полный граф.

На рис. 2 изображены следующие графы: G_1 – полный граф с пятью вершинами, G_2 – некоторый граф, имеющий пять вершин, G_2 *(надчерк.)* – дополнение графа G_2.

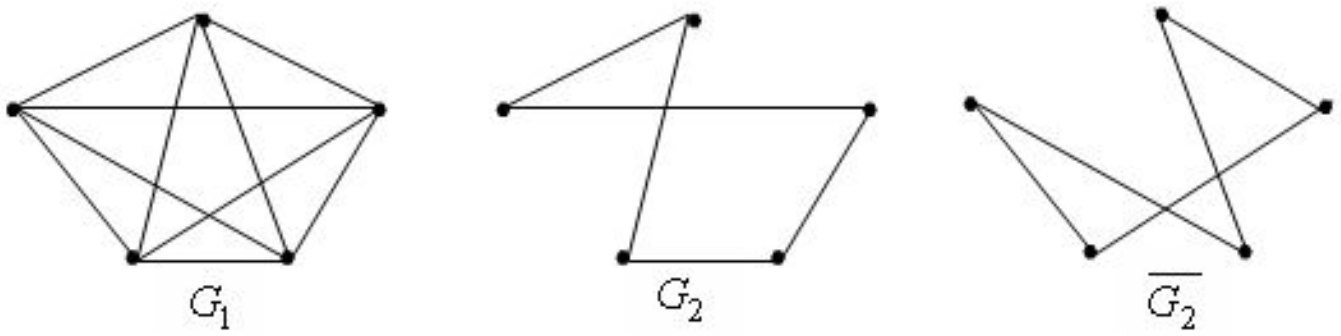


Рис. 2

Когда каждому ребру графа поставлено в соответствие некоторое значение, называемое весом ребра, тогда такой граф взвешенный. В разных задачах в качестве веса могут выступать различные виды измерений, например длины, цены, скорости передачи данных и т. п. В графическом представлении графа весовые значения указываются, как правило, рядом с ребрами.

Графовые модели систем защиты информации

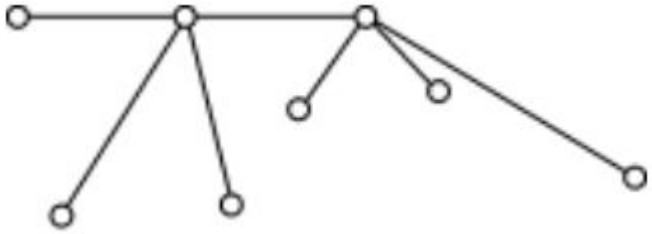
Плоским графом G называется граф, изображенный на плоскости так, что никакие два его ребра геометрически не пересекаются нигде, кроме инцидентной им обоим вершины.

Граф G называется плоским, если он может быть изображен на плоскости так, что все пересечения ребер являются его вершинами.

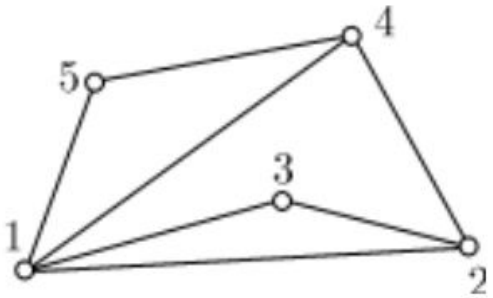
Граф, изоморфный* плоскому графу, называется **планарным**. Планарный граф можно определить еще так: граф планарен, если его можно уложить на плоскости. Рисунок графа, в котором никакие два его ребра не пересекаются, если не считать точками пересечения общие вершины, называют плоским представлением графа. Ясно, что плоское представление имеет только плоский граф. Обратно, у всякого плоского графа непременно найдется плоское представление.

Примером неплоского графа может служить полный граф с пятью вершинами. Любые попытки начертить его плоское представление обернутся неудачей.

На рис. 2а изображены следующие графы: G_1 – плоский граф с восемью вершинами, G_2 – плоское представление некоторого неполного графа, имеющего пять вершин. Полный граф с пятью вершинами не может быть плоским.



G_1



G_2

Рис. 2а

*два графа G_1 и G_2 называются изоморфными, если между их вершинами установлено взаимнооднозначное соответствие, такое, что любые две вершины графа G_1 соединены так же, как и соответствующие вершины графа G_2.

Иными словами, изоморфные графы различаются только обозначением вершин.

Графовые модели систем защиты информации

Двудольный граф или биграф — это математический термин теории графов, обозначающий граф, множество вершин которого можно разбить на две части таким образом, что каждое ребро графа соединяет какую-то вершину из одной части с какой-то вершиной другой части, то есть не существует ребра, соединяющего две вершины из одной и той же части.

Полный двудольный граф

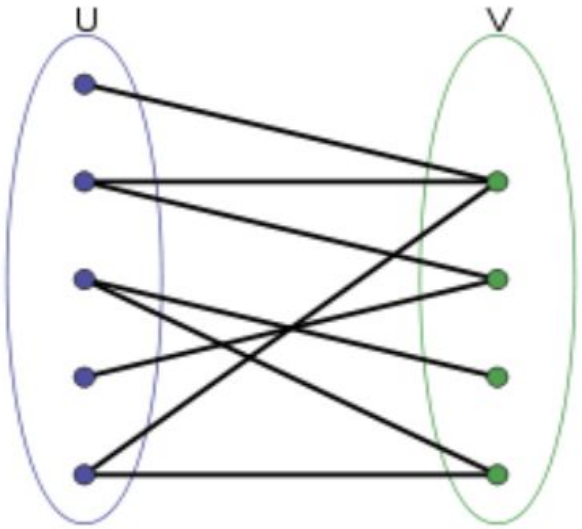
Неориентированный граф $G=(W,E)$ называется двудольным, если множество его вершин можно разбить на две части $U \cup V = W$, так, что ни одна вершина в U не соединена с вершинами в U и ни одна вершина в V не соединена с вершинами в V.

В этом случае, подмножества вершин U и V называются долями двудольного графа G.

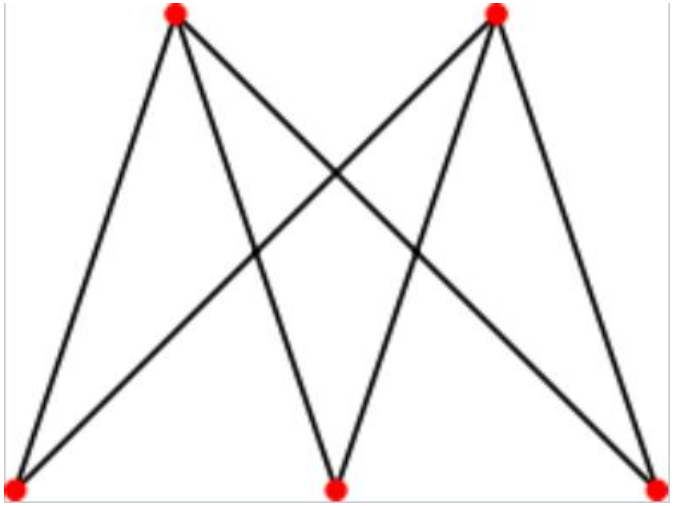
Двудольный граф называется **полным двудольным** (это понятие отлично от полного графа; то есть, такого, в котором каждая пара вершин соединена ребром), если для каждой пары вершин $u \in U$, $v \in V$, существует ребро $u, v \in E$.

Для $|U|=i, |V|=j$ такой граф обозначается символом $K_{i,j}$.

Двудольные графы естественно возникают при моделировании отношений между двумя различными классами объектов. К примеру граф футболистов и клубов, ребро соединяет соответствующего игрока и клуб, если игрок играл в этом клубе.



Двудольный граф



Полный двудольный граф $K_{3,2}$

Графовые модели систем защиты информации. Матричное представление

Граф может быть задан разными способами: рисунком, перечислением вершин и ребер (или дуг) и т. д.

Граф, как и большинство других математических объектов, может быть представлен на компьютере (сохранен в его памяти).

Существуют несколько способов интерпретации графа, вот наиболее известные из них:

· матрица смежности;

· матрица инцидентности;

· список смежности;

· список ребер.

Использование двух первых методов предполагает хранение графа в виде двумерного массива (матрицы). Причем размеры этих массивов, зависят от количества вершин и/или ребер в конкретном графе.

Так размер матрицы смежности $n \times n$, где n – число вершин, а матрицы инцидентности $n \times m$, где n – число вершин, m – число ребер в графе.

Графовые модели систем защиты информации. Матричное представление

Одним из самых удобных способов является задание графа с помощью матрицы.

Матрица смежности графа — это квадратная матрица, в которой каждый элемент принимает одно из двух значений: 0 или 1.

Матрица смежности графа G с конечным числом вершин n (пронумерованных числами от 1 до n) — это квадратная матрица A размера n, в которой значение элемента a_{ij} равно числу рёбер из i-й вершины графа в j-ю вершину.

Иногда, особенно в случае неориентированного графа, петля (ребро из i-й вершины в саму себя) считается за два ребра, то есть значение диагонального элемента a_{ij} в этом случае равно удвоенному числу петель вокруг i-й вершины.

Матрица смежности простого графа (не содержащего петель и кратных ребер) является двоичной (бинарной) матрицей и содержит нули на главной диагонали.

Это двоичная квадратная матрица, т. к. число строк в ней равно числу столбцов, и любой из ее элементов имеет значение либо 1, либо 0. Первая строка и первый столбец (не входят в состав матрицы и не показаны здесь, содержат номера, на пересечении которых находится каждый из элементов, и они определяют индексное значение последних. Имея в наличии лишь матрицу такого типа, несложно построить соответствующий ей граф.

Ниже (на рис. 3) приведён пример неориентированного графа и соответствующей ему матрицы смежности A. Этот граф содержит петлю вокруг вершины 1, при этом в зависимости от конкретных приложений элемент a_{11} может считаться равным либо одному (как показано ниже), либо двум.

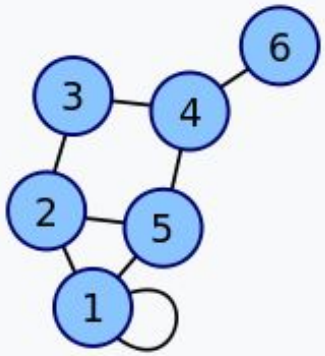
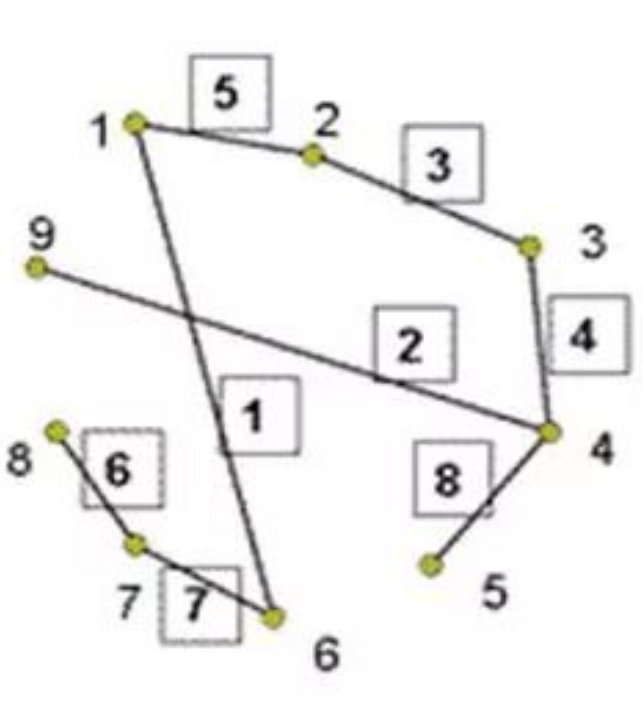
Граф	Матрица смежности
	$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$

Рис. 3

Графовые модели систем защиты информации. Матричное представление

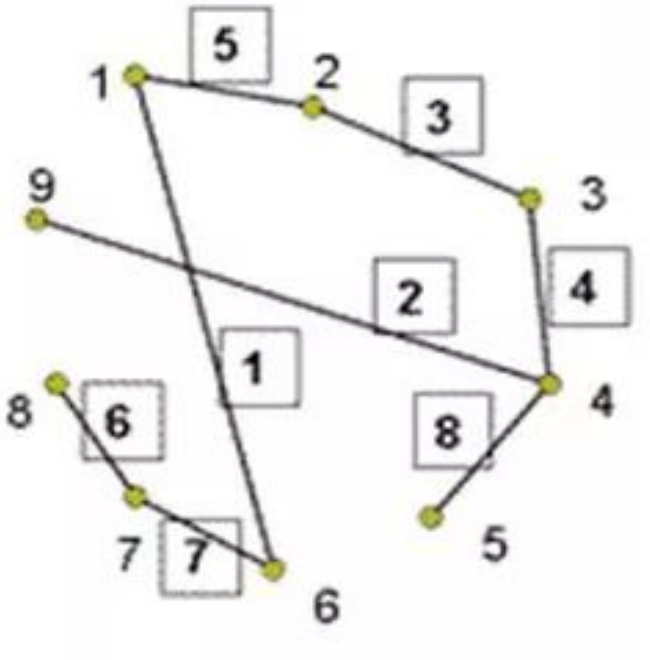
Самостоятельное задание:
Составить матрицу смежности неориентированного графа *G*, представленного на рисунке.



Граф *G*

Графовые модели систем защиты информации. Матричное представление

Контроль выполнения самостоятельного задания:
На рисунке представлен неориентированный граф *G* и соответствующая ему матрица смежности.



	1	2	3	4	5	6	7	8	9
1	0	1	0	0	0	1	0	0	0
2	1	0	1	0	0	0	0	0	0
3	0	1	0	1	0	0	0	0	0
4	0	0	1	0	1	0	0	0	1
5	0	0	0	1	0	0	0	0	0
6	1	0	0	0	0	0	1	0	0
7	0	0	0	0	0	1	0	1	0
8	0	0	0	0	0	0	1	0	0
9	0	0	0	1	0	0	0	0	0

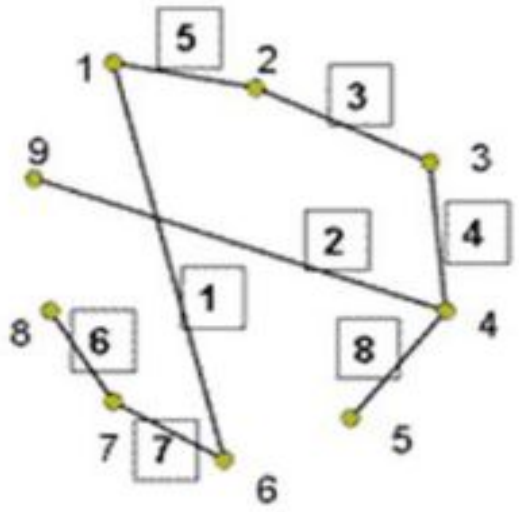
Граф *G* с матрицей смежности

Графовые модели систем защиты информации. Матричное представление

Матрица смежности с учетом весов ребер

Представим, что под вершинами подразумеваются уязвимости информационной системы, а под ребрами — информационные угрозы. Веса в этом случае могут обозначать вероятность реализации или сложность (возможность) реализации по шкале от 1 до 10.

На рисунке представлен неориентированный граф *G* и соответствующая ему матрица смежности.



	1	2	3	4	5	6	7	8	9
1	0	5	0	0	0	1	0	0	0
2	5	0	3	0	0	0	0	0	0
3	0	3	0	4	0	0	0	0	0
4	0	0	4	0	8	0	0	0	2
5	0	0	0	8	0	0	0	0	0
6	1	0	0	0	0	0	7	0	0
7	0	0	0	0	0	7	0	6	0
8	0	0	0	0	0	0	6	0	0
9	0	0	0	2	0	0	0	0	0

Граф *G* и его матрица смежности с учетом весов ребер

Графовые модели систем защиты информации. Матричное представление

Матрица инцидентности строится по следующему принципу: матрица инцидентности имеет размер $n \times m$, где n – число вершин графа, m – число ребер, чтобы задать значение какой-либо ячейки, нужно сопоставить вершину с ребром.

Пусть некоторый граф G имеет n вершин и m ребер. Построим матрицу, имеющую n строк и m столбцов. Каждая строка матрицы будет соответствовать вершине, а столбец – ребру графа.

В каждой ячейке матрицы инцидентности неориентированного графа стоит 0 или 1, а в случае ориентированного графа, вносятся 1, 0 или -1. То же самое, но наиболее структурировано:

1. неориентированный граф:
· 1 – вершина инцидентна ребру;
· 0 – вершина не инцидентна ребру.

2. ориентированный граф:
· 1 – вершина инцидентна ребру, и является его началом;
· 0 – вершина не инцидентна ребру;
· -1 – вершина инцидентна ребру, и является его концом.

Построим матрицу инцидентности сначала для неориентированного графа (рис. 4), а затем для ориентированного графа (рис. 5). Ребра обозначим буквами от a до e, вершины – цифрами. Все ребра графа не направленны, поэтому матрица инцидентности заполнена положительными значениями.

	a	b	c	d	e
1	1	1	0	0	0
2	1	0	1	1	0
3	0	0	0	1	1
4	0	1	1	0	1

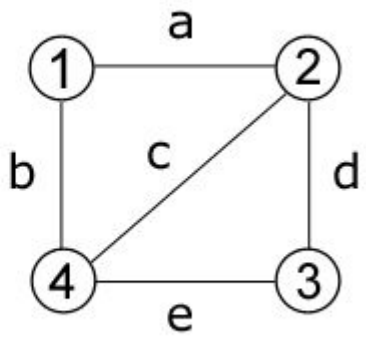


Рис. 4

Графовые модели систем защиты информации. Матричное представление

Для ориентированного графа матрица имеет немного другой вид. В каждую из ее ячеек внесено одно из трех значений. Обратите внимание, что нули в двух этих матрицах занимают одинаковые позиции, ведь в обоих случаях структура графа одна. Но некоторые положительные единицы сменились на отрицательные, например, в неориентированном графе ячейка (1, b) содержит 1, а в ориентированном графе -1. Дело в том, что в первом случае ребро b не направленное, а во втором – направленное, и, причем вершиной входа для него является вершина «1».

Каждый столбец отвечает за какое-либо одно ребро, поэтому граф, описанный при помощи матрицы инцидентности, всегда будет иметь следующий признак*: любой из столбцов матрицы инцидентности содержит две единицы (когда это неориентированное ребро), либо 1 и -1 когда это ориентированное ребро, все остальное в нем – нули.

В программе матрица инцидентности задается, также как и матрица смежности, а именно при помощи двумерного массива. Его элементы могут быть инициализированы при объявлении, либо по мере выполнения программы.

	a	b	c	d	e
1	1	-1	0	0	0
2	-1	0	1	1	0
3	0	0	0	-1	-1
4	0	1	-1	0	1

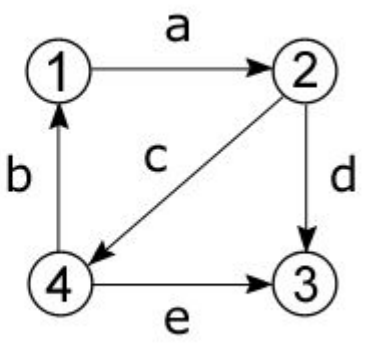
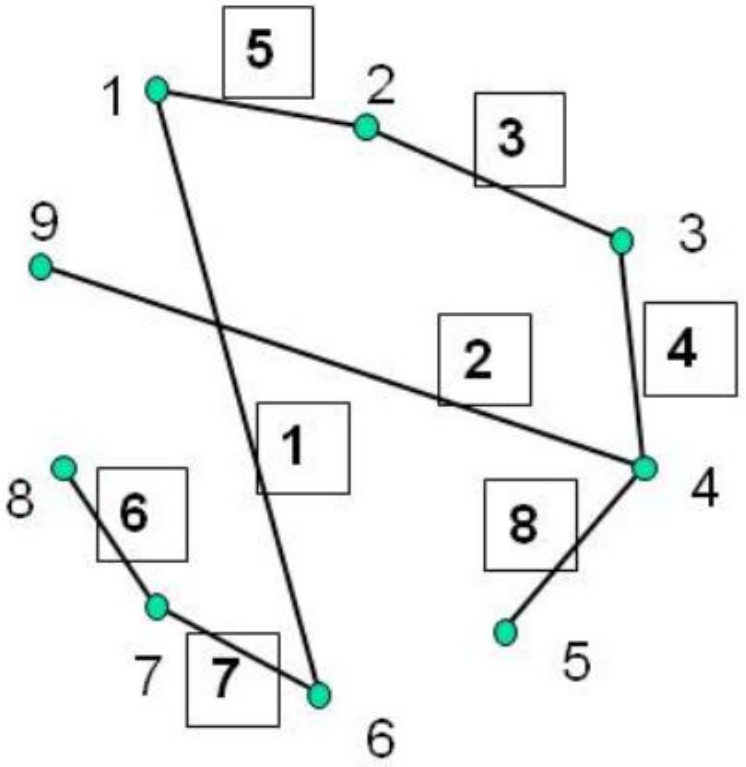


Рис. 5

*если в графе нет петель и изолированных вершин

Графовые модели систем защиты информации. Матричное представление

Самостоятельное задание:
Составить матрицу инцидентности неориентированного графа *G,* представленного на рисунке.

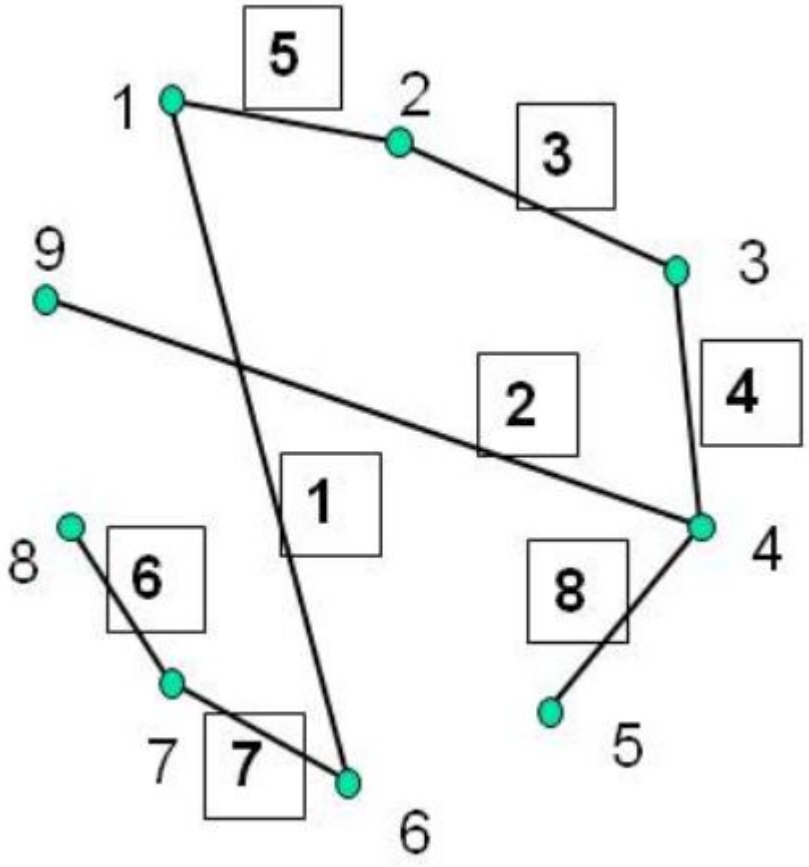


Граф *G*

Графовые модели систем защиты информации. Матричное представление

Контроль выполнения самостоятельного задания:

На рисунке представлен неориентированный граф *G* и соответствующая ему матрица инцидентности.



	1	2	3	4	5	6	7	8
1	1	0	0	0	1	0	0	0
2	0	0	1	0	1	0	0	0
3	0	0	1	1	0	0	0	0
4	0	1	0	1	0	0	0	1
5	0	0	0	0	0	0	0	1
6	1	0	0	0	0	0	1	0
7	0	0	0	0	0	1	1	0
8	0	0	0	0	0	1	0	0
9	0	1	0	0	0	0	0	0

Граф *G* с матрицей инцидентности

2. Графовые модели компьютерных атак

Графовые модели компьютерных атак

Рассмотрим далее несколько приложений математической теории графов к моделированию СЗИ, первым из которых являются графы компьютерных атак*. Неформально, граф атаки — это граф, представляющий все возможные последовательности действий нарушителя для реализации угрозы. Такие последовательности действий называются путями атак (рис. 7).

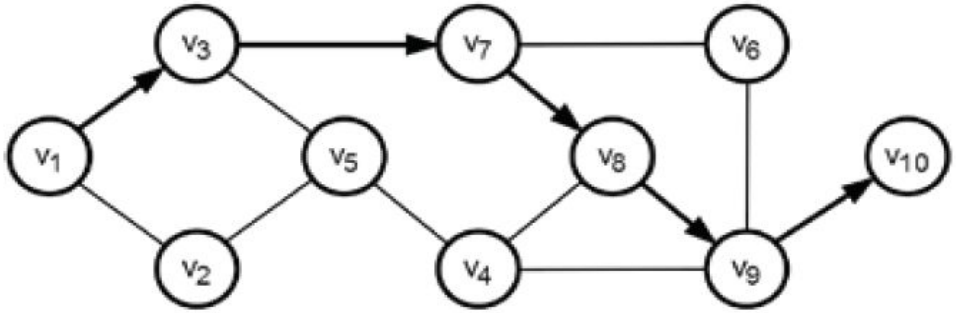


Рис. 7. Граф атаки

Выделяют следующие виды графов атак:

− **state enumeration graph** (граф перечисления состояний) — в таких графах вершинам соответствуют тройки *(s, d, a)*, где *s* — источник атаки, *d* — цель атаки, *a* — элементарная атака (или использование уязвимости); дуги обозначают переходы из одного состояния в другое;

− **condition-oriented dependency graph** (граф зависимостей, ориентированных на условия) — вершинам соответствуют результаты атак, а дугам — элементарные атаки, приводящие к таким результатам;

− **exploit dependency graph** (граф зависимостей эксплойтов или **г**раф условий реализации возможностей эксплойтов**) — вершины соответствуют результатам атак или элементарным атакам, дуги отображают зависимости между вершинами — условия, необходимые для выполнения атаки и следствие атаки.

Такие модели применяются в основном на этапе аудита безопасности сетей для выявления слабых мест системы защиты и прогнозирования действий нарушителя.

*компьютерная атака: Целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств (ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения)

**Эксплойты — это подвид вредоносных программ. Они содержат данные или исполняемый код, способный воспользоваться одной или несколькими уязвимостями в программном обеспечении на локальном или удаленном компьютере.

Графовые модели атак

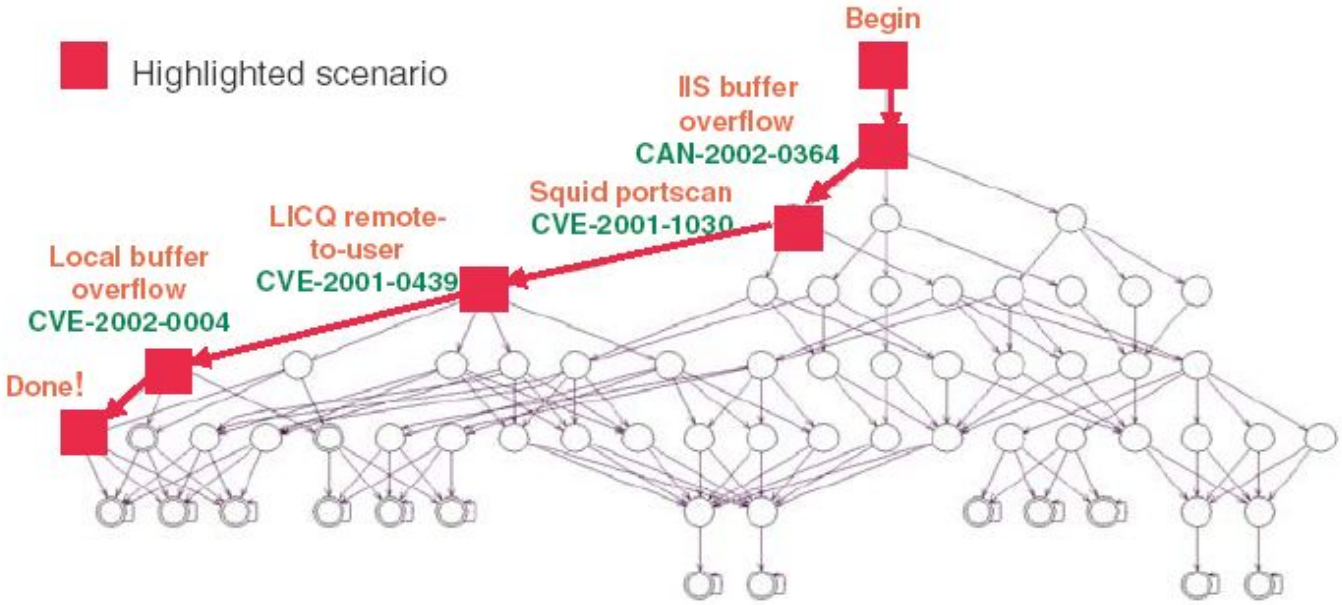
Исследования, связанные с построением, анализом и применением графов атак, ведутся приблизительно с 1994 года. В отечественной литературе данной тематике уделяется незначительное внимание, несмотря на то, что в зарубежных публикациях приводятся примеры эффективно работающих систем, в том числе и коммерческих.

Неформально, граф атак – это граф, представляющий всевозможные последовательности действий нарушителя для достижения угроз (целей). Такие последовательности действий называются трассами (путями) атак.

На рис. 8 – 10 изображены примеры графов атак.

State enumeration graph (граф перечисления состояний) (рис. 8) – в таких графах вершинам соответствуют тройки (s, d, a), где s – источник атаки, d – цель атаки, a – элементарная атака*; дуги обозначают переходы из одного состояни

Рис. 8



*Под элементарной атакой (atomic attack) понимают использование нарушителем уязвимости, например, переполнение буфера службы SSH, позволяющее удаленно получить права администратора системы.

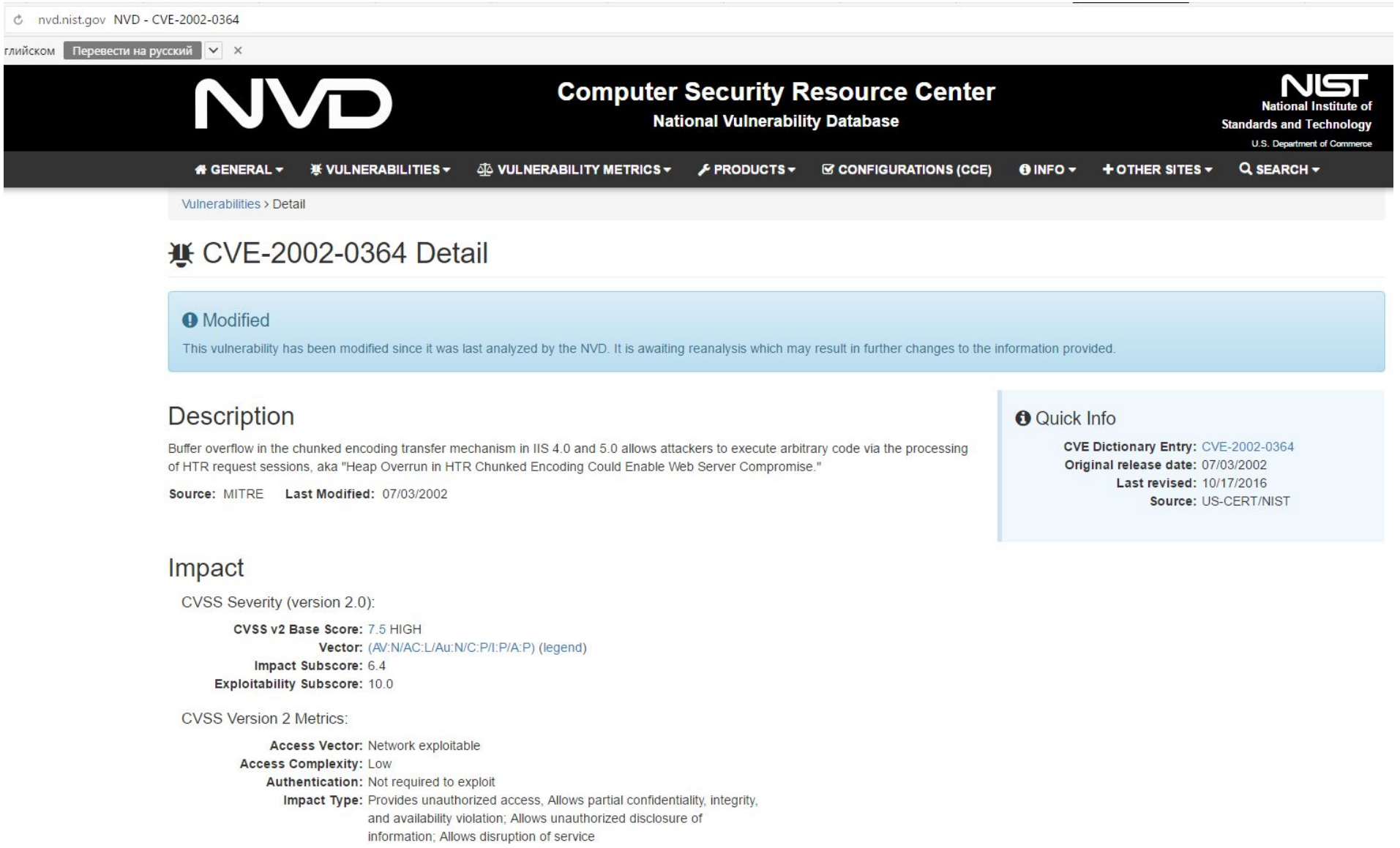
CVE — базы уязвимостей NIST США (CVE-2002-0364 – идентификатор уязвимости);

IIS (Internet Information Services, до версии 5.1 — Internet Information Server) —набор серверов для нескольких служб Интернета от компании Майкрософт (распространяется с операционными системами семейства Windows NT).

Основным компонентом IIS является веб-сервер, который позволяет размещать в Интернете сайты. IIS поддерживает протоколы HTTP, HTTPS, FTP, POP3, SMTP, NNTP. По данным компании Netcraft на июнь 2015 года, почти 22 млн сайтов обслуживаются веб-сервером IIS, что составляет 12,32 % от общего числа веб-сайтов.

Национальная база данных уязвимостей (NIST США)

Исследования,



Графовые модели атак

Condition-oriented dependency graph (граф зависимостей, ориентированных на условия) (рис. 9) – вершинам соответствуют результаты атак, а дугам – элементарные атаки, приводящие к таким результатам;

Exploit dependency graph (граф условий реализации возможностей эксплойтов*) (рис. 10) – вершины соответствуют результатам атак или элементарным атакам, дуги отображают зависимости между вершинами – условия, необходимые для выполнения атаки и следствие атаки. Например, атака RSH*** возможна, если нарушитель имеет привилегии суперпользователя на хосте** 1 и хост 3 доверяет хосту 1. В результате атаки нарушитель получает привилегии пользователя на хосте 3.

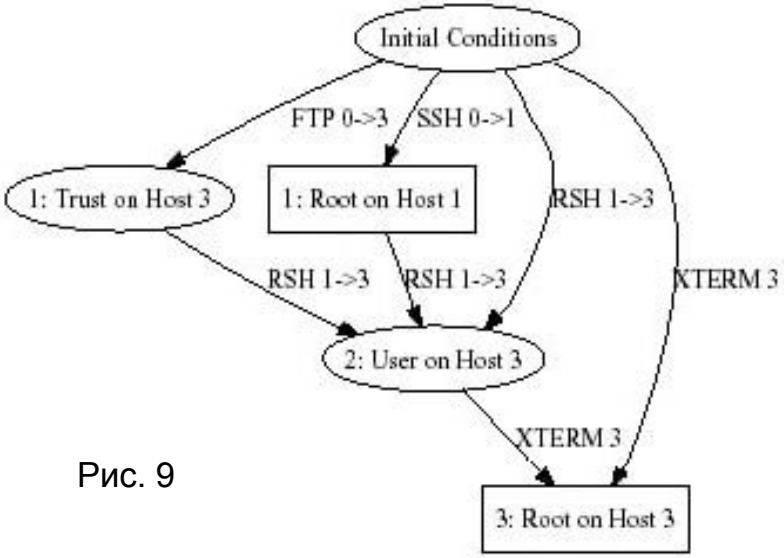


Рис. 9

Рис. 10

*Эксплойт (от англ. exploit - эксплуатировать) - это компьютерная программа, фрагмент кода или последовательность команд, использующих уязвимости в ПО и предназначенные для проведения атаки на вычислительную систему.

**Хост (от англ. host — «хозяин, принимающий гостей») — любое устройство, предоставляющее сервисы формата «клиент-сервер» в режиме сервера по каким-либо интерфейсам и уникально определённое на этих интерфейсах.

***RSH расшифровывается как Remote SHell - протокол, позволяющий подключаться удаленно к устройству и выполнять на нем команды. Типичным (и самым опасным) механизмом, использующим доверие, является механизм доверенных хостов, при подключении с которых с помощью r-служб можно зарегистрироваться под любым именем, кроме root, без указания пароля. Вскрыв один из хостов, кракер сможет легко по цепочке добраться до следующих. Опаснее другое: если система, которую собираются атаковать, содержит шаблон "+" (в некоторых системах он стоит по умолчанию) в файлах, где описываются доверенные хосты, то все хосты становятся доверенными для данного.

****xterm является стандартным эмулятором терминала в Unix. Пользователь имеет возможность работать с несколькими xterm терминалами, запущенными в одно и то же время на одном и том же дисплее. Каждый из виртуальных терминалов предоставляет независимый ввод-вывод для процессов, запущенных в каждом из них.

Графовые модели атак

Использование недостатков идентификации tcp-пакетов для атаки на rsh-сервер

В ОС UNIX существует понятие: доверенный хост. Доверенным по отношению к данному хосту называется хост, доступ на который пользователю с данного хоста возможен без его аутентификации и идентификации с помощью r-службы. Обычно, в ОС UNIX существует файл rhost, в котором находится список имен и IP-адресов доверенных хостов. Для получения к ним удаленного доступа пользователю необходимо воспользоваться программами, входящими в r-службу (например, rlogin, rsh и.т.д.). В этом случае при использовании r-программ пользователю для получения удаленного доступа не требуется проходить стандартную процедуру идентификации и аутентификации, заключающуюся во вводе его логического имени и пароля. Аутентифицирующей информацией для r-службы является IP-адрес хоста, с которого пользователь осуществляет r-доступ. Отметим, что все программы из r-службы реализованы на базе протокола TCP. Одной из программ, входящих в r-службу, является rsh,с помощью которой возможно осуществление данной атаки. Программа rsh (remote shell) позволяет отдавать команды shell удаленному хосту. При этом, что является чрезвычайно важным в данном случае, для того, чтобы отдать команду, достаточно послать запрос, но необязательно получать на него ответ. При атаке на r-службы вся сложность для атакующего заключается в том, что ему необходимо послать пакет от имени доверенного хоста, то есть, в качестве адреса отправителя необходимо указать IP-адрес доверенного хоста. Следовательно, ответный пакет будет отправлен именно на доверенный хост, а не на хост атакующего.

Схема удаленной атаки на rsh-сервер была впервые описана небезызвестным P.T. Моррисом в Belt Labs computer Science Technical Report #117, February 25, 1985. Она заключается в следующем:

Пусть хост A доверяет хосту B. Хост X - это станция атакующего.

Вначале атакующий X открывает настоящее TCP-соединение с хостом B на любой TCP-порт (mail, echo и т.д.). В результате X получит текущее значение на данный момент времени ISSb. Далее, X от имени A посылает на B TCP-запрос на открытие соединения:

1. X->B: SYN.ISSx

Получив этот запрос, B анализирует IP—адрес отправителя и решает, что пакет пришел с хоста A. Следовательно, B в ответ посылает на A новое значение ISSb':

2. B ->A: SYN,ACK, ISSb', ACK(ISSx+1)

X никогда не получит это сообщение от B, но, используя предыдущее значение ISSb и схему для получения ISSb‘ (см. выше),может послать на B:

3. X ->B: ACK, ISSx+1, ACK(ISSb'+1)

Отметим, что для того, чтобы послать этот пакет потребуется перебрать некоторое количество возможных значений ACK(ISSb'+1), но не потребуется подбор ISSx+1,так как этот параметр TCP-соединения был послан с X на B в первом пакете.

В итоге rsh-сервер на хосте B считает, что к нему подключился пользователь с доверенного хоста A, а на самом деле это атакующий с хоста X. И хотя X никогда не увидит пакеты с хоста B, но он сможет выполнять на нем команды.

Графовые модели атак

При синтезе графа атак возникают следующие задачи: формализация понятия атаки, разработка формального языка моделирования атак и компьютерной системы (включающей нарушителя, его цели, сеть, средства защиты, отношение достижимости хостов и т.д.), выбор или разработка средств построения графа атаки и его визуализации, разработка средств автоматизации построения и анализа графа.

В основном графы атак рассматриваются в контексте анализа защищенности сетей. Обычно такой анализ сводится к последовательному сканированию всех хостов сети на наличие известных уязвимостей. Результатом является отчет, содержащий перечень найденных уязвимостей и рекомендации по их устранению.

В настоящее время постепенно внедряется другая парадигма анализа защищенности, учитывающая “топологию” компьютерной системы – взаимосвязь объектов компьютерной системы, их свойств и характеристик. Такой анализ защищенности называется топологическим, а средства, его выполняющие, топологическими сканерами безопасности.

Топологический анализ защищенности предполагает построение графа атак на основе результатов сканирования сети, модели нарушителя и данных о конфигурации сети (фильтрации МЭ, маршрутизации, обнаружения атак, достижимости хостов и т.д.) **и его анализ** (вероятностный, минимизационный и т.д.).

Построенный граф содержит все известные сценарии атак для достижения нарушителем угроз.

Результатом его анализа может являться:

- перечень успешных атак, не обнаруживаемых IDS*;
- соотношение реализуемых мер безопасности и уровня защищенности сети;
- перечень наиболее критичных уязвимостей;
- перечень мер, позволяющих предотвратить использование уязвимостей в ПО, для которого отсутствуют обновления;
- наименьшее множество мер, реализация которых сделает сеть защищенной.

Графы атак также используются при расследовании компьютерных инцидентов, для анализа рисков и корреляций предупреждений систем обнаружения атак.

Первоначально графы атак строили вручную, затем были предложены различные подходы к автоматизации данного процесса.

Ключевой проблемой построения графа атак является масштабируемость – возможность построения графа атаки для сети с большим числом хостов и уязвимостей.

*Система обнаружения вторжений (СОВ), английский термин — Intrusion Detection System (IDS).— программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет. Системы обнаружения вторжений обеспечивают дополнительный уровень защиты компьютерных систем.

3. Риск-ориентированные графовые модели систем защиты информации

Риск-ориентированные графовые модели систем защиты информации

Одной из основных целей моделирования СЗИ является создание максимально эффективной системы.

Под эффективностью здесь понимается следование принципу «разумной достаточности», который можно описать следующим набором утверждений:

− абсолютно непреодолимой защиты создать нельзя;

− необходимо соблюдать баланс между затратами на защиту и получаемым эффектом, в т. ч. экономическим — снижении потерь от нарушения безопасности;

− стоимость средств защиты не должна превышать стоимости активов;

− затраты нарушителя на несанкционированный доступ (НСД) к активам должны превосходить эффект в соответствующем выражении, получаемый злоумышленником при осуществлении такого доступа.

Именно принцип «разумной достаточности» является базой подхода управления рисками, минимизирующего затраты от происшествий в сфере ИБ.

Рассмотрим далее вариант риск-ориентированной модели, использующей теорию графов.

Риск-ориентированные графовые модели систем защиты информации

Представим СЗИ в виде ориентированного графа $G = (T,C)$, **где вершинами** $T = \{ t_i \}, i = 1,n$ **будут угрозы активам со стороны злоумышленников, а дугами** C **— их связи** (рис. 11). При этом каждая дуга (t_k, t_l) будет обозначать связь угрозы t_k с угрозой t_l, вероятная реализация которой является прямым следствием реализации угрозы t_k.

Каждой угрозе поставим в соответствие параметры:

ω_{ti} — частота возникновения угрозы t_i;

p_{ti} — вероятность реализации угрозы t_i (например, вследствие успешной эксплуатации некоторой уязвимости);

d_{ti} — коэффициент разрушительности, выражающий степень разрушительности воздействия угрозы t_i на актив(ы);

$O_{ti} \subset O$ — набор активов или ресурсов, на которые направлена угроза t_i, где O — множество всех активов, задействованных в модели;

s_{ti} — стоимость средств и мер защиты от реализации угрозы t_i.

Каждую связь охарактеризуем величиной вероятности выбора злоумышленником пути реализации связанной угрозы — $p_{(ti, tj)}$.

Рис. 11. Граф угроз

Риск-ориентированные графовые модели систем защиты информации

Представим СЗИ в виде ориентированного графа $G = (T,C)$, **где вершинами** $T = \{ t_i \}, i = 1,n$ **будут угрозы активам со стороны злоумышленников, а дугами** C **— их связи** (рис. 11).

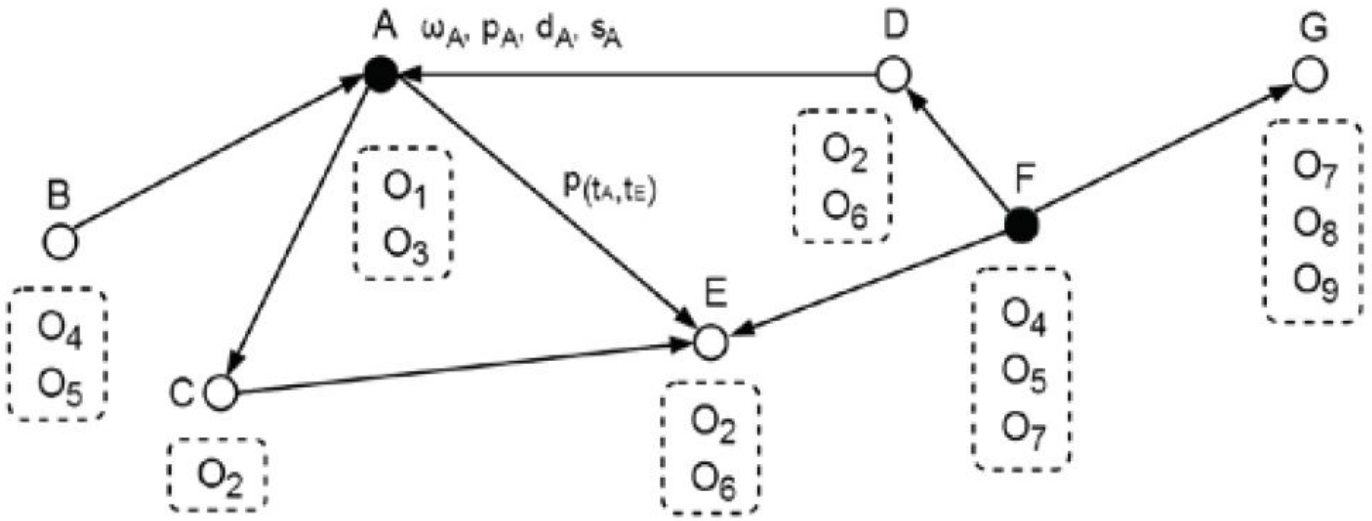


Рис. 11. Граф угроз

Риск-ориентированные графовые модели систем защиты информации

Вполне можно ожидать, что такой граф окажется двудольным*, поскольку не все угрозы могут быть реализованы непосредственно — осуществление некоторых атак возможно лишь при условии реализации «родительских» угроз (на рис. 6 схематично обозначены ●). Примером может служить НСД к конфиденциальной информации, требующий физического вмешательства в сетевую инфраструктуру.

Множества угроз и связей, а также их параметры определяются владельцами активов при участии экспертов — специалистов в области ИБ. Благодаря использованию такого набора данных и описанной структуры, появляется возможность устранить недостатки модели безопасности с полным перекрытием, в которой каждой угрозе противопоставлено свое средство защиты, однако вопросам экономической эффективности внимание не уделяется.

Сначала с помощью формул расчета стоимости риска вычисляются вероятные потери от реализации отдельных угроз (1),

$$R_{t_i} = \sum_{\substack{k, \\ o_k \in O_{t_i}}} \omega_{t_i} p_{t_i} d_{t_i} \mathrm{c}(o_k) \qquad (1)$$

где $c(o_к)$ — стоимость актива $o_к \in O_{τi}$,
и угроз, реализуемых друг за другом по некоторому пути $P(t_a,t_b)$ (2);

$$R_{P(t_a,t_b)} = R_{t_a} + \sum_{\substack{i,j \\ t_i,t_j \in P(t_a,t_b) \\ \exists(t_i,t_j)}} p_{(t_i,t_j)} R_{t_j} \qquad (2)$$

Затем, проводится сравнение стоимости риска с затратами на обеспечение ИБ: s_{ti} (от реализации угрозы t_i) или $S_{P(ta,tb)}$ (от реализации пути угроз $P(t_a,t_b)$, вычисляется по формуле (3), и принимается решение в отношении этого риска.

$$S_{P(t_a,t_b)} = \sum_{\substack{i \\ t_i \in P(t_a,t_b)}} s_{t_i} \qquad (3)$$

*граф, множество вершин которого можно разбить на две части таким образом, что каждое ребро графа соединяет какую-то вершину из одной части с какой-то вершиной другой части, то есть не существует ребра, соединяющего две вершины из одной и той же части.

Риск-ориентированные графовые модели систем защиты информации

Риск может быть:

− принят, если $R_{ti} \approx s_{ti}$;

− снижен за счет внедрения новых средств защиты, если $R_{ti} > s_{ti}$;

− устранен, если есть возможность отказаться от использования подверженного риску актива;

− передан третьей стороне, например, застрахован;

− игнорирован при незначительности своей величины.

Кроме того, при $R_{ti} < s_{ti}$ появляется возможность оптимизировать затраты на средства защиты.

Таким образом, **использование представленной модели, сочетающей в себе применение формальной математической теории и неформальных методов, таких как экспертное оценивание и поиск оптимальных решений, позволит решить прикладную задачу по минимизации рисков от происшествий в сфере ИБ.**

Доклад закончен. Прошу задать вопросы

Лекция:

Графовые модели систем защиты информации