УДК 004.056 **DOI** 10.15622/sp.57.9

Е.В. Дойникова, И.В. Котенко

СОВЕРШЕНСТВОВАНИЕ ГРАФОВ АТАК ДЛЯ МОНИТОРИНГА КИБЕРБЕЗОПАСНОСТИ: ОПЕРИРОВАНИЕ НЕТОЧНОСТЯМИ, ОБРАБОТКА ЦИКЛОВ, ОТОБРАЖЕНИЕ ИНЦИДЕНТОВ И АВТОМАТИЧЕСКИЙ ВЫБОР ЗАЩИТНЫХ МЕР

Дойникова Е.В., Котенко И.В. **Совершенствование графов атак для мониторинга кибербезопасности: оперирование неточностями, обработка циклов, отображение инцидентов и автоматический выбор защитных мер.**

Аннотация. Своевременность и адекватность реагирования на инциденты компьютерной безопасности, а также потери организаций от компьютерных атак, зависят от точности определения ситуации при мониторинге кибербезопасности. Статья посвящена совершенствованию моделей атак в виде графов для задач мониторинга кибербезопасности. Рассматривается ряд актуальных проблем, связанных с использованием графов атак, и способов их решения, в том числе оперирование неточностями при определении пред- и постусловий выполнения атакующих действий, обработка циклов при использовании байесовского вывода для анализа графа атак, отображение инцидентов на графе атак, а также автоматический выбор защитных мер в случае высокого уровня риска. Представлен реализованный ранее и модифицированный с учетом предложенных изменений программный прототип компонента системы мониторинга кибербезопасности и результаты экспериментов. Влияние изменений на результаты мониторинга кибербезопасности показано на примере оценки защищенности фрагмента компьютерной сети.

Ключевые слова: граф атак, вероятность атаки, мониторинг кибербезопасности, компьютерные сети, оценка защищенности, показатели защищенности, реагирование на атаки, оценивание уязвимостей.

1. Введение. В современном мире, когда компьютерные сети являются важнейшей частью инфраструктуры большинства организаций, наблюдается повышенный интерес к проведению кибератак, использующих уязвимости компьютерных сетей. Успешная реализация таких атак может привести к серьезному ущербу для деятельности организаций, напрямую зависящих от информационных технологий. Поскольку задача интегрированной киберзащиты организаций и устранения уязвимостей является трудоемкой, затратной по стоимости и не всегда оправданной, особенно важно проводить проактивный мониторинг кибербезопасности [1, 2] для своевременного выявления кибератак, распознавания целей и квалификации атакующих, эффективного предотвращения развития атак в системе, выявления текущего состояния защищенности и слабых мест системы, а также решения задач компьютерной криминалистики (форензики).

Для выявления возможных путей атак в компьютерных сетях широко используются графы атак. Они представляют собой множество

возможных атакующих действий и переходов между ними. В существующих исследованиях описываются различные виды графов атак [3-18]. Данное исследование основано на работах [19, 20], в которых каждое атакующее действие представляет собой эксплуатацию уязвимости сети. Переходы между действиями задаются пред- и постусловиями эксплуатации уязвимостей, определяемыми на основе индексов (показателей) системы оценивания уязвимостей Common Vulnerability Scoring System (CVSS) версии 2.0 [21]. На основе графа атак можно проследить путь атаки в системе от источника до цели атаки, определить, какие ресурсы сети находятся под угрозой, определить текущее состояние атаки на основе информации об инцидентах безопасности и сделать выводы о характеристиках атакующего.

Тем не менее практическое применение графов атак для заявленных целей мониторинга кибербезопасности затрудняется такими аспектами, как неопределенность исходных данных, сложность построения и анализа графов, и отсутствие удовлетворительных программных решений в области их построения и анализа.

В работе развивается метод построения и анализа модели атак в виде графа, предложенный в [19, 20, 22, 23]. Метод усовершенствован для удовлетворения целей мониторинга кибербезопасности и выбора защитных мер. Основной особенностью исходного метода является автоматизированное оперативное построение и анализ графов атак с применением открытых стандартов представления данных по безопасности и открытых баз уязвимостей. При этом к методу предъявляются следующие требования: учет всех возможных последовательностей атакующих действий; адекватная оценка защищенности анализируемой системы за счет вычисления уровня риска на основе вероятностей успешной реализации атакующих действий и тщательного учета ущерба, наносимого в результате успешной реализации атакующих действий.

Основными недостатками с точки зрения поставленных целей и требований являются:

– неточность определения значений индексов CVSS версии 2.0, что ведет к неточностям при построении графа (под неточностью в данном случае понимается такое определение значений, индексов, которое допускает неоднозначное толкование) и нарушает требование учета всех возможных последовательностей атакующих действий;

– отсутствие учета атак, не использующих уязвимости, что нарушает требование учета всех возможных последовательностей атакующих действий и создает сложности при отображении инцидентов на граф атакующих действий;

– удаление циклических связей между узлами графа в процесс анализа графа, что также нарушает требование учета всех возможных последовательностей атакующих действий;

– отсутствие выделения классов угроз на графе, что препятствует тщательному учету ущерба, наносимого в результате успешной реализации атакующих действий, и затрудняет автоматический выбор контрмер (в текущей реализации угроза определяется как последовательность эксплуатации уязвимостей, ущерб от их эксплуатации может отличаться, соответственно, различные классы угроз не разделяются).

Цель исследования — разработка эффективного подхода к построению и анализу графов атак, который позволит осуществлять адекватный мониторинг кибербезопасности и выбирать рациональные защитные меры. В данной работе в рамках поставленной цели решаются задачи по модификации метода построения и анализа графа атак для устранения перечисленных выше недочетов, а именно:

– для устранения неточностей, связанных с применением CVSS версии 2.0, предложены модификации подхода к построению и анализу графа атак на основе использования новой версии CVSS версии 3.0 [24];

– для учета атак, не использующих уязвимости, предложены модификации подхода на основе использования шаблонов атак CAPEC [25];

– определены модификации подхода для обработки циклов на графе атак для последующего анализа;

– узлы графа атак переопределены путем разбиения уязвимостей на новые группы, определенные в зависимости от причиняемого ущерба, для выделения различных классов угроз и эффективного выбора контрмер.

В статье проведен анализ влияния предложенных изменений на процесс мониторинга кибербезопасности и выбора контрмер. Таким образом, основной вклад данной статьи состоит в совершенствовании подхода к построению и анализу графа атак (на основе CVSS версии 3.0 и CAPEC, выделения и обработки различных типов циклов графа, а также выделения различных классов угроз в зависимости от причиняемого ущерба), необходимого для мониторинга кибербезопасности и выбора контрмер. Статья организована следующим образом. Во втором разделе рассмотрены релевантные исследования в области генерации графов атак, анализа защищенности и мониторинга кибербезопасности. В третьем разделе приведено описание подхода к построению и анализу графа атак, взятого за

основу, и предложения по его изменению. В четвертом разделе приведен пример применения подхода, кратко описаны результаты экспериментов и дискуссия. В заключении сделаны выводы по результатам работы и описаны будущие направления исследований.

2. Релевантные исследования. Для решения задач мониторинга кибербезопасности были разработаны различные классы систем мониторинга и управления инцидентами (SIEM). Тем не менее они, как правило, не реализуют функции детальной оценки рисков, моделирования и прогнозирования атак. Шаги в этом направлении были сделаны, например, в системе MaxPatrol SIEM компании Positive Technologies [26] и продукте OSSIM компании AlientVault [27], а также в рамках проекта MASSIF FP7 путем внедрения компонента моделирования атак на основе графов и оценки защищенности [28].

В то же время существует большое количество исследований в области построения и анализа графов атак [3-20]. В [3, 4] предлагаются подходы к повышению защищенности компьютерной сети с использованием графов атак. В [9] рассматривается анализ защищенности с использованием деревьев атак. Подходы к оценке риска на основе графов атак сформулированы в [13, 15]. В [14] для повышения защищенности компьютерной сети используются графы атак совместно с теорией игр. В [16] анализа графов атак применяется приближенный вывод. В [17] защищенность компьютерной сети оценивается на основе графов зависимостей эксплойтов. Основным недостатком графов, предложенных в данных работах, является сложность построения. В [5, 6, 20] рассматривается решение проблемы оперативного построения графов.

В ряде работ предлагается использовать вероятностные графы атак для оценки риска [13, 29], анализа защищенности с учетом характеристик атакующего [8], повышения защищенности динамических сетей [18], реагирования на вторжения [30, 31]. В других работах применяются байесовские графы атак. В том числе для оценки защищенности [11, 32, 33], оценки защищенности с учетом характеристик атакующего [34], динамической оценки защищенности [36].

Одной из основных сложностей при формировании байесовских графов атак является обработка циклов. Этот вопрос рассматривается в [35-37].

Кроме того, существуют инструменты, реализующие методики моделирования атак и оценки защищенности. К ним относятся система построения и анализа графов NetSPA [4], CAULDRON [38], SecurITree [39] и другие.

Несмотря на большое количество исследований, в них в недостаточной степени учитываются аспекты комплексного применения открытых стандартов, таких как система оценивания уязвимостей (CVSS) [21, 24] и классификация шаблонов атак (CAPEC) [25], для аналитического моделирования атак и контрмер. В данной работе эта задача рассматривается с учетом некоторых недостатков моделирования атак, которые необходимо решить для эффективного мониторинга кибербезопасности и выбора защитных мер. Предлагается модифицированный подход к построению и анализу графа, который учитывает особенности CVSS версии 3.0 и шаблоны CAPEC, позволяет обрабатывать циклы графа для вычисления показателей защищенности, а также выделять различные классы угроз для последующего выбора защитных мер путем переопределения узлов графа за счет разбиения уязвимостей на группы в зависимости от причиняемого ущерба.

3. Модель атак для мониторинга кибербезопасности и поддержки принятия решений. Развиваемый авторами подход к мониторингу кибербезопасности и поддержке принятия решений базируется на аналитическом моделировании. Основой для последующих модификаций является модель атак в виде графа, предложенная и подробно описанная в [20]. Входными данными для построения модели являются данные об анализируемой компьютерной сети, данные об уязвимостях ее программно-аппаратного обеспечения, и характеристики уязвимостей, полученные из открытых источников. Результатом является множество возможных последовательностей атакующих действий. Методика анализа защищенности и выбора контрмер на базе данного графа представлена в [22, 23].

В основе подхода к построению и анализу графа, а также выбору контрмер лежит применение открытых стандартов, позволяющих формализовать исходные данные, (CVSS — для определения связей в графе и вычисления показателей защищенности [21], Common Platform Enumeration (CPE) [40] — для представления программно-аппаратного обеспечения и Common Configuration Enumeration (CCE) [41] — для представления уязвимых конфигураций) и данных по безопасности из открытых источников (база NVD [42]) для автоматизации процесса анализа защищенности. В процессе исследований был выявлен ряд недочетов, уже освященных в предыдущих разделах. Модификации процесса генерации графа атак для устранения этих недочетов описаны ниже.

3.1. Модель атак с учетом CVSS версии 3.0. Граф атак задается как множество взаимосвязанных атакующих действий [20]. Каждое атакующее действие определяется как эксплуатация уязвимости некоторой группы. Для связи атакующих действий в последовательности атак, группы выделяются в соответствии с предусловиями эксплуатации уязвимостей на основе индексов CVSS версии 2.0 (*AccessVector* (*AV*) — вектор доступа к уязвимости) и постусловиями их эксплуатации (*priv* — полученные привилегии и/или *CIA* — ущерб конфиденциальности, целостности и доступности) (таблица 1).

Таблица 1. Группы уязвимостей, выделенные на основе CVSS версии 2.0

Группа	Индексы CVSS		
	AV	*priv*	*CIA*
Группа 1	N/A (сетевой доступ или доступ из смежной сети)	user/other (привилегии пользователя или другое)	any (любой ущерб)
Группа 2	N/A	admin (привилегии администратора)	any
Группа 3	N/A	none (не дает привилегий)	P/C (частичный или полный ущерб)
Группа 4	L (локальный доступ)	admin	any
Группа 5	L	user/other	$CIA > CIA_{группа1}$ (учитываются только те уязвимости, чья эксплуатация ведет к большему ущербу, чем при эксплуатации уязвимостей группы 1)
Группа 6	L	none	$CIA > CIA_{группа1}$

На рисунке 1*а* представлены связи между атакующими действиями, использующими уязвимости соответствующей группы в рамках одного хоста (узла сети).

Однако определение индексов CVSS версии 2.0 имеет ряд неопределенностей, что ведет к неточностям при формировании графа атакующих действий, в том числе:

– индекс *AV* принимает значение L (локальный доступ) как в случае физического, так и в случае логического доступа к компьютеру;

– индексы *Impact* не учитывают область, на которую распространяется ущерб от эксплуатации уязвимости.

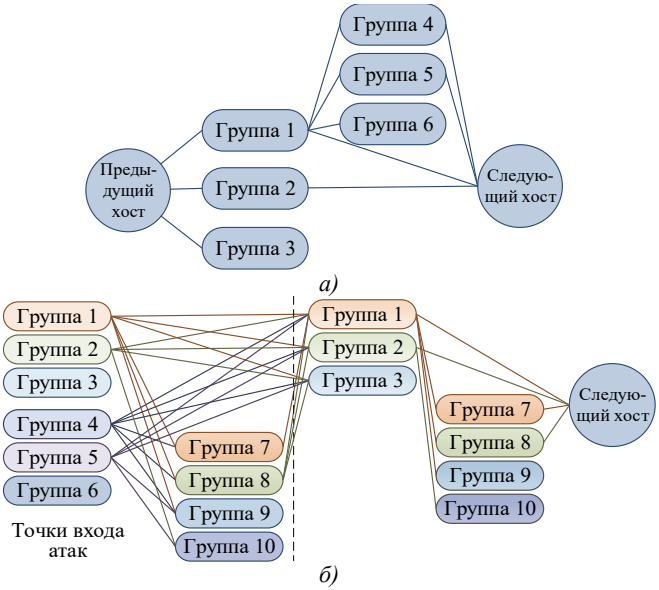

Рис. 1. Связи между группами уязвимостей для CVSS 2.0 (а) и CVSS 3.0 (б)

Кроме того, ряд неопределенностей ведет к неточностям при анализе графа атакующих действий, в том числе:

– индекс *AccessComplexity* (*AC*), характеризующий сложность эксплуатации уязвимости, не позволяет отдельно учитывать необходимость взаимодействия с пользователем;

– индекс *Authentication* (*Au*) определяет, требуется ли прохождение дополнительной процедуры аутентификации для эксплуатации уязвимости, но не определяет требуемый уровень привилегий.

Спецификация CVSS версии 3.0 была сформирована, чтобы устранить проблемы CVSS версии 2.0. При этом изменились определения и возможные значения ряда индексов CVSS:

– индекс *AV* переименован в *AttackVector* (обозначим его AV_{v3}, чтобы избежать путаницы с индексом *AV* CVSS версии 2.0), его значения разделены на «локальный» (L) и «физический» (P), чтобы выделить физический и логический тип доступа к компьютеру;

– для определения области, на которую распространяется ущерб от эксплуатации уязвимости, введен новый индекс *Scope* (*S*);

– индекс *AC* переименован в *AttackComplexity* (обозначим его AC_{v3}, чтобы избежать путаницы с индексом *AC* CVSS версии 2.0), и больше не включает взаимодействие с пользователем. Для учета необходимости взаимодействия с пользователем введен отдельный индекс *UserInteraction*;

– индекс *Au* заменен на индекс *PrivilegesRequired* (*PR*), определяющий требуемый для эксплуатации уязвимостей уровень привилегий.

На основе новых индексов CVSS версии 3.0 и их значений авторами данной работы были сформированы новые группы уязвимостей (таблица 2). На рисунке 1*б* представлены связи между атакующими действиями, использующими уязвимости соответствующей группы (с учетом входных точек атаки: Группа 1 — Группа 3 — у атакующего есть сетевой (удаленный) доступ к хосту в терминах сетевого уровня модели OSI, Группа 7 — Группа 10 — у атакующего есть локальный доступ к хосту, то есть для эксплуатации уязвимости атакующий должен быть авторизован на хосте или дождаться определенных действий авторизованного пользователя, и Группа 4 — Группа 6 — у атакующего есть физический доступ к хосту).

Таблица 2. Группы уязвимостей, выделенные на основе CVSS версии 3.0

Группа	Индексы CVSS			
	AV_{v3}	*PR*	*priv*	*CIA*
Группа 1	N/A	N (доступ к файлам и настройкам не требуется)	user/ other	any
Группа 2	N/A	N	admin	any
Группа 3	N/A	N	none	P/C
Группа 4	P (физический доступ)	N	user/ other	any
Группа 5	P	N	admin	any
Группа 6	P	N	none	P/C
Группа 7	L	L/N (L — атакующий зарегистрирован в системе с привилегиями, предоставляющими базовые возможности пользователя)	admin	any
Группа 8	L	L/N	user/ other	CIA>($CIA_{группа1}$) ИЛИ ($CIA_{группа4}$)
Группа 9	L	L/N	none	CIA>($CIA_{группа1}$) ИЛИ ($CIA_{группа4}$) ИЛИ ($CIA_{группа5}$)
Группа 10	L	H (для эксплуатации уязвимости требуются привилегии администратора)	any	CIA> ($CIA_{группа2}$) ИЛИ ($CIA_{группа5}$)

Как видно из рисунка 1*б*, схема связей между группами уязвимостей усложнилась, однако она позволяет сформировать возможные пути атак точнее, чем предложенная ранее схема, представленная на рисунке 1*а*.

Тем не менее в данном случае все еще не учитываются атакующие действия, не использующие уязвимости программно-аппаратного обеспечения, например разведывательные действия.

3.2. Модель атак с учетом шаблонов атак CAPEC. Для учета атакующих действий, не использующих уязвимости программно-аппаратного обеспечения, предлагается применять шаблоны атак CAPEC [25].

Шаблоны атак можно классифицировать по целям атаки. Для этого предлагается использовать значение поля «Цель» (“Purpose”) шаблона атаки. Данное поле может принимать значения: разведка, проникновение, эксплуатация, обфускация [25]. Например, шаблон CAPEC-169 «Footrinting» относится к шаблонам с целью «разведка», а шаблон CAPEC-100 «Overflow Buffers» — к шаблонам с целями «проникновение» и «эксплуатация».

При моделировании атак для учета данных шаблонов применяется следующий алгоритм:

1. Для атакующего выбираются доступные шаблоны атак с целью «разведка» с учетом уровня навыков атакующего (на основе значения поля шаблона «Attacker Skills or Knowledge Required») и слабых мест из базы CWE (Common Weakness Enumeration [43, 44]) доступных хостов (в случае, если не существует шаблонов с целью «разведка», соответствующих слабым местам доступных хостов, данный узел добавлен не будет). Указанные шаблоны добавляются между хостами как узел графа «Разведка» (рисунок 2*а*).

2. Узел «Разведка» соединяется с группами уязвимостей доступных хостов (рисунок 2*а*).

3. Узел графа «Обфускация» добавляется после группы уязвимостей в случае, если существуют шаблоны атак с целью «обфускация», соответствующие слабым местам CWE уязвимостей группы. Данный узел соединяется с соответствующей группой уязвимостей и следующей доступной группой уязвимостей, либо с узлом графа «Разведка» (см. шаг 4, рисунок 2*б*).

4. Узел графа «Разведка» добавляется после группы уязвимостей внутри хоста (либо после узла графа «Обфускация»), в случае, если существуют шаблоны атак с целью «разведка», соответствующие слабым местам CWE уязвимостей доступных групп (рисунок 2*в*).

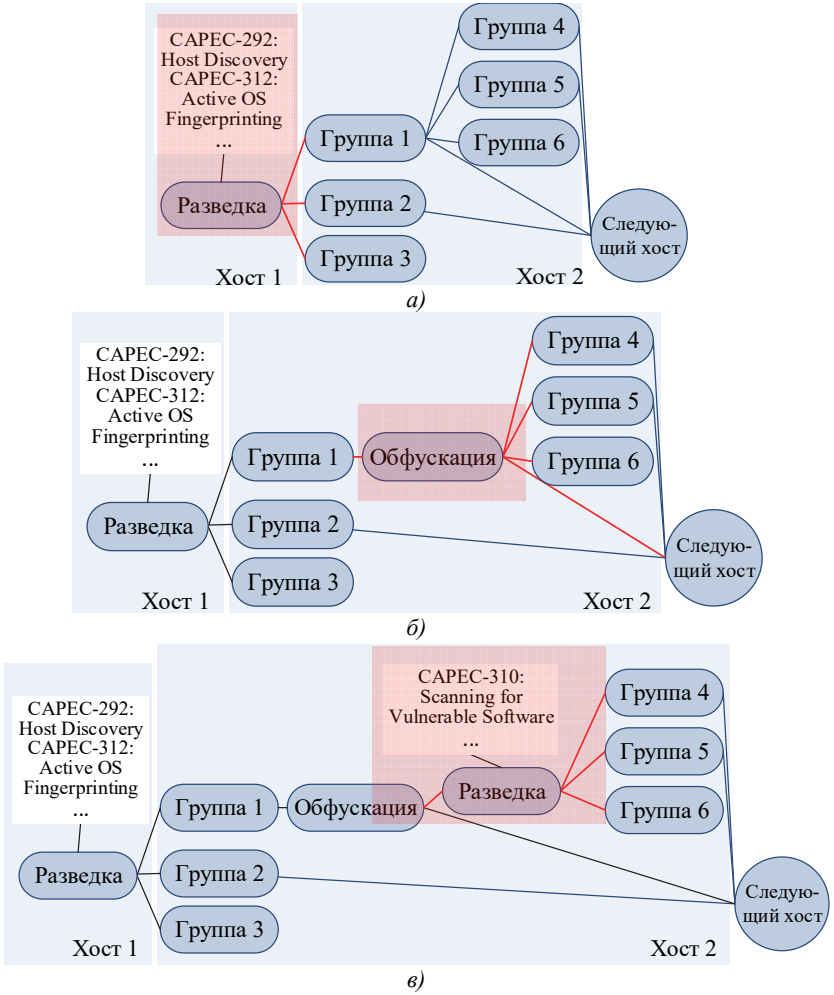

Рис. 2. Добавление шаблонов атак CAPEC на граф атакующих действий

Вышеперечисленные шаги выполняются для всех хостов компьютерной сети одновременно с формированием графа атак на основе уязвимостей. Добавление узлов, соответствующих шаблонам атак, позволяет сопоставить им обнаруженные инциденты разведывательной деятельности или заметания следов, информация о которых поступает от модуля корреляции событий безопасности SIEM-системы. Сопоставление осуществляется компонентом программы для целей анализа защищенности и выбора контрмер на

основе информации об узле сети, на котором зафиксирован инцидент, и последствий обнаруженного инцидента.

3.3. Обработка циклов для формирования вероятностного графа атак. Для анализа защищенности компьютерной сети при мониторинге кибербезопасности был выбран подход на основе байесовского вывода. Для преобразования исходного графа в байесовский граф атак каждому узлу графа были поставлены в соответствие следующие параметры: состояние атакующего действия *St* (вводится для последующего учета динамического характера атак, *St*={True, False}, где True означает, что узел скомпрометирован), локальная вероятность успешной реализации атакующего действия (вероятность, что *St*=True, без учета вероятности компрометации связанных узлов), условная вероятность успешной реализации атакующего действия (вероятность того, что *St*=True в случае различных состояний связанных узлов), и полная вероятность успешной реализации атакующего действия (или того, что действие находится в состоянии *St* (Pr∈[0,1]), с учетом всех возможных состояний связанных узлов). Кроме того, для графа атак определены два типа отношений между связями: И — для перехода в скомпрометированное состояние необходимо, чтобы все узлы-предки, связанные данным отношением, были скомпрометированы (цепочка последовательно связанных узлов графа); ИЛИ — для перехода в скомпрометированное состояние необходимо, чтобы хотя бы один из узлов-предков, связанных данным отношением, был скомпрометирован (узлы графа, находящиеся на одном уровне) [33, 36].

Данная модель была выбрана, так как байесовские графы атак позволяют учитывать влияние событий на состояние системы и в соответствии с этим делать предположения о предыдущих шагах атаки и прогнозировать развитие атаки в будущем. Кроме того, они позволяют делать выводы об атаке на основе субъективных знаний при отсутствии статистических данных об успешном использовании уязвимостей сети. Байесовский вывод применим только для графов, не содержащих циклов, поэтому для его использования необходимо обработать циклы исходного графа.

Исходный алгоритм формирования графа атак включает два основных шага:

1 Определение возможных атакующих действий на объекты компьютерной сети.

2 Формирование связей между ними.

На шаге 2 могут образоваться циклы. Типы циклов, которые возникают в процессе формирования связей, представлены на рисунке 3.

Предлагаются следующие методы обработки циклов:

– циклы *типа 1* (рисунок 3*а*) — узлы графа атак находятся на одном уровне структуры графа) могут быть удалены, поскольку вероятность попасть в вершину напрямую, а не через соседнюю вершину графа, будет выше (то есть вероятность попасть в вершину «Атакующее действие 2» напрямую из вершины «Атакующее действие 1» выше, чем вероятность попасть в вершину «Атакующее действие 2» из вершины «Атакующее действие 1» через вершину «Атакующее действие 3», так как во втором случае добавляется дополнительный элемент цикла, а любой дополнительный элемент уменьшает вероятность);

– циклы *типа 2* (рисунок 3*б*) — целевой узел расположен на более высоком уровне структуры графа (уровни структуры графа могут отличаться от структуры анализируемой компьютерной сети), чем исходный узел, и связан с ним путем на графе) могут быть удалены, поскольку для атакующего не имеет смысла возвращаться назад;

– циклы *типа 3* (рисунок 3*в*) сохраняются, но их связи помечаются как несуществующие и обрабатываются отдельно при анализе графа атак (входящая связь обрабатывается с учетом предположения, что исходящая связь не существует, и наоборот).

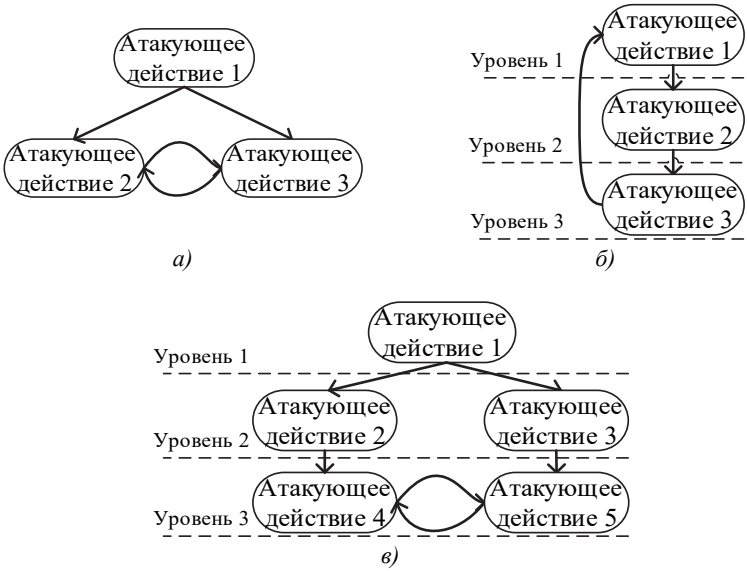

Рис. 3. Типы циклов для графа атакующих действий

На рисунке 4*а* приведен пример фрагмента компьютерной сети, граф атак для которой содержит цикл типа 1. Граф атак, содержащий цикл типа 1 представлен на рисунке 4*б*. На рисунке 4*в* представлен граф после обработки цикла.

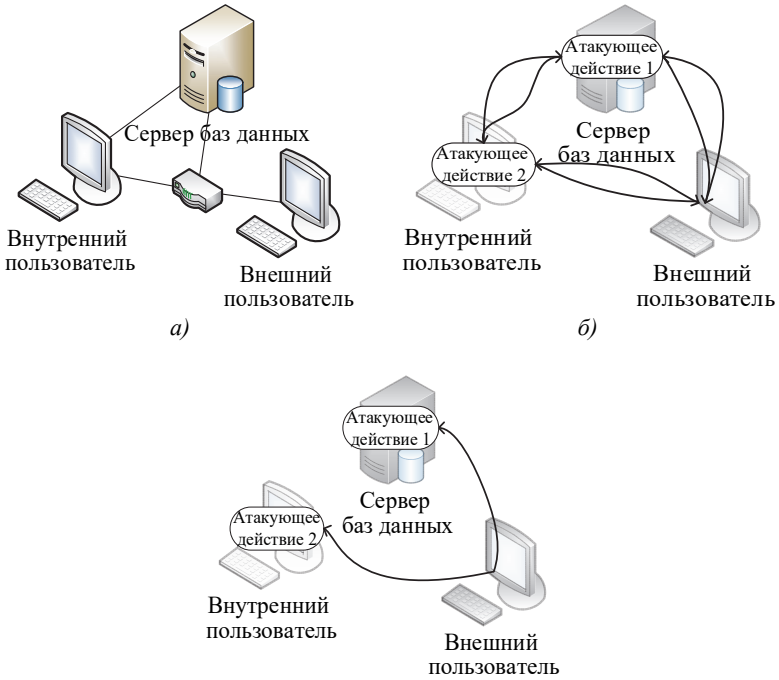

Рис. 4. Пример удаления циклов типа 1 для графа атакующих действий

На рисунке 5а приведен пример фрагмента компьютерной сети, граф атак для которой содержит цикл типа 2. Граф атак, содержащий цикл типа 2, представлен на рисунке 5*б*. При этом предполагается, что циклы типа 1 уже удалены. На рисунке 5*в* представлен граф после обработки цикла.

На рисунке 6а приведен пример фрагмента компьютерной сети, граф атак для которой содержит цикл типа 3. Граф атак, содержащий цикл типа 3, представлен на рисунке 6*б*. При этом предполагается, что циклы типа 1 и 2 уже удалены. На рисунке 6*в* представлен граф после обработки цикла.

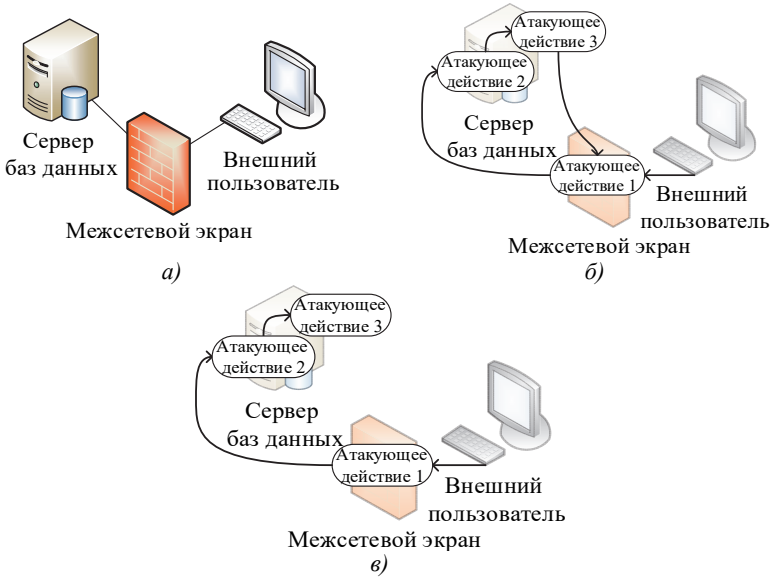

Рис. 5. Пример удаления циклов типа 2 для графа атакующих действий

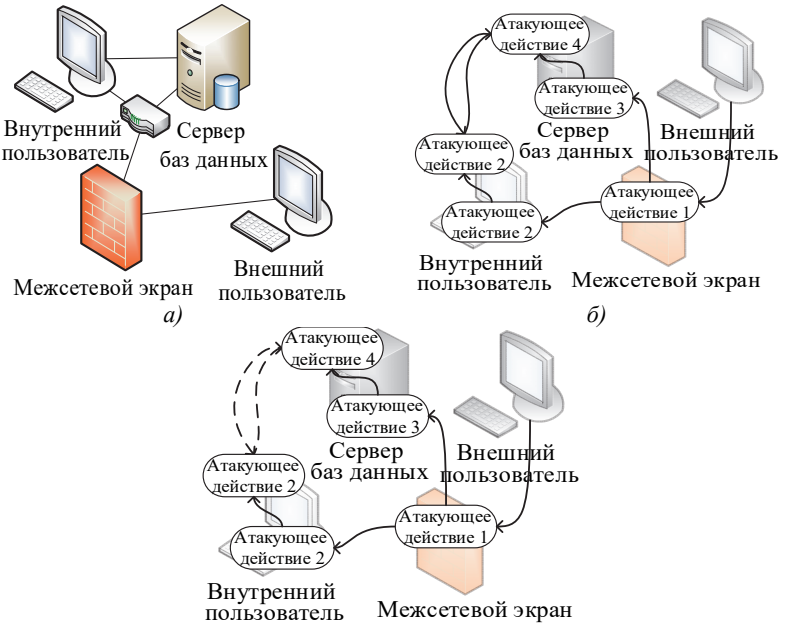

Рис. 6. Пример удаления циклов типа 3 для графа атакующих действий

Данное решение позволяет вычислять вероятность атаки для узлов и путей графа атак и выбирать контрмеры для узлов с неприемлемым уровнем риска, но вводит ограничения на идентификацию пути атакующего на графе атак после возникновения инцидента (некоторые пути графа атак, соответствующие выполненным атакующим действиям, могут быть удалены с графа атак).

3.4. Переопределение модели атак для локализации угроз. Еще одно ограничение исходного графа было выявлено при отображении различных инцидентов безопасности на граф атак для последующего выбора защитных мер. В рамках введенной модели атак под путем атаки понимается последовательность атакующих действий (узлов графа атак). Каждый путь соответствует угрозе для некоторого сетевого актива. Инциденты безопасности отображаются на граф согласно нанесенному ущербу и активу, на который они повлияли. Однако при текущей реализации, когда атакующие действия определены на основе групп (таблица 1 и таблица 2), не учитывающих различные виды ущерба, они могут отображаться сразу на несколько узлов.

С другой стороны, защитные действия ограничиваются добавлением или удалением путей на граф атак (например, закрытие доступа к хосту, удаление уязвимостей) и не учитывают тип угроз. При этом не очевидно, каким образом защитные меры, действующие против нарушения конфиденциальности и целостности, влияют на граф атак.

Поэтому предлагается ввести новое разделение уязвимостей на группы по типам угроз для точного отображения инцидента на узлы графа атак в зависимости от ущерба, нанесенного атакой.

Согласно системе CVSS, выделяются показатели ущерба конфиденциальности (C), целостности (I) и доступности (A). Можно выделить следующие сочетания данных показателей: CIA, C, I, A, CI, CA, IA, и none (нет ущерба). В соответствии с этим каждая группа в таблицах 1 и 2 будет поделена на 8 подгрупп по полю *CIA*.

Для каждого вида ущерба должны быть определены соответствующие защитные меры. Например, в таблице 3 выделены угрозы и возможные контрмеры согласно стандарту ГОСТ Р ИСО/МЭК 27005-2010 [23, 45] (где C обозначает ущерб конфиденциальности, I — ущерб целостности, A — ущерб доступности).

Угрозы и защитные меры определяются индивидуально для каждой сети. Каждый класс защитных мер в таблице 3 включает конкретные меры, имеющиеся в наличии в анализируемой системе для статического режима (т.е. режима проектирования) и динамического режима (т.е. режима эксплуатации) [23].

Таблица 3. Классы угроз и защитные меры

Угрозы	Свойство безопасности	Контрмеры							
		Предохранение от вредоносного кода	Идентификация и аутентификация	Логическое управление и аудит доступа	Управление безопасностью сети	Криптография	Обнаружение и предотвращение вторжений	Резервные копии	Управление персоналом
Злонамеренный код	C	SD					D		
	I	SD					D	SD	
	A	SD					D		
Подмена личности пользователя	C	SD	SD	SD	SD	S			
	I	SD	SD	SD	SD	S		SD	
	A	SD	SD	SD	SD	S		SD	
Ложная маршрутизация/перенаправление сообщений	C				SD	S			
	I				SD	S			
	A				SD	S			
Несанкционированный доступ к компьютерам, данным, сервисам и приложениям	C		SD	SD	SD	S			
	I		SD	SD	SD	S		SD	
	A		SD	SD	SD	S			
Разрушительная атака									
	A		SD	SD				SD	S
Неправильное использование ресурсов									
	A		SD	SD	SD				S
Перегрузка трафика									
	A				SD			SD	

Например, мера «Идентификация и аутентификация» может быть реализована с использованием программного токена в статическом режиме работы системы (обозначение S в таблице 3). В динамическом режиме работы системы (обозначение D в таблице 3), при поступлении информации об инциденте безопасности, соответствующем несанкционированному доступу, программный токен используется для активации многофакторной аутентификации. Контрмеры отображаются на соответствующие свойства безопасности, что позволяет отобразить их на узлы графа атак.

3.5. Оценка защищенности с использованием модифицированного графа атак. Мониторинг кибербезопасности с использованием описанного графа происходит на основе ряда показателей защищенности [22, 23]. Предложенные модификации методики формирования графа атак влияют на процесс оценки защищенности. Переход на CVSS версии 3.0 привел к модификации уравнений вычисления показателей. Обработка циклов графа позволила применить байесовский метод для вычисления показателей вероятности успешной реализации атаки. Однако при этом необходимо выполнить дополнительные действия при вычислении вероятностей, что повысило сложность обработки графа атак. Новое определение групп уязвимостей не повлияло на уравнения для вычисления показателей.

Ниже рассмотрены некоторые показатели защищенности, используемые для мониторинга кибербезопасности и выбора контрмер, на которые повлияли предложенные в предыдущих разделах изменения модели атак, в том числе:

– сложность атакующего действия (вычисляется на основе индекса CVSS *AccessComplexity*);

– ущерб для свойств безопасности от атакующего действия (вычисляется на основе индексов CVSS ущерб конфиденциальности, целостности и доступности);

– ущерб от атакующего действия (с учетом критичности активов);

– вероятность атаки (вычисляется на основе индексов CVSS *AccessVector*, *Authentication* и *AccessComplexity*).

При мониторинге показатель сложности атакующего действия *a* *AttackComplexity*(*a*) используется для определения уровня навыков атакующего. Более точное определение данного показателя ведет в свою очередь к более корректным выводам о навыках атакующего. Переход к CVSS версии 3.0 привел к изменению формулы для вычисления данного показателя. Для CVSS версии 2.0:

$$AttackComplexity(a) = AccessComplexity,$$

где *AccessComplexity* — максимальная сложность эксплуатации уязвимостей группы, соответствующей атакующему действию *a*, согласно CVSS версии 2.0, $AccessComplexity \in \{\text{High}, \text{Medium}, \text{Low}\}$.

Для CVSS версии 3.0 уравнение меняется следующим образом:

$$AttackComplexity(a) = AttackComplexity,$$

где *AttackComplexity* — максимальная сложность атаки для уязвимостей группы, соответствующей атакующему действию *a*, согласно CVSS версии 3.0, $AttackComplexity \in \{\text{High}, \text{Low}\}$.

Ущерб от атакующего действия *a* используется при расчете уровней риска узлов графа атак для выявления слабых мест сети и для последующего выбора защитных мер. Точное определение данного показателя позволяет корректно определить уровень возможных потерь организации в случае успешной атаки. Переход к CVSS версии 3.0 привел к изменению формулы для вычисления данного показателя. При использовании CVSS версии 2.0 показатель определялся следующим образом:

$$AttackImpact(a) = Criticality \times [CI \quad II \quad AI],$$

где *Criticality* — критичность актива, против которого направлено атакующее действие *a*, *CI*, *II*, *AI* — ущерб конфиденциальности, целостности и доступности согласно CVSS версии 2.0 соответственно.

При переходе на CVSS версии 3.0 показатели ущерба CVSS версии 2.0 заменяются на соответствующие индексы CVSS версии 3.0. Качественные значения индексов меняются с {None, Partial, Complete} на {None, Low, High}. Новая шкала интуитивно понятнее. Количественные значения индексов CVSS версии 3.0 немного ниже, чем значения индексов CVSS версии 2.0. Это незначительно уменьшает ущерб, создаваемый эксплуатацией уязвимостей.

Показатель вероятности атаки при мониторинге используется, с одной стороны, для расчета уровня риска, для выявления слабых мест сети и для последующего выбора защитных мер, а с другой стороны, для локализации пути атаки, ее источника и целей. Соответственно, более точное определение данного показателя ведет к более точному определению характеристик атаки и эффективному проактивному выбору защитных мер.

Для вычисления вероятности успешного выполнения атакующего действия (полных вероятностей для узлов графа атак) используется формула определения полной вероятности. При обходе графа в случае наличия циклов третьего типа (рисунок 3в), полная вероятность рассчитывается без учета исходящей дуги (образующей цикл), но с учетом входящей дуги. При этом вероятность связанного узла рассчитывается без учета исходящей дуги, но с учетом входящей дуги.

Для определения дискретных локальных распределений условных вероятностей *Pc* используются формулы из [33]. В случае связей типа «И» между узлами предками (для успешной компрометации узла потомка *S* необходимо, чтобы все узлы предки *Pa*(*S*) были скомпрометированы) применяется уравнение:

$$Pc(S \mid Pa(S)) = \begin{cases} 0, & \exists S \in Pa(S) \mid S = 0 \\ p(S), & \text{иначе} \end{cases}, \quad (1)$$

где $p(S)$ — локальная вероятность, соответствующая узлу *S*.

В случае связей типа «ИЛИ» между узлами предками (для успешной компрометации узла потомка необходимо, чтобы хотя бы один узел предок был скомпрометирован) применяется уравнение:

$$Pc(S \mid Pa(S)) = \begin{cases} 0, & \forall S \in Pa(S) \mid S = 0 \\ p(S), & \text{иначе} \end{cases}. \quad (2)$$

Локальную вероятность $p(S)$ атакующего действия *a*, соответствующую узлу *S*, предлагается определять на основе индексов CVSS. Поэтому формулы вычисления локальной вероятности меняются при переходе на CVSS версии 3.0. При использовании CVSS версии 2.0 этот показатель определялся следующим образом:

$$p(S) = \begin{cases} 2 \times AV \times AC \times Au, & \text{если } S \in S_r \\ 2 \times AC \times Au, & \text{иначе} \end{cases}, \quad (3)$$

где S_r — множество корневых (входных) узлов графа; *AV* — показатель, характеризующий доступ, необходимый для эксплуатации уязвимости по CVSS версии 2.0; *AC* — сложность доступа к уязвимости по CVSS версии 2.0; *Au* — аутентификация, требуемая для эксплуатации уязвимости по CVSS версии 2.0 [22, 23].

При использовании CVSS версии 3.0 указанный показатель предлагается определять на основе CVSS уравнения для показателя эксплуатации уязвимости следующим образом:

$$p(S) = \begin{cases} (8.22 \times AV \times AC \times PR \times UI - 0.2) \times 2.7 / 10, & \text{если } S \in S_r \\ (8.22 \times AC \times PR \times UI - 0.2) \times 2.7 / 10, & \text{иначе} \end{cases}, \quad (4)$$

где коэффициенты введены для нормализации значения вероятности от 0 до 1; *AV* — показатель, характеризующий доступ, необходимый для эксплуатации уязвимости (*AttackVector* по CVSS версии 3.0); *AC* — показатель, характеризующий сложность эксплуатации уязвимости (*AttackComplexity* по CVSS версии 3.0); *PR* — привилегии,

требуемые для эксплуатации уязвимости по CVSS версии 3.0; и *UI* — показатель, определяющий, требуется ли взаимодействие с пользователем для эксплуатации уязвимости по CVSS версии 3.0.

В следующих разделах анализируются результаты применения заданных уравнений.

4. Пример применения, эксперименты и дискуссия. Программный прототип, реализующий предложенный подход к мониторингу кибербезопасности и выбору контрмер, разработан с использованием Java на Microsoft Windows Intel Core i7 ЦПУ и 12 Гб ОЗУ [19, 20, 22, 23].

Для проведения экспериментов прототип был модифицирован с учетом предложенных изменений модели атак и методики анализа. На примере фрагмента тестовой сети рассмотрим результаты предложенных изменений (рисунок 7).

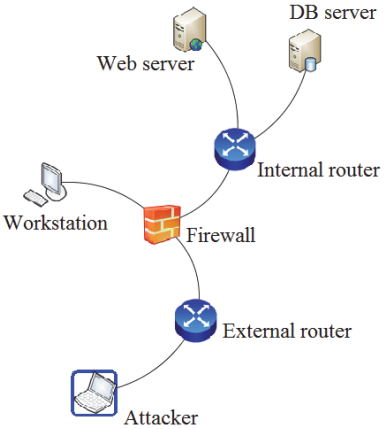

Рис. 7. Фрагмент тестовой сети

Фрагмент тестовой сети содержит:

– веб сервер *Web server* (с Windows Server 2008 R2 SP1 (64 бит), JBoss AS 5.0.1, ApacheStruts2 framework);

– сервер баз данных *DB server* (с Windows Server 2008 R2 (64 бит), Microsoft SQL Server 2008 R2 (64 бит), CA Spectrum 9.2, EMC Unisphere for VMAX 8.1);

– межсетевой экран *Firewall* (с Novell SUSE Linux Enterprise Server 11.0 SP3 Long Term Service Pack Support, Netfilter);

– рабочую станцию *Workstation* (с Microsoft Windows 7 64-bit, Apple ITunes 9.0.3, Microsoft Office 2007 SP1, Microsoft Internet Explorer 7).

На рисунке 7 представлены связи между объектами сети (на сетевом уровне).

Итоговый ациклический граф, сгенерированный с использованием CVSS версии 2.0, представлен на рисунке 8.

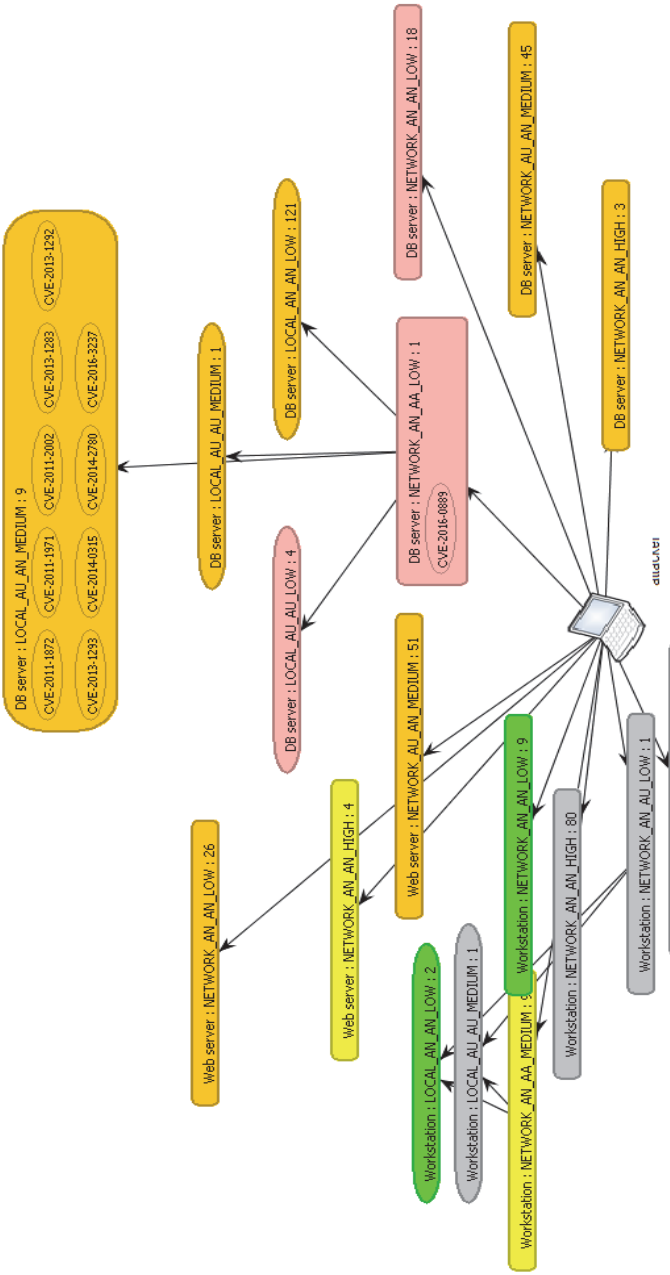

Рис. 8. Исходный граф атак для фрагмента тестовой сети

Узлы графа в рамках программного прототипа раскрашены в соответствии с уровнем риска:

- зеленый цвет — низкий уровень риска;
- желтый цвет — средний уровень риска;
- оранжевый цвет — высокий уровень риска;
- красный цвет — критичный уровень риска.

Каждый узел, соответствующий группе уязвимостей CVSS версии 2.0 обозначается с использованием показателей CVSS версии 2.0 в следующем формате:

“Host_name : AccessVector_Authentication_ GainedPrivileges_
AccessComplexity : number_of_vulnerabilities”,

где Host_name — имя хоста; AccessVector — показатель, характеризующий доступ, необходимый для эксплуатации уязвимости по CVSS версии 2.0; Authentication — аутентификация, требуемая для эксплуатации уязвимости по CVSS версии 2.0; GainedPrivileges — привилегии, полученные в результате эксплуатации уязвимости; AccessComplexity — показатель, характеризующий сложность эксплуатации уязвимости по CVSS версии 2.0; number_of_vulnerabilities — количество уязвимостей в группе.

Каждый узел содержит уязвимости соответствующей группы.

Граф атак с учетом модификаций в результате применения CVSS версии 3.0 представлен на рисунке 9.

Уязвимости, перемещенные в другие группы, определенные с использованием CVSS версии 3.0, выделены красными прямоугольниками. Красные стрелки, идущие от прямоугольников, показывают перемещение уязвимостей в новые группы. Каждый узел, соответствующей группе, выделенной с использованием CVSS версии 3.0, обозначается следующим образом:

“Host_name : AttackVector_PrivilegesRequired_
GainedPrivileges_AttackComplexity”,

где Host_name — имя хоста; AttackVector — показатель, характеризующий доступ, необходимый для эксплуатации уязвимости по CVSS версии 3.0; PrivilegesRequired — привилегии, требуемые для эксплуатации уязвимости по CVSS версии 3.0; GainedPrivileges — привилегии, полученные в результате эксплуатации уязвимости; AttackComplexity — сложность эксплуатации уязвимости по CVSS версии 3.0.

Поскольку в настоящий момент открытые базы уязвимостей содержат оценки CVSS версии 3.0 не для всех уязвимостей, полностью перейти на CVSS версии 3.0 невозможно. Поэтому в рамках прототипа две системы оценки используются совместно.

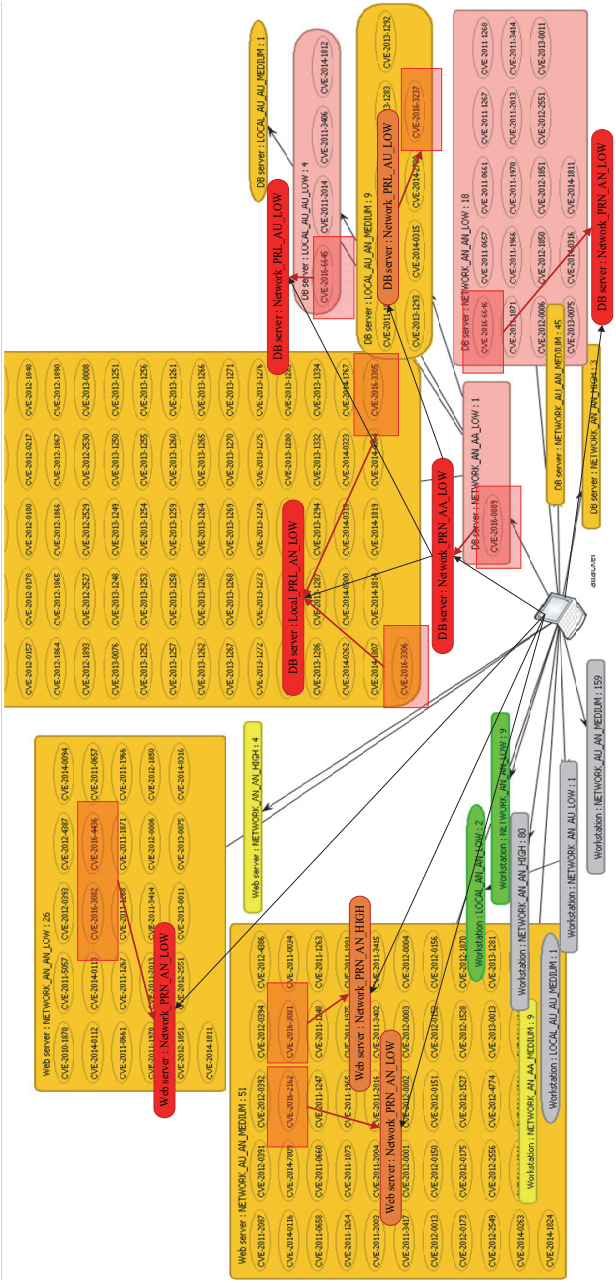

Рис. 9. Граф атак с учетом модификаций в результате применения CVSS версии 3.0

Из рисунка 9 видно, что структура графа в целом совпадает со структурой исходного графа (рисунок 8), за исключением новых узлов, соответствующих уязвимостям, оцененным с использованием CVSS версии 3.0. Большинство групп CVSS версии 3.0 имеют тот же уровень риска, что и соответствующие группы CVSS версии 2.0 (из которых уязвимости были перемещены). Но для хоста «Web server» есть две уязвимости, изменившие свои оценки риска с «Высокий» на «Критичный», то есть общий уровень риска для данного хоста вырос. Таким образом, новые оценки могут значительно изменить распределение уровней риска в компьютерных сетях. Для анализа возможных изменений продолжаются эксперименты с различными сетевыми топологиями. Другие эксперименты были проведены для оценки выбора контрмер с использованием новых групп, сгенерированных с учетом различных видов ущерба.

Все еще остается ряд аспектов, которые необходимо исследовать, например: сложность анализа графа атак; некоторые показатели CVSS, которые все еще не учитываются при оценке (“User Interaction” и “Scope”); дальнейшее развитие модели атак с применением шаблонов атак и показателей CAPEC. Их планируется исследовать в будущем.

5. Заключение. В работе рассмотрены вопросы модификации процесса генерации модели атак и методики его анализа для более адекватного мониторинга кибербезопасности и выбора защитных мер. Выделены существующие ограничения, в том числе неточность графа атакующих действий, обусловленная неоднозначностью индексов CVSS, лежащих в его основе, отсутствием учета атак, не использующих уязвимости, пренебрежением циклическими связями на графе, а также допущения при определении ущерба от атак вследствие неоднозначного определения области воздействия атаки. Приведены предложения по устранению указанных ограничений за счет использования новой спецификации CVSS версии 3.0, использования шаблонов атак CAPEC и обработки циклических связей графа. Проведен анализ влияния введенных изменений на результаты анализа защищенности, показавший изменение распределения уровней риска в тестовой компьютерной сети.

Изменения реализованы в рамках ранее разработанного программного прототипа для проведения экспериментов. На примере показано влияние предложенных изменений на результаты оценки защищенности. Кратко описаны проведенные эксперименты, показавшие качественное улучшение процессов оценки защищенности и выбора контрмер с точки зрения корректности прогнозирования атак и рациональности выбора контрмер.

В будущем планируется дополнительно провести ряд экспериментов для тщательной проверки адекватности предложенной модели и получения количественных оценок улучшения процессов оценки защищенности и выбора контрмер, развить модель атак с учетом сложности анализа графа атак, проанализировать еще неучтенные показатели системы CVSS, а также показатели и шаблоны атак CAPEC.

Литература

1. *Котенко И.В., Саенко И.Б.* Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. 2012. Вып. 3(22). С. 84–100.
2. *Котенко И.В., Саенко И.Б.* Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2013. Вып. 1(24). С. 21–40.
3. *Artz M.* NetSPA, a network security planning architecture. Master's thesis // Massachusetts Institute of Technology. 2002. 96 p.
4. *Lippmann R.P. et al.* Validating and restoring defense in depth using attack graphs // Proceedings of the 2007 IEEE Military Communications Conference. 2006. pp. 1–10.
5. *Ingols K., Lippmann R., Piwowarski K.* Practical attack graph generation for network defense // Proceedings of the 22nd Annual Conference on the Computer Security Applications. 2006. pp. 121–130.
6. *Singhal A., Ou X.* Security risk analysis of enterprise networks using probabilistic attack graphs // Network Security Metrics. 2017. pp. 53–73.
7. *Abraham S., Nair S.* A predictive framework for cyber security analytics using attack graphs // International Journal of Computer Networks & Communications (IJCNC). 2015. vol. 7. no.1. pp. 1–17.
8. *Janse van Rensburg A., Nurse J.R.C., Goldsmith M.* Attacker-Parametrised Attack Graphs // Proceedings of the Tenth International Conference on Emerging Security Information, Systems and Technologies. 2016. pp. 316–319.
9. *Kordy B., Pièvre-Cambacédès L., Schweitzer P.* DAG-based attack and defense modeling: don't miss the forest for the attack trees // Computer Science Review. 2014. vol. 13–14. pp. 1–38. URL: http: // www.sciencedirect.com/science/article/pii/S1574013714000100 (дата обращения: 17.07.2017).
10. *Shandilya V., Simmons C.B., Shiva S.* Use of attack graphs in security systems // Journal of Computer Networks and Communications. 2014. vol. 2014. 13 p. URL: http: // dx.doi.org/10.1155/2014/818957 (дата обращения: 17.07.2017).
11. *Muñoz-González L., Sgandurra D., Barrère M., Lupu E.C.* Exact inference techniques for the analysis of Bayesian attack graphs // IEEE Transactions on Dependable and Secure Computing. 2017. pp. 1–14.
12. *Noel S., Jajodia S.* Metrics suite for network attack graph analytics // Proceedings of the 9th Cyber and Information Security Research Conference. 2014. pp. 5–8.
13. *Alhomidi M., Reed M.* Attack graph-based risk assessment and optimisation approach // International Journal of Network Security & Its Applications (IJNSA). 2014. vol. 6. no. 3. pp. 31–43.
14. *Durkota K., Lisy V., Bošansky B., Kiekintveld C.* Optimal network security hardening using attack graph games // Proceedings of the Twenty-Fourth International Joint Conference on Artificial Intelligence. 2015. pp. 526–532.
15. *Sembiring J., Ramadhan M., Gondokaryono Y.S., Arman A.A.* Network security risk analysis using improved MulVAL Bayesian attack graphs // International Journal on Electrical Engineering and Informatics. 2015. vol. 7. no. 4. pp. 735–753.

16. *Muñoz-Gonzalez L., Sgandurra D., Paudice A., Lupu E.C.* Efficient attack graph analysis through approximate inference // ACM Transactions on Privacy and Security. 2017. vol. 20. no. 3. 30 p.
17. *Bhattacharya P. Ghosh S.K.* Analytical framework for measuring network security using exploit dependency graph // IET Information Security. 2012. vol. 6. no. 4. pp. 264–270.
18. *Almohri H.M.J., Watson L.T., Yao D., Ou X.* Security optimization of dynamic networks with probabilistic graph modeling and linear programming // IEEE Transactions on Dependable and Secure Computing. 2016. vol. 13. no. 4. pp. 474–487.
19. *Kotenko I., Stepashkin M.* Attack graph based evaluation of network security // Proceedings of the Communications and Multimedia Security (CMS 2006). 2006. LNCS 4237. pp. 216–227.
20. *Kotenko I., Chechulin A.* Attack Modeling and Security Evaluation in SIEM Systems // International Transactions on Systems Science and Applications. 2012. vol. 8. pp. 129–147.
21. *Mell P., Scarforne K., Romanosky S.* A Complete Guide to the Common Vulnerability Scoring System (CVSS) Version 2.0. 2007. URL: https://www.first.org/cvss/v2/guide (дата обращения: 17.07.2017).
22. *Kotenko I., Doynikova E.* Dynamical calculation of security metrics for countermeasure selection in computer networks // Proceedings of the 24th Euromicro International Conference on Parallel, Distributed and network-based Processing. 2016. pp. 558–565.
23. *Doynikova E., Kotenko I.* Countermeasure selection based on the attack and service dependency graphs for security incident management // Proceedings of the 10th International Conference on Risks and Security of Internet and Systems. 2016. LNCS 9572. pp. 107–124.
24. FIRST Org. Inc, Common Vulnerability Scoring System v3.0: Specification Document. 2015. URL: https://www.first.org/cvss/specification-document (дата обращения: 17.07.2017).
25. *Barnum S.* Common Attack Pattern Enumeration and Classification (CAPEC). Schema Description. 2008. 26 p.
26. Positive Technologies web site. URL: https:/www.ptsecurity.com/ww-en (дата обращения: 17.07.2017).
27. *Lorenzo J.M.* Alienvault users manual. Version 1.0. Alienvault LC. 2011. 225 p.
28. CORDIS website. URL: http://cordis.europa.eu/project/rcn/95310_en.html (дата обращения: 17.07.2017).
29. *Man D. et al.* A quantitative evaluation model for network security // Proceedings of the 2007 Intern. Conference on Computational Intelligence and Security. 2007. pp. 773–777.
30. *Wu Y.-S. et al.* Automated adaptive intrusion containment in systems of interacting services // Computer Networks: The International Journal of Computer and Telecommunications Networking. 2007. vol. 51. pp. 1334–1360.
31. *Stakhanova N., Basu S., Wong J.* A cost-sensitive model for preemptive intrusion response systems // Proceedings of the 21st International Conference on Advanced Networking and Applications. 2007. pp. 1–8.
32. *Liu Y., Man H.* Network vulnerability assessment using Bayesian networks // SPIE. 2005. vol. 5812. pp. 61–71.
33. *Frigault M., Wang L., Singhal A., Jajodia S.* Measuring network security using dynamic Bayesian network // Proceedings of the ACM Workshop on Quality of Protection. 2008. pp. 23–30.
34. *Dantu R., Kolan P., Cangussu J.* Network risk management using attacker profiling // Security and Communication Networks. 2009. vol. 2. no. 1. pp. 83–96.
35. *Wang L. et al.* An attack graph-based probabilistic security metric // Proceedings of the 22nd annual IFIP WG 11.3 working conference on Data and Applications Security. 2008. pp. 283–296.
36. *Poolsappasit N., Dewri R., Ray I.* Dynamic security risk management using Bayesian attack graphs // Proceedings of the IEEE Transactions on Dependable and Security Computing. 2012. vol. 9. no. 1. pp. 61–74.

37. *Dacier M., Deswarte Y., Kaâniche M.* Quantitative assessment of operational security: Models and tools // Information Systems Security. 1996. pp. 179–86.
38. CyVision website. CAULDRON tool. URL: https://www.benvenisti.net/cauldron/ (дата обращения: 17.07.2017).
39. SecurITree. Amenaza Technologies Limited. URL: http://www.amenaza.com (дата обращения: 17.07.2017).
40. Common Platform Enumeration (CPE). NVD website. URL: https://nvd.nist.gov/cpe.cfm (дата обращения: 17.07.2017).
41. Common Configuration Enumeration (CCE). NVD website. URL: https://nvd.nist.gov/cce/index.cfm (дата обращения: 17.07.2017).
42. NVD website. URL: https://nvd.nist.gov (дата обращения: 17.07.2017).
43. Common Weakness Enumeration (CWE). MITRE website. URL: https://cwe.mitre.org/ (дата обращения: 15.08.2017).
44. *Wu Y., Yesha Y., Bojanova I.* They Know Your Weaknesses – Do You?: Reintroducing Common Weakness Enumeration // CrossTalk: The Journal of Defense Software Engineering. 2016. vol. 29. no. 3. pp. 19–24.
45. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности // М.: Стандартинформ. 2011. 47 с.

Дойникова Елена Владимировна — научный сотрудник лаборатории проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), научный сотрудник международной лаборатории информационной безопасности киберфизических систем, ФГАОУ ВО "Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики" (Университет ИТМО). Область научных интересов: безопасность компьютерных сетей, методы анализа рисков компьютерных сетей, управление информационными рисками. Число научных публикаций — 71. elenadoynikova@mail.ru; 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ; р.т.: +7(812)328-7181, Факс: +7(812)328-4450.

Котенко Игорь Витальевич — д-р техн. наук, профессор, заведующий лабораторией проблем компьютерной безопасности, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН), руководитель международной лаборатории информационной безопасности киберфизических систем, ФГАОУ ВО "Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики" (Университет ИТМО). Область научных интересов: безопасность компьютерных сетей, в том числе управление политиками безопасности, разграничение доступа, аутентификация, анализ защищенности, обнаружение компьютерных атак, межсетевые экраны, защита от вирусов и сетевых червей, анализ и верификация протоколов безопасности и систем защиты информации, защита программного обеспечения от взлома и управление цифровыми правами, технологии моделирования и визуализации для противодействия кибер–терроризму. Число научных публикаций — 500. ivkote@comsec.spb.ru, http://www.comsec.spb.ru; 14-я линия В.О., 39, Санкт-Петербург, 199178; р.т.: +7-(812)328-7181, Факс: +7(812)328–4450.

Поддержка исследований. Работа выполнена при финансовой поддержке РФФИ (проекты 16-37-00338, 16-29-09482 и 18-07-01488), гранта Президента РФ № МК-314.2017.9, стипендии Президента РФ № СП-751.2018.5, при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007, а также при государственной финансовой поддержке ведущих университетов Российской Федерации (субсидия 074-U01).

DOI 10.15622/sp.57.9

E.V. DOYNIKOVA, I.V. KOTENKO

IMPROVEMENT OF ATTACK GRAPHS FOR CYBERSECURITY MONITORING: HANDLING OF INACCURACIES, PROCESSING OF CYCLES, MAPPING OF INCIDENTS AND AUTOMATIC COUNTERMEASURE SELECTION

Doynikova E.V., Kotenko I.V. **Improvement of Attack Graphs for Cybersecurity Monitoring: Handling of Inaccuracies, Processing of Cycles, Mapping of Incidents and Automatic Countermeasure Selection.**

Abstract. Both timely and adequate response on the computer security incidents and organization losses from the computer attacks depend on the accuracy of situation recognition under the cybersecurity monitoring. The paper is devoted to the enhancement of the attack models in the form of attack graphs for the cybersecurity monitoring tasks. A number of important issues related to the application of attack graphs and their solutions are considered. They include inaccuracies in the definition of the pre- and post-conditions of attack actions, the processing of attack graph cycles for the application of Bayesian inference for the attack graph analysis, the mapping of security incidents on an attack graph, the automatic countermeasure selection in case of a high security risk level. The paper demonstrates a software prototype of the security monitoring system component which was earlier implemented and modified considering the suggested enhancements. The results of experiments are described. The influence of the modifications on the cybersecurity monitoring results is shown on a case study.

Keywords: attack graph, attack probability, cybersecurity monitoring, computer networks, security assessment, security metrics, attack response, vulnerability assessment.

Doynikova Elena Vladimirovna — researcher of computer security problems laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS), researcher of information security of cyber-physical systems international laboratory , ITMO University (Saint Petersburg National Research University of Information Technologies, Mechanics and Optics). Research interests: computer network security, risk analysis methods for computer networks, information security risk management. The number of publications — 71. elenadoynikova@mail.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7(812)328-7181, Fax: +7(812)328-4450.

Kotenko Igor Vitalievich — Ph.D., Dr. Sci., professor, head of computer security problems laboratory, St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS), head of information security of cyber-physical systems international laboratory , ITMO University (Saint Petersburg National Research University of Information Technologies, Mechanics and Optics). Research interests: computer network security, including security policy management, access control, authentication, network security analysis, intrusion detection, firewalls, deception systems, malware protection, verification of security systems, digital right management, modeling, simulation and visualization technologies for counteraction to cyber terrorism. The number of publications — 500. ivkote@comsec.spb.ru, http://www.comsec.spb.ru; 39, 14-th Line V.O., St. Petersburg, 199178, Russia; office phone: +7-(812)328-7181, Fax: +7(812)328–4450.

Acknowledgements. This research is supported by RFBR (projects No. 16-37-00338, 16-29-09482 and 18-07-01488), Grants of the President of the Russian Federation No. MK-314.2017.9, SP-751.2018.5, by the budget (projects No. 0073-2015-0004 and 0073-2015-0007), and by Government of the Russian Federation, Grant 074-U01.

References

1. Kotenko I.V., Saenko I.B. [Developing the system of intelligent services to protect information in cyber warfare]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2012. vol. 3(22). pp. 84–100. (In Russ.).

2. Kotenko I.V., Saenko I.B. [Architecture of the system of intelligent services to protect information in cyber warfare]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2013. vol. 1(24). pp. 21–40. (In Russ.).
3. Artz M. NetSPA, a network security planning architecture. Master's thesis. Massachusetts Institute of Technology. 2002. 96 p.
4. Lippmann R.P. et al. Validating and restoring defense in depth using attack graphs. Proceedings of the 2007 IEEE Military Communications Conference. 2006. pp. 1–10.
5. Ingols K., Lippmann R., Piwowarski K. Practical attack graph generation for network defense. Proceedings of the 22nd Annual Conference on the Computer Security Applications. 2006. pp. 121–130.
6. Singhal A., Ou X. Security risk analysis of enterprise networks using probabilistic attack graphs. Network Security Metrics. 2017. pp. 53–73.
7. Abraham S., Nair S. A predictive framework for cyber security analytics using attack graphs. *International Journal of Computer Networks & Communications (IJCNC)*. 2015. vol. 7. no.1. pp. 1–17.
8. Janse van Rensburg A., Nurse J.R.C., Goldsmith M. Attacker-Parametrised Attack Graphs. Proceedings of the Tenth International Conference on Emerging Security Information, Systems and Technologies. 2016. pp. 316–319.
9. Kordy B., Pièrre-Cambacédès L., Schweitzer P. DAG-based attack and defense modeling: don't miss the forest for the attack trees. Computer Science Review. 2014. vol. 13–14. pp. 1–38. Available at: http: // www.sciencedirect.com/science/article/pii/S1574013714000100 (access: 17.07.2017).
10. Shandilya V., Simmons C.B., Shiva S. Use of attack graphs in security systems. Journal of Computer Networks and Communications. 2014. vol. 2014. 13 p. Available at: http://dx.doi.org/10.1155/2014/818957 (access: 17.07.2017).
11. Muñoz-González L., Sgandurra D., Barrère M., Lupu E.C. Exact inference techniques for the analysis of Bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*. 2017. pp. 1–14.
12. Noel S., Jajodia S. Metrics suite for network attack graph analytics. Proceedings of the 9th Cyber and Information Security Research Conference. 2014. pp. 5–8.
13. Alhomidi M., Reed M. Attack graph-based risk assessment and optimisation approach. *International Journal of Network Security & Its Applications (IJNSA)*. 2014. vol. 6. no. 3. pp. 31–43.
14. Durkota K., Lisy V., Bošansky B., Kiekintveld C. Optimal network security hardening using attack graph games. Proceedings of the Twenty-Fourth International Joint Conference on Artificial Intelligence. 2015. pp. 526–532.
15. Sembiring J., Ramadhan M., Gondokaryono Y.S., Arman A.A. Network security risk analysis using improved MulVAL Bayesian attack graphs. *International Journal on Electrical Engineering and Informatics*. 2015. vol. 7. no. 4. pp. 735–753.
16. Muñoz-Gonzalez L., Sgandurra D., Paudice A., Lupu E.C. Efficient attack graph analysis through approximate inference. *ACM Transactions on Privacy and Security*. 2017. vol. 20. no. 3. 30 p.
17. Bhattacharya P. Ghosh S.K. Analytical framework for measuring network security using exploit dependency graph. IET Information Security. 2012. vol. 6. no. 4. pp. 264–270.
18. Almohri H.M.J., Watson L.T., Yao D., Ou X. Security optimization of dynamic networks with probabilistic graph modeling and linear programming. *IEEE Transactions on Dependable and Secure Computing*. 2016. vol. 13. no. 4. pp. 474–487.
19. Kotenko I., Stepashkin M. Attack graph based evaluation of network security. Proceedings of the Communications and Multimedia Security (CMS 2006). 2006. LNCS 4237. pp. 216–227
20. Kotenko I., Chechulin A. Attack Modeling and Security Evaluation in SIEM Systems. *International Transactions on Systems Science and Applications*. 2012. vol. 8. pp. 129–147.
21. Mell P., Scarforne K., Romanosky S. A Complete Guide to the Common Vulnerability Scoring System (CVSS) Version 2.0. 2007. Available at: https://www.first.org/cvss/v2/guide (accessed: 17.07.2017).

22. Kotenko I., Doynikova E. Dynamical calculation of security metrics for countermeasure selection in computer networks. Proceedings of the 24th Euromicro International Conference on Parallel, Distributed and network-based Processing. 2016. pp. 558–565.
23. Doynikova E., Kotenko I. Countermeasure selection based on the attack and service dependency graphs for security incident management. Proceedings of the 10th International Conference on Risks and Security of Internet and Systems. 2016. LNCS 9572. pp. 107–124.
24. FIRST Org. Inc, Common Vulnerability Scoring System v3.0: Specification Document. 2015. Available at: https://www.first.org/cvss/specification-document (accessed: 17.07.2017).
25. Barnum S. Common Attack Pattern Enumeration and Classification (CAPEC). Schema Description. 2008. 26 p.
26. Positive Technologies web site. Available at: https:/www.ptsecurity.com/ww-en (accessed: 17.07.2017).
27. Lorenzo J.M. Alienvault users manual. Version 1.0. Alienvault LC. 2011. 225 p.
28. CORDIS website. Available at: http://cordis.europa.eu/project/rcn/95310_en.html (accessed: 17.07.2017).
29. Man D. et al. A quantitative evaluation model for network security. Proceedings of the 2007 Intern. Conference on Computational Intelligence and Security. 2007. pp. 773–777.
30. Wu Y.-S. et al. Automated adaptive intrusion containment in systems of interacting services. Computer Networks: *The International Journal of Computer and Telecommunications Networking*. 2007. vol. 51. pp. 1334–1360.
31. Stakhanova N., Basu S., Wong J. A cost-sensitive model for preemptive intrusion response systems. Proceedings of the 21st International Conference on Advanced Networking and Applications. 2007. pp. 1–8.
32. Liu Y., Man H. Network vulnerability assessment using Bayesian networks. SPIE. 2005. vol. 5812. pp. 61–71.
33. Frigault M., Wang L., Singhal A., Jajodia S. Measuring network security using dynamic Bayesian network. Proceedings of the ACM Workshop on Quality of Protection. 2008. pp. 23–30.
34. Dantu R., Kolan P., Cangussu J. Network risk management using attacker profiling. Security and Communication Networks. 2009. vol. 2. no. 1. pp. 83–96.
35. Wang L. et al. An attack graph-based probabilistic security metric. Proceedings of the 22nd annual IFIP WG 11.3 working conference on Data and Applications Security. 2008. pp. 283–296.
36. Poolsappasit N., Dewri R., Ray I. Dynamic security risk management using Bayesian attack graphs. Proceedings of the IEEE Transactions on Dependable and Security Computing. 2012. vol. 9. no. 1. pp. 61–74.
37. Dacier M., Deswarte Y. et al. Quantitative Assessment of Operational Security: Models and Tools. *Information Systems Security*. 1996. pp. 179–86.
38. CyVision website. CAULDRON tool. Available at: https://www.benvenisti.net/cauldron/ (accessed: 17.07.2017).
39. SecurITree. Amenaza Technologies Limited. Available at: http://www.amenaza.com (accessed: 17.07.2017).
40. Common Platform Enumeration (CPE). NVD website. Available at: https://nvd.nist.gov/cpe.cfm (accessed: 17.07.2017).
41. Common Configuration Enumeration (CCE). NVD website. Available at: https://nvd.nist.gov/cce/index.cfm (accessed: 17.07.2017).
42. NVD website. Available at: https://nvd.nist.gov (accessed 17.07.2017).
43. Common Weakness Enumeration (CWE). MITRE website. Available at: https://cwe.mitre.org/ (accessed: 15.08.2017).
44. Wu Y., Yesha Y., Bojanova I. They Know Your Weaknesses – Do You?: Reintroducing Common Weakness Enumeration. *CrossTalk: The Journal of Defense Software Engineering*. 2016. vol. 29. no. 3. pp. 19 –24.
45. *GOST R ISO/IEC 27005-2010* [Information technology. Security techniques. Information security risk management]. M.: Standartinform. 2011. 47 p. (In Russ.).