УДК 004.056
doi:10.15217/issn1684-8853.2016.5.54

МЕТОДИКИ И ПРОГРАММНЫЙ КОМПОНЕНТ ОЦЕНКИ РИСКОВ НА ОСНОВЕ ГРАФОВ АТАК ДЛЯ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ

Е. В. Дойникова[a], *научный сотрудник*
И. В. Котенко[a], *доктор техн. наук, профессор*
[a]*Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербург, РФ*

Постановка проблемы: *тема реагирования на компьютерные атаки остается актуальной, так как количество компьютерных угроз год от года не уменьшается, информационные технологии применяются повсеместно, а сложность и размер сетевых инфраструктур растет. Соответственно, растет и необходимость в усовершенствовании механизмов оценки защищенности и выбора мер реагирования. Для адекватного реагирования на атаки необходим грамотный всесторонний анализ рисков системы, дающий значимую и реально отражающую ситуацию по защищенности оценку. Хотя исследователями были предложены различные подходы, универсального решения найти не удалось.* ***Цель:*** *разработка методик оценки риска, адекватно отражающих текущую ситуацию по защищенности на основе автоматизированной обработки доступных данных по безопасности; разработка реализующего их программного средства; оценка эффективности методик на основе экспериментов.* ***Результаты:*** *разработаны и реализованы в рамках программного средства методики оценки рисков, основанные на ранее предложенной авторами комплексной системе показателей защищенности. Уточнены некоторые аспекты вычисления показателей для оценки рисков, отличающие предложенные методики от аналогичных работ. Выбор методики в программном компоненте осуществляется в зависимости от текущей ситуации и требований пользователя программного средства. Для проверки результатов работы методик проведены эксперименты. На основе экспериментов выделены достоинства и недостатки предложенных методик.* ***Практическая значимость:*** *разработанные методики и программный компонент позволят повысить защищенность информационных систем за счет предоставления значимой и адекватной оценки защищенности системы.*

Ключевые слова *— методика оценки рисков, показатели защищенности, граф атак, граф зависимостей сервисов, инциденты безопасности.*

Введение

Вопросы оценки рисков компьютерных сетей широко рассмотрены в литературе, в том числе в отечественных и международных стандартах [1–4], корпоративных стандартах [5, 6] и множестве исследовательских работ [7–12]. Популярность данной тематики не снижается, так как количество компьютерных угроз год от года растет, соответственно, растет и необходимость в усовершенствовании механизмов оценки защищенности.

Для адекватного реагирования на атаки необходим грамотный всесторонний анализ рисков системы, дающий значимую и реально отражающую ситуацию по защищенности оценку. Исследователями были предложены различные подходы, в том числе к определению риска на основе вероятностей атак [7, 8] и возможного ущерба от атак [9, 10]; основанные на определении поверхности атаки [11]; учитывающие возможные финансовые потери [12].

В процессе изучения данной темы авторами был предложен подход, объединяющий модели, методики и алгоритмы вычисления показателей [13]. Данному подходу присущи следующие особенности: унификация представления входных данных на основе открытых стандартов для автоматизации процесса; совместный учет характеристик различных объектов оценки (программно-аппаратного обеспечения, уязвимостей, атак, атакующего, инцидентов безопасности и контрмер) для более точной оценки ситуации по защищенности; применение графов зависимости сервисов и байесовских графов атак для вычисления показателей; иерархическое деление показателей на группы, позволяющее получать оценку на основе минимального количества данных.

В работе [13] рассматривались модели и методики вычисления показателей защищенности, применяемые для выбора контрмер. В настоящей статье описывается программный компонент оценки защищенности, реализующий интегрированный комплекс методик оценки рисков. Компонент позволяет гибко выбирать методику в зависимости от текущей ситуации и требований пользователя программного средства. Также в исследовании рассматриваются некоторые аспекты вычисления показателей для оценки рисков, отличающие его от аналогичных работ. Описывается архитектура прототипа программного средства и элементы интерфейса. На экспериментах показана реализация методик в программном средстве, резуль-

таты их работы, выделены достоинства и недостатки.

Таким образом, основной вклад данной работы состоит в сведении ряда показателей защищенности в полноценные методики оценки рисков, демонстрации результатов работы реализующего их программного средства и оценке соответствия методик заявленным требованиям на основе экспериментов.

Методики оценки риска

В зависимости от применяемых для определения уровня риска входных данных и показателей защищенности и в соответствии с традиционным делением методик оценки рисков выделяются методики статической (включая базовую и детальную) и динамической оценки риска.

Входными данными методик оценки риска являются модель компьютерной сети (КС) и модель атак; показатели защищенности разных уровней (топологического, графа атак, атакующего и инцидентов), выделенных в зависимости от применяемых входных данных [13].

Общая схема методик в рамках процесса оценки защищенности представлена на рис. 1. Методики включают следующие этапы:

1) сбор входных данных: компонент оценки риска получает данные от компонента обработки входных данных и компонента вычисления показателей;

2) определение методики вычислений: в зависимости от получаемых входных данных выбирается методика определения уровня риска;

3) вычисление значения риска и получение оценки защищенности.

Выходными данными работы методик являются значения риска для объектов сети и оценка защищенности.

Базовая статическая методика оценки риска

Простым и очевидным решением для верхнеуровневой оценки риска является применение оценок CVSS для уязвимостей [14].

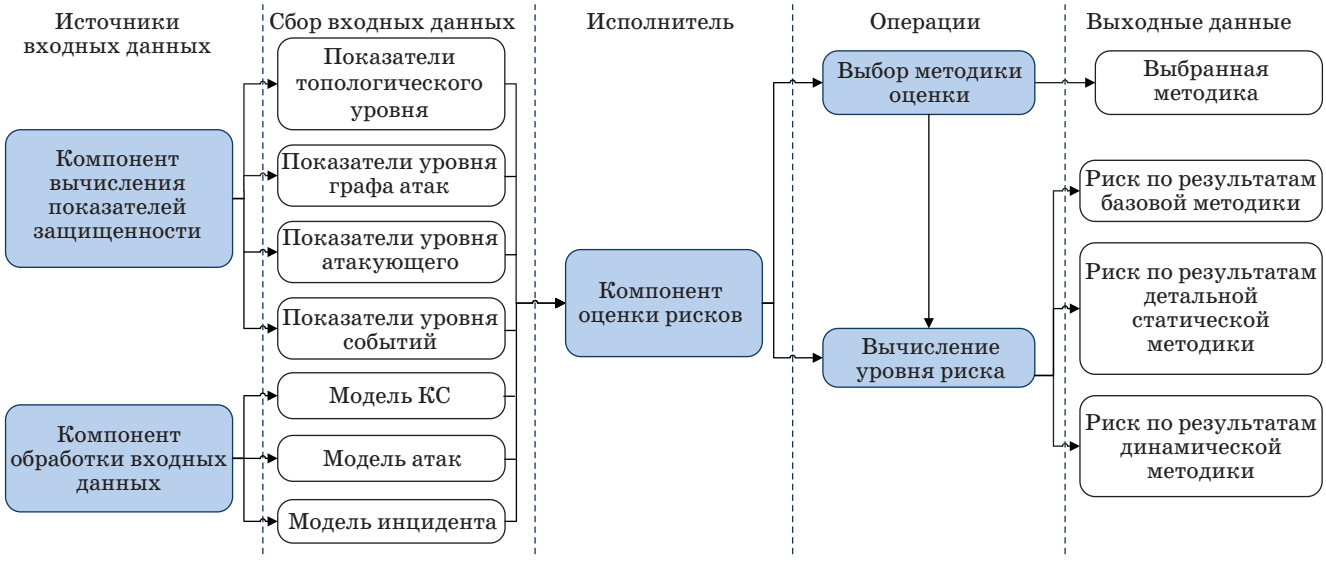
Уровень риска предлагается определять на основе модифицированного контекстного уравнения CVSS, так как оно позволяет учитывать связь между оценкой уязвимости и критичностью активов. Для учета критичности активов воспользуемся показателем CVSS *SecurityRequirements* (требования безопасности). Данный показатель может принимать три значения (0,5; 1,0; 1,51) и устанавливается вручную для каждой системы. Заменим его показателем *Criticality*, который определяет ценность актива для организации. Показатель вычисляется с учетом финансовой ценности активов и зависимостей между свойствами безопасности активов. Шкала возможных значений показателя: 0 – 100 ([0:0,01) — ничтожно малая; [0,01:0,1) — малая; [0,1:1) — значительная; [1:10) — повреждающая; [10:100) — серьезная; 100 — смертельная). Преобразование шкалы для применения в уравнении оценки риска приведено в табл. 1.

Контекстное уравнение CVSS

$$Risk = \text{round\_to\_1\_decimal}(AdjustedBase)$$

в раскрытом виде выглядит следующим образом:

$$Risk = \text{round\_to\_1\_decimal}(((0{,}6 \times AdjustedImpact) + (0{,}4 \times Exploitability) - 1{,}5) \times f(AdjustedImpact)).$$



■ ***Рис. 1.*** Общая схема методик определения уровня риска

■ ***Таблица 1***. Преобразование оценок критичности актива для применения в уравнении оценки риска

Критичность	Значение
[0:0,01)	0
[0,01:0,1)	0,5
[0,1:1)	1
[1:10)	1,2
[10:100)	1,4
100	1,51

Здесь *Exploitability* — возможность использования уязвимости; $f(AdjustedImpact) = \begin{cases} 0, \text{ если } AdjustedImpact = 0 \\ 1{,}176, \text{ если } AdjustedImpact \neq 0 \end{cases}$,

$$AdjustedImpact = \min(10{,}10{,}41 \times (1 - (1 - ConfImpact \times ConfReq) \times (1 - IntegImpact \times IntegReq) \times (1 - AvailImpact \times AvailReq))),$$

где *ConfImpact*, *IntegImpact*, *AvailImpact* — влияние на конфиденциальность, целостность и доступность в результате эксплуатации уязвимости соответственно; *ConfReq*, *IntegReq*, *AvailReq* — требования безопасности, которые в данном контексте рассматриваются как критичность актива, т. е. уравнение принимает вид

$$AdjustedImpact = \min(10{,}10{,}41 \times (1 - (1 - ConfImpact \times Criticality(c)) \times (1 - IntegImpact \times Criticality(i)) \times (1 - AvailImpact \times Criticality(a)))),$$

где *Criticality*(*c*), *Criticality*(*i*) и *Criticality*(*a*) — критичность конфиденциальности, целостности и доступности актива соответственно.

Таким образом, риск может принимать значения от 0 до 10. После того как определен риск каждой уязвимости хоста, оценка риска для экземпляра программно-аппаратного обеспечения определяется как максимальная из данных оценок, а оценка риска для хоста — как максимальная из оценок для программно-аппаратного обеспечения. Уровень риска для КС в целом определяется максимальной оценкой риска хостов как «высокий»/«средний»/«низкий» в соответствии с уровнями CVSS-оценок. Таким образом, можно выделить наиболее незащищенные участки системы.

Разработка данной методики включала выделение показателей, применяемых для вычисления уровня риска, преобразование уравнения CVSS для включения показателя критичности, преобразование шкалы значений показателя критичности для включения в уравнение CVSS, формирование правил определения уровня риска для КС в целом и ее объектов (уязвимостей, программного обеспечения, хостов).

Детальная статическая методика оценки рисков и динамическая методика

В рамках детальной статической методики и динамической методики риск предлагается определять на основе классического уравнения для вычисления риска [2]

$$Risk = AttackImpact \times AttackPotentiality,$$

где *AttackImpact* — ущерб от атаки (комбинация разрушительности атаки и критичности актива); *AttackPotentiality* — вероятность атаки.

Риск определяется для узлов графа атак (каждый узел соответствует атакующему действию). Граф атак задается следующим образом: $G = (S, L, Pc)$, где S — множество узлов графа (атакующих действий); L — множество связей ($L \subseteq S \times S$); Pc — дискретные локальные распределения условных вероятностей.

Значение риска варьируется от 0 до 100. При этом риск от 0 до 0,1 принимается низким (т. е. риском можно пренебречь), риск от 0,1 до 1 — средним (меры необходимо принять), риск от 1 до 10 — высоким (меры необходимо принять как можно скорее), а от 10 до 100 — критическим (меры необходимо принять немедленно).

Риск для атаки (последовательности атакующих действий) определяется как произведение минимальной вероятности из узлов атаки на графе на максимальный ущерб; риск для хоста — как максимальный из рисков всех атак, проходящих через хост; риск для КС — как максимальный из рисков хостов.

Предлагаемая авторами методика определения *AttackPotentiality* для узлов графа использует и развивает работы, применяющие байесовские графы атак [15, 8]. Отличиями являются метод формирования графа атак и метод вычисления локальных вероятностей компрометации узлов.

Байесовский граф атак был выбран для интеграции с динамической методикой, так как позволяет учитывать влияние событий на состояние системы и прогнозировать развитие атаки, а также определять предыдущие шаги атаки.

Алгоритм определения *AttackPotentiality* включает три шага: определение локальных вероятностей узлов; определение дискретных условных распределений вероятностей и определение полных вероятностей.

Локальные вероятности компрометации узлов найдем на основе индекса CVSS *Exploitability*:

$$Exploitability = 20 \times AccessVector \times AccessComplexity \times Authentication,$$

где *AccessVector* определяет доступность уязвимости, *AccessComplexity* определяет сложность эксплуатации уязвимости и *Authentication* определяет, требуется ли дополнительная аутентификация при эксплуатации уязвимости [8].

Поскольку предлагаемый граф атак построен таким образом, что переход из состояния в состояние возможен только в случае наличия доступа к соответствующему узлу, переопределим формулу определения *Exploitability* для определения локальной вероятности узла S_i, соответствующего атакующему действию a_i, следующим образом:

$$p(a_i) = 2 \times AccessVector \times AccessComplexity \times \times Authentication,$$

если $S_i \in S_r$, где S_r — множество корневых (входных) узлов графа. В этом случае локальная вероятность успешной компрометации узла может принимать значения от 0,1 до 1,0 (в соответствии с возможными значениями индексов CVSS). Если $S_i \notin S_r$:

$$p(a_i) = 2 \times AccessComplexity \times Authentication.$$

Локальная вероятность успешной компрометации узла может принимать значения от 0,3 до 1,0. Вероятность того, что узел не будет скомпрометирован, определяется как $1 - p(a_i)$.

Для определения условных распределений вероятностей всех узлов $Pc(S_i|Pa(S_i))$ (т. е. вероятностей компрометации узла S_i с учетом различных комбинаций состояний его предков $Pa(S_i)$) применяется обратный обход графа атак в глубину, начиная с терминальных узлов (узлов, у которых нет потомков) и заканчивая узлами, доступными атакующему. Типы связей между узлами-предками учитываются в соответствии с работой [15]. В случае связей типа «И» между узлами-предками (для успешной компрометации узла-потомка необходимо, чтобы все узлы-предки были скомпрометированы)

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

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

$$Pc\left(S_i \mid Pa(S_i)\right) = \begin{cases} 0, & \forall S_i \in Pa(S_i) \mid S_i = 0 \\ p(S_i), & \text{иначе} \end{cases}.$$

Безусловные вероятности компрометации узлов графа (вероятности атаки) определяются на основе локальных вероятностей и распределений условных вероятностей по формуле полной вероятности путем маргинализации по известным вероятностям: $Pr(S_1, \ldots, S_n) = \prod_{i=1}^{n} Pc\left(S_i \left| Pa[S_i] \right.\right)$.

Показатель ущерба от атаки (*AttackImpact*) для узла вычисляется на основе критичности актива R_k ($k \in [1, l]$, l — количество всех программных активов организации) и разрушительности соответствующего атакующего действия a_i в результате успешной эксплуатации уязвимости v_i ($i \in [1, m]$, m — множество всех уязвимостей данного актива) путем их перемножения. Критичность актива определяется по параметрам конфиденциальности $cCrit_k$, целостности $iCrit_k$ и доступности $aCrit_k$ так же, как в базовой методике. Разрушительность атакующего действия определяется на основе базовых показателей CVSS в виде вектора $[ConfImpact_{k,i}(c)\ IntegImpact_{k,i}(i)\ AvailImpact_{k,i}(a)]$, где $ConfImpact_{k,i}(c)$ — влияние на конфиденциальность актива R_k в случае успешной реализации атакующего действия a_i, использующего уязвимость v_i; $IntegImpact_{k,i}(i)$ — влияние на целостность актива R_k; $AvailImpact_{k,i}(a)$ — влияние на доступность актива R_k. $ConfImpact_{k,i}(c)$, $IntegImpact_{k,i}(i)$ и $AvailImpact_{k,i}(a)$ могут принимать значения {0,0; 0,275; 0,660} в соответствии с возможными значениями показателей CVSS влияние на конфиденциальность, влияние на целостность и влияние на доступность. Общий ущерб определяется суммированием ущерба по трем свойствам:

$$AttackImpact = cCrit_k \times ConfImpact_{k,i}(c) + + iCrit_k \times IntegImpact_{k,i}(i) + + aCrit_k \times AvailImpact_{k,i}(a).$$

В динамическом случае *AttackPotentiality* для узла S графа определяется с учетом модели инцидента ev, включающей показатель надежности информации $p(ev|S)$, который определяет вероятность того, что инцидент ev действительно произошел. Тогда вероятность того, что узел скомпрометирован, определяется как $p(ev|S)$:

$$p(S \mid ev) = \frac{p(ev \mid S) \times p(ev)}{p(S)} = = \frac{p(ev \mid S) \times \left(p(ev \mid S) \times p(S) + p(ev \mid \neg S) \times p(\neg S) \right)}{p(S)},$$

где $p(S)$ — вероятность компрометации узла до поступления инцидента; $p(ev|\neg S)$ — вероятность того, что инцидент ev не произошел (false positive).

Узел графа, соответствующий инциденту безопасности, определяется на основе следующих шагов: а) определение хоста, для которого обнаружен инцидент; б) определение узлов графа атак, соответствующих данному хосту; в) выделение узлов, дающих привилегии и (или) ведущих к ущербу, соответствующему инциденту безопасности (полученный набор узлов используется для переопределения вероятностей; если ни одного

узла не выбрано, то инцидент определяется как использование уязвимости 0-дня).

Вероятности узлов-потомков путей атак, проходящих через скомпрометированный узел, пересчитываются с учетом новой вероятности компрометации узла, для которого поступил инцидент безопасности.

Прототип и эксперименты

Архитектура прототипа

Разработанные методики реализованы в рамках системы оценивания защищенности КС. Архитектура системы представлена на рис. 2.

Компонент обработки данных получает входные данные от администратора, компонента сбора информации (который получает входные данные от сенсоров, сетевых сканеров, хостовых программных агентов, SIEM-системы и обрабатывает получаемые данные), компонента моделирования атак и генерирует обработанные входные данные. Полученные данные применяются как входные данные для компонента оценки защищенности.

Компонент оценки защищенности включает набор функций, реализующих методики вычисления показателей различного уровня и методику оценки защищенности. При поступлении новых данных показатели пересчитываются.

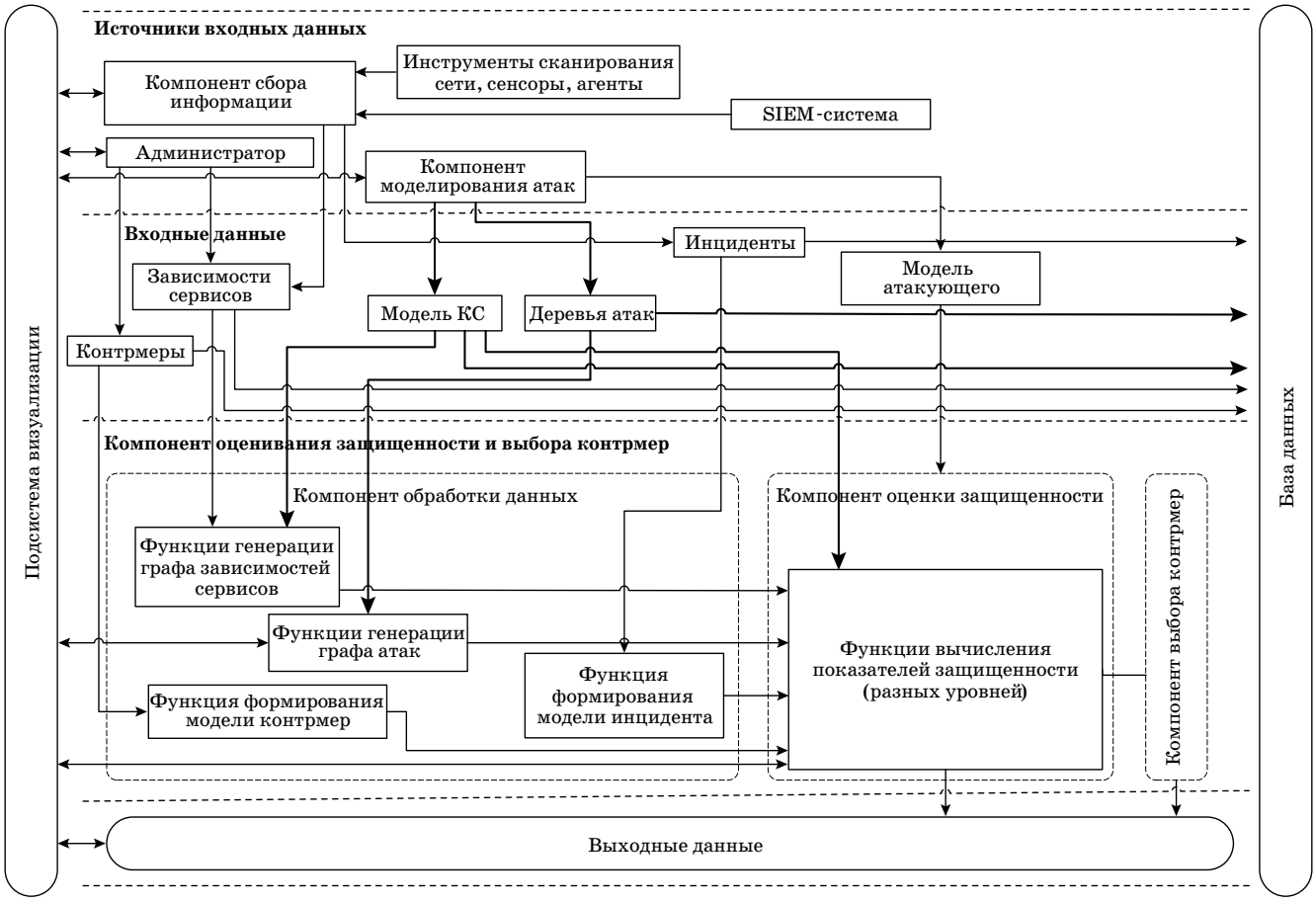
Выходные данные компонента (вычисленные показатели защищенности и оценка риска) передаются системе визуализации и компоненту выбора контрмер.

Прототип был реализован на языке Java с использованием принципов объектно-ориентированного программирования, на Microsoft Windows, Intel Core i7 CPU и 12 GB RAM.

Входные данные

Для проведения экспериментов использовались различные спецификации КС. Одна из спецификаций состояла из 10 хостов (рис. 3).

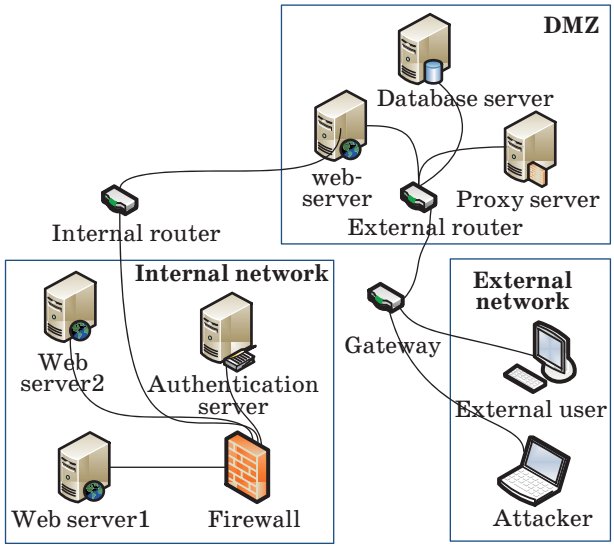
Ресурсы сети и значения их критичности представлены в табл. 2. Значения критичности определены по параметрам конфиденциальности, целостности и доступности на основе критичности бизнес-сервисов и зависимости их свойств безопасности от свойств безопасности программно-аппаратного обеспечения хостов.



■ *Рис. 2.* Архитектура системы оценивания защищенности и выбора контрмер

■ ***Таблица 2.*** Ресурсы тестовой сети и значения критичности

Сервис	Хост	Критичность
Веб-приложение (web application)	Web server1	[10,0 10,0 10,0]
ОС (cpe:/o:microsoft:windows_server_2008::r2:x64)	То же	[10,0 10,0 10,0]
ApacheStruts2 (cpe:/a:apache:struts:2.0.0)	–"–	[7,0 10,0 10,0]
JBoss AS (cpe:/a:redhat:jboss_community_application_server:5.0.1)	– "–	[10,0 10,0 10,0]
port tcp/443	– "–	[0,0 8,0 10,0]
port http/8080	– "–	[0,0 8,0 10,0]
Веб-приложение (web application)	Web server2	[10,0 10,0 10,0]
ApacheStruts2 (cpe:/a:apache:struts:2.0.0)	То же	[7,0 10,0 10,0]
ОС (cpe:/o:microsoft:windows_server_2008::r2:x64)	– "–	[10,0 10,0 10,0]
port http/8080	– "–	[0,0 8,0 10,0]
port tcp/443	– "–	[0,0 8,0 10,0]
JBoss AS (cpe:/a:redhat:jboss_community_application_server:5.0.1)	– "–	[10,0 10,0 10,0]
Сервис аутентификации (authentication service)	Authentication server	[20,0 20,0 20,0]
ОС (cpe:/o:suse:linux_enterprise_server:9)	То же	[20,0 20,0 20,0]
port tcp/ldaps 636	– "–	[0,0 16,0 20,0]
LDAP (slapd service)	– "–	[20,0 20,0 20,0]
ОС (cpe:/o:linux:linux_kernel:2.6.27.33)	DB server	[20,0 20,0 20,0]
SQL (cpe:/a:oracle:mysql:5.5.25)	То же	[20,0 20,0 20,0]
port tcp/443	– "–	[20,0 20,0 20,0]
Citrix (cpe:/a:citrix:ica_client:6.1)	Firewall	[20,0 20,0 20,0]
ОС (cpe:/o:linux:linux_kernel:2.6.27.33)	То же	[20,0 20,0 20,0]



■ ***Рис. 3.*** Топология тестовой сети

Представим результаты экспериментов для внешнего атакующего с высоким уровнем навыков. На рис. 4 изображен граф атакующих действий для тестовой сети в окне интерфейса пользователя программного средства.

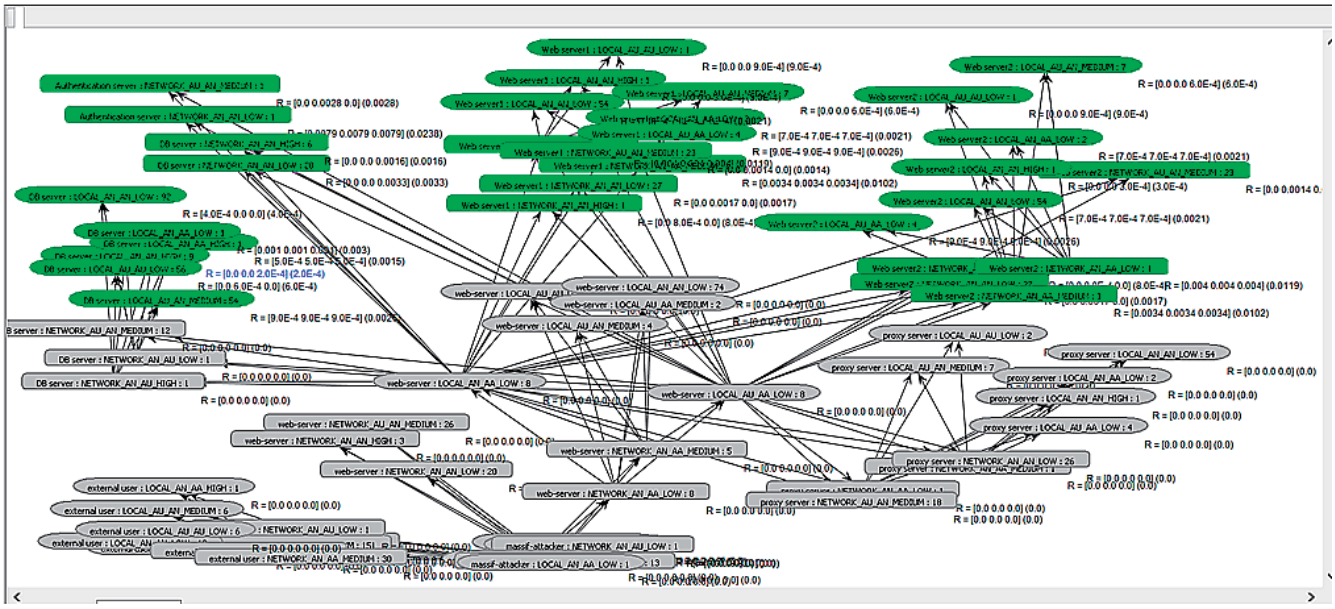
Каждый узел графа соответствует атакующему действию, которое может быть осуществлено путем эксплуатации одной из уязвимостей. Стрелки показывают возможность перехода от одного атакующего действия к другому. Уязвимости объединены в группы по совпадению таких параметров, как вектор доступа к уязвимости (*AccessVector*), требования аутентификации для эксплуатации уязвимости (*Authentication*), сложность доступа к уязвимости (*AccessComplexity*) и привилегии на хосте, получаемые после успешной эксплуатации уязвимости (*GainedPrivileges*). Данные параметры определяются на основе значений в открытой базе уязвимостей NVD [16, 17]. Каждый узел графа в окне интерфейса задан вектором в формате

H_NAME: *AccessVector_Authentication_*

GainedPrivileges_AccessComplexity,

где H_NAME — название хоста.

Для каждого узла отображается значение риска его успешной компрометации R в формате $R = [ConfRisk\ IntegRisk\ AvailRisk]$ (*FullRisk*), где *ConfRisk*, *IntegRisk*, *AvailRisk* — риск нарушения конфиденциальности, целостности и доступности соответственно; *FullRisk* — суммарный риск



■ ***Рис. 4.*** Граф атакующих действий для тестовой сети

по параметрам конфиденциальности, целостности и доступности.

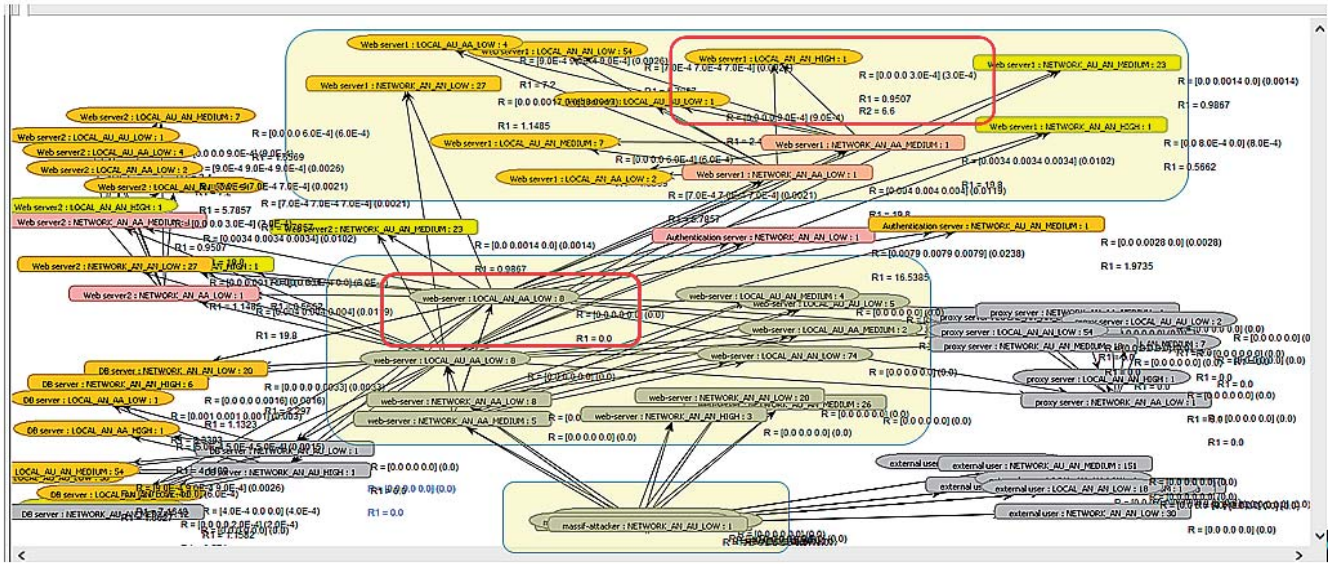
В программном средстве используется цветовая индикация узлов: зеленый — для низкого уровня риска, желтый — для среднего, оранжевый — для высокого и красный — для критического. Серым обозначаются узлы, для которых риск равен 0. Как видно из рисунка, риск находится в пределах нормы (т. е. низкий).

Эксперименты

Для применения динамической методики необходимы данные об инцидентах безопасности. При проведении экспериментов использовались сгенерированные данные, имитирующие реальные последовательности атак и инцидентов в сети на основе шаблонов CAPEC [18] (табл. 3). Это позволило проанализировать реакцию системы на разные типы последовательностей [19].

■ ***Таблица 3.*** Примеры последовательностей атак и инцидентов безопасности для экспериментов

Последовательность атакующих действий	Последовательность инцидентов безопасности
Attacker: CAPEC-170: Web Application Fingerprinting web-server: CAPEC-76: Manipulating Input to File System Calls web-server: CAPEC-224: Fingerprinting Web server1: CAPEC-10_descr Web server1: CAPEC-285: ICMP Echo Request Ping Web server1: CAPEC-10_descr	**Инцидент 1:** хост Attacker CAPEC-10_event **Инцидент 2:** хост Web server1 CAPEC-10_event **Инцидент 3:** хост Web server1 CAPEC-10_event
Attacker: CAPEC-299: TCP SYN Ping web-server: CAPEC-10_descr web-server: CAPEC-300: Port Scanning Web server1: CAPEC-10_descr	**Инцидент 1:** хост web-server CAPEC-10_event **Инцидент 2:** хост Web server1 CAPEC-10_event
Attacker: CAPEC-327: TCP Options Probe Attacker: CAPEC-76: Manipulating Input to File System Calls web-server: CAPEC-139: Relative Path Traversal web-server: CAPEC-328: TCP 'RST' Flag Checksum Probe Web server2: CAPEC-244: Cross-Site Scripting via Encoded URI Schemes Web server2: CAPEC-329: ICMP Error Message Quoting Probe Web server2: CAPEC-45: Buffer Overflow via Symbolic Links	**Инцидент 1:** хост Web server2 CAPEC-45 [An attacker creating or modifying Symbolic links is a potential signal of attack in progress. An attacker deleting temporary files can also be a sign that the attacker is trying to replace legitimate resources with malicious ones.]
Attacker: CAPEC-322: TCP (ISN) Greatest Common Divisor Probe Attacker: CAPEC-10_descr Attacker: CAPEC-323: TCP (ISN) Counter Rate Probe Attacker: CAPEC-76: Manipulating Input to File System Calls web-server: CAPEC-10_descr web-server: CAPEC-324: TCP (ISN) Sequence Predictability Probe Web server2: CAPEC-67: String Format Overflow in syslog() Web server2: CAPEC-325: TCP Congestion Control Flag (ECN) Probe Web server2: CAPEC-78: Using Escaped Slashes in Alternate Encoding	**Инцидент 1:** хост Attacker CAPEC-10_event **Инцидент 2:** хост web-server CAPEC-10_event **Инцидент 3:** хост Web server2 CAPEC-78 [An attacker can use a fuzzer in order to probe for this vulnerability. The fuzzer should generate suspicious network activity noticeable by an intrusion detection system.]



■ ***Рис. 5.*** Фрагмент интерфейса системы оценивания защищенности после поступления инцидентов безопасности

■ ***Таблица 4.*** Значения вероятности и риска для узлов графа после поступления инцидентов

Узел	Нет инцидента		Инцидент 1	
	Вероятность	Риск	Вероятность	Риск
web-server: LOCAL_AN_AA_LOW	0,0023	0,0	1,0	0,0
proxy server: LOCAL_AU_AN_MEDIUM	0,00009	0,0	0,2510	0,0
proxy server: LOCAL_AN_AN_HIGH	0,00005	0,0	0,1440	0,0
Web server1: NETWORK_AN_AN_HIGH	0,0003	0,0008 (низкий)	0,206	0,566 (средний)
Web server1: NETWORK_AU_AN_MEDIUM	0,0005	0,0014 (низкий)	0,3588	0,9867 (средний)
Web server1: NETWORK_AN_AA_MEDIUM	0,0005	0,0102 (низкий)	0,98	19,8 (критический)
Web server1: LOCAL_AN_AN_HIGH*	0,0005	0,0003 (низкий)	0,144	0,95 (средний)
Web server1: LOCAL_AU_AN_MEDIUM	0,00009	0,0006 (низкий)	0,2511	1,6569 (высокий)
Web server1: LOCAL_AN_AN_LOW	0,0001	0,0021 (низкий)	0,2922	5,79 (высокий)
Web server1: LOCAL_AN_AA_LOW	0,0001	0,0021 (низкий)	0,2922	5,79 (высокий)
Web server1: LOCAL_AU_AU_LOW	0,0001	0,0008 (низкий)	0,3636	2,4 (высокий)
Web server1: LOCAL_AU_AA_LOW	0,0001	0,0027 (низкий)	0,3636	7,2 (высокий)
Web server1: NETWORK_AN_AA_LOW	0,0006	0,012 (низкий)	0,98	19,8 (критический)
Web server2: NETWORK_AN_AN_LOW	0,0006	0,0017 (низкий)	0,4176	1,1485 (высокий)
Web server2: LOCAL_AN_AA_LOW	0,00007	0,003 (низкий)	0,2106	8,31 (высокий)
Web server2: LOCAL_AN_AN_HIGH	0,00003	0,0002 (низкий)	0,1038	0,571 (средний)
Web server2: NETWORK_AN_AA_ LOW	0,0006	0,0102 (низкий)	0,98	19,8 (критический)
Web server2: LOCAL_AU_AA_LOW	0,0001	0,0026 (низкий)	0,3636	7,2 (высокий)
Web server2: LOCAL_AU_AU_LOW	0,0001	0,0009 (низкий)	0,3636	2,4 (высокий)
Web server2: NETWORK_AN_AA_MEDIUM	0,0005	0,012 (низкий)	0,98	19,8 (критический)
Web server2: LOCAL_AN_AN_LOW	0,0001	0,0021 (низкий)	0,2922	5,79 (высокий)
DB server: NETWORK_AN_AN_HIGH	0,0003	0,0016 (низкий)	0,2059	1,1323 (высокий)
DB server: LOCAL_AN_AN_LOW	0,00007	0,0004 (низкий)	0,2106	1,1582 (высокий)
DB server: LOCAL_AU_AU_LOW	0,0001	0,0006 (низкий)	0,3023	1,6627 (высокий)
DB server: LOCAL_AU_AN_MEDIUM	0,00006	0,0026 (низкий)	0,1809	7,164 (высокий)
DB server: LOCAL_AN_AA_HIGH	0,000037	0,0015 (низкий)	0,1038	4,11 (высокий)
Authentication server: NETWORK_AU_AN_MEDIUM	0,0005	0,0028 (низкий)	0,3588	1,9735 (высокий)
Authentication server: NETWORK_AN_AN_LOW	0,0006	0,0237 (низкий)	0,4176	16,54 (критический)

* *Примечание*: после поступления второго инцидента значения показателей изменились только для узла Web server1: LOCAL_AN_AN_HIGH: вероятность = 1,0; риск = 6,6 (высокий).

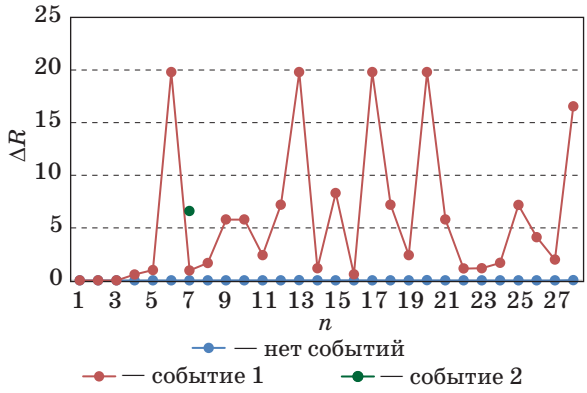
Фрагмент интерфейса системы оценивания защищенности после пересчета значений риска для сгенерированной последовательности атаки и последовательности инцидентов представлен на рис. 5: R обозначает исходное значение риска для узла графа, R_N — значение после обработки N-го инцидента безопасности. Последовательность атаки: CAPEC-299: TCP SYN Ping с хоста Attacker -> CAPEC-10_descr на хосте web-server -> CAPEC-300: Port Scanning на хосте web-server -> CAPEC-10_descr на хосте Web server1, где CAPEC-10_descr — CAPEC-10: Buffer Overflow via Environment Variables на хосте web-server. Узлы графа, соответствующие последовательности атаки, выделены прямоугольниками бледно-желтого цвета. Последовательность инцидентов: Инцидент 1 (хост web-server, шаблон атаки CAPEC-10): CAPEC-10_event -> Инцидент 2 (хост Web server1, шаблон атаки CAPEC-10) CAPEC-10_event, где CAPEC-10_event — «If the application does bound checking, it should fail when the data source is larger than the size of the destination buffer. If the application's code is well written, that failure should trigger an alert». Узлы графа, на которые отображены инциденты безопасности, выделены красной рамкой.

Новые значения вероятности и риска для узлов графа после поступления инцидентов приведены в табл. 4. Учет инцидентов безопасности позволяет зафиксировать повышение риска для узла Web server1 с низкого до критического, когда необходимо срочно приводить в действие контрмеры.

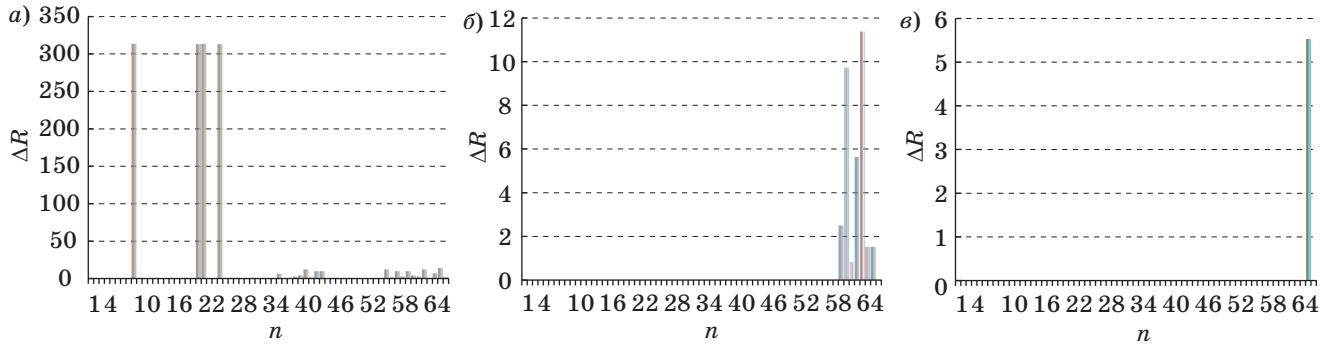
Сравнение с посланной на вход инструмента оценивания защищенности атакой показывает, что для узлов, входящих в атаку, уровень риска вырос как минимум до среднего (см. рис. 5). При этом важно отметить, что точность локализации атаки зависит от количества узлов графа (а соответственно, хостов сети), находящихся на одном уровне поддерева (в одной подсети). Для более точного определения цели атаки можно использовать различные характеристики атакующего. Тем не менее для проведенных экспериментов реально атакуемые узлы попадают во множество узлов, для которых выросло значение риска, что позволяет эффективно применять контрмеры на уровне подсети. Точность повышается при поступлении новых инцидентов безопасности, но она также зависит от внешнего фактора (точности поступившего инцидента).

На рис. 6 приведены значения риска для обрабатываемых узлов графа атак (в соответствии с табл. 4) до поступления инцидентов (синяя кривая), после поступления первого инцидента (красная кривая) и после поступления второго инцидента (зеленая точка), когда риск изменяется только для одного узла. Реально атакованные узлы Web server1 (точки *4–13*) имеют высокий уровень риска. При этом узел web-server (точка *1*) имеет низкий уровень риска, что объясняется его низкой критичностью.

Изменение значений риска в результате проведения различных атак на хосты сети показано на рис. 7: видно существенное изменение уровня риска для ряда узлов после поступления первого инцидента (рис. 7, *а*); после поступления второго инцидента количество узлов, для которых изменилось значение риска, основательно снизилось,



■ ***Рис. 6.*** График изменения значений риска ΔR для узлов графа n после поступления последовательности инцидентов безопасности



■ ***Рис. 7.*** График изменения значений риска ΔR для узлов графа n после поступления первого (*а*), второго (*б*) и третьего (*в*) инцидентов безопасности для различных атак на хосты сети

и можно локализовать узел, на который нацелена атака (рис. 7, *б*); после третьего инцидента количество затронутых узлов уменьшилось еще заметнее (рис. 7, *в*). Таким образом, уровень риска позволяет отследить наиболее критичные узлы сети, а изменение уровня риска позволяет локализовать цель атаки.

Так же, как и для атаки из примера на рис. 6, полученные оценки рисков сравнивались с реально атакованными узлами. Сравнение показало, что атакованным узлам назначаются высокие оценки, точность совпадения зависит от количества инцидентов, расположения атакованных хостов в сети, точности информации о поступающих событиях.

Таким образом, эксперименты подтвердили, что дополнительная информация влияет на изменение уровня риска и позволяет локализовать узлы для реализации контрмер.

В отличие от аналогичных работ в этой области, инструмент использует комплекс показателей, позволяющих учесть при оценке риска большее количество параметров. Так, подходы на основе вероятностей атак [7, 8] не учитывают зависимости между критичностью ресурсов и навыки атакующего; подходы, учитывающие возможный ущерб от атак [9, 10], не рассматривают вероятность атаки; подходы, учитывающие возможные финансовые потери [12], обычно не используют детальную оценку рисков. В предлагаемом инструменте мы попытались объединить достоинства всех перечисленных подходов, чтобы более точно отразить ситуацию для последующего рационального выбора контрмер.

Заключение

В работе предлагается компонент оценки рисков, интегрированный с SIEM-системой. Компонент реализует комплекс методик оценки рисков, основанных на показателях защищенности. Описываются некоторые особенности вычисления показателей. Описывается обобщенная архитектура программного компонента и элементы его интерфейса. Проведены эксперименты с использованием разработанного программного средства, демонстрирующие работу методик. По результатам экспериментов выделены достоинства и недостатки предложенных методик. Подтверждено влияние дополнительных данных на точность оценок. Приведено краткое сравнение с аналогичными подходами.

В будущем планируется детальнее рассмотреть характеристики и мотивацию различных типов атакующих для повышения точности оценки рисков.

Работа выполнена при финансовой поддержке РФФИ (проекты № 14-07-00697, 14-07-00417, 15-07-07451, 16-37-00338) и при частичной поддержке бюджетных тем № 0073-2015-0004 и 0073-2015-0007.

Литература

1. ГОСТ Р ИСО/МЭК 27004–2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. — Введ. 2011-12-01. — М.: Стандартинформ, 2012. — 56 с.
2. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. — Введ. 2010-11-30. — М.: Стандартинформ, 2011. — 47 с.
3. ISO/IEC 27005:2011. Information Technology. Security Techniques. Information Security Risk Management (second edition). — Switzerland: ISO/IEC, 2011. — 68 p.
4. ISO/IEC 27035:2011. Information Technology. Security Techniques. Information Security Incident Management. — Switzerland: ISO/IEC, 2011. — 78 p.
5. The Center for Internet Security. The CIS Security Metrics, 2009. https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf (дата обращения: 28.09.2016).
6. **Singhal A., Ou X.** Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs // NIST Interagency Report 7788. Gaithersburg, Aug. 2011, National Institute of Standards and Technology. — 24 p.
7. **Chunlu W., Yancheng W., Yingfei D., Tianle Z.** A Novel Comprehensive Network Security Assessment Approach // IEEE Intern. Conf. on Communications. IEEE, 2011. P. 1–6.
8. **Poolsappasit N., Dewri R., Ray I.** Dynamic Security Risk Management Using Bayesian Attack Graphs // IEEE Transactions on Dependable and Security Computing. 2012. Vol. 9. N 1. P. 61–74.
9. **Kheir N., Cuppens-Boulahia N., Cuppens F., Debar H.** A Service Dependency Model for Cost-Sensitive Intrusion Response // ESORICS'10. 2010. P. 626–642.
10. **Wu Y.-S.,** et al. Automated Adaptive Intrusion Containment in Systems of Interacting Services Computer Networks/ Y.-S. Wu, B. Foo, Y.-C. Mao, S. Bagchi, E. H. Spafford// The Intern. Journal of Computer and Telecommunications Networking. 2007. Vol. 51. P. 1334–1360.
11. **Manadhata P. K., Wing J. M.** An Attack Surface Metric // IEEE Transactions on Software Engineering. 2010. P. 371–386.
12. **Cremonini M., Martini P.** Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA) // Proc. of Fourth

Workshop on the Economics of Information Security, June 2–3, 2005. http://www.infosecon.net/workshop/pdf/23.pdf (дата обращения: 28.09.2016).
13. **Котенко И. В., Дойникова Е. В.** Методика выбора контрмер на основе комплексной системы показателей защищенности в системах управления информацией и событиями безопасности // Информационно-управляющие системы. 2015. № 3. С. 60–69. doi:10.15217/issn1684-8853.2015.3.60
14. **Mell P., Scarfone K.** A Complete Guide to the Common Vulnerability Scoring SystemVersion 2.0. 2007. https://www.first.org/cvss/cvss-v2-guide.pdf (дата обращения: 28.09.2016).
15. **Frigault M., Wang L., Singhal A. and Jajodia S.** Measuring Network Security Using Dynamic Bayesian Network // 2008 ACM Workshop on Quality of Protection, Oct. 2008. P. 23–30.
16. NVD website. https://nvd.nist.gov/ (дата обращения: 30.06.2016).
17. **Федорченко А. В., Чечулин А. А., Котенко И. В.** Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей // Информационно-управляющие системы. 2014. № 5. С. 72–79.
18. Common Attack Pattern Enumeration and Classification (CAPEC). https://capec.mitre.org (дата обращения: 30.06.2016).
19. **Kotenko I. and Doynikova E.** The CAPEC based Generator of Attack Scenarios for Network Security Evaluation // Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2015): proc. of the IEEE 8th Intern. Conf., Warsaw, Poland, Sept. 24–26, 2015. P. 436–441.

UDC 004.056
doi:10.15217/issn1684-8853.2016.5.54

Techniques and Software Tool for Risk Assessment on the Base of Attack Graphs in Information and Security Event Management Systems

Doynikova E. V.[a], Researcher, doynikova@comsec.spb.ru
Kotenko I. V.[a], Dr. Sc., Tech., Professor, ivkote@comsec.spb.ru
[a]Saint-Petersburg Institute for Informatics and Automation of the RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation

Introduction: The problem of response to computer attacks is still very important. Information technologies are used everywhere, computer networks become more complex and huge, therefore the number of computer threats always stays large. The procedures of security assessment and countermeasure selection should be constantly improved. Accurate and comprehensive risk analysis providing a valid and valuable assessment is crucial for giving the best response to an attack. Though researches have suggested a number of various approaches, a universal solution has not been found yet. **Purpose:** The goal is to develop risk assessment techniques which would accurately reflect the current security situation on the base of the available security data automatically processed, in order to develop a software tool implementing these techniques, and to evaluate their efficiency on experimental basis. **Results:** Techniques for security assessment have been developed and implemented as a software tool. The developed techniques are based on the complex system of security metrics suggested earlier by the authors. Some technique-specific aspects of calculating the security metrics have been reconsidered. The developed software tool allows you to choose a technique according to the current situation and user's demands. The techniques have been tested, and their advantages and disadvantages have been outlined. **Practical relevance:** The developed techniques and software tool can enhance information system security by providing valid and valuable assessment of the current security situation.
Keywords — Risk Assessment Technique, Security Metrics, Attack Graph, Service Dependency Graph, Security Incidents.

References

1. State Standard R ISO/IEC 27004–2011. Information Technology. Security Techniques. Information Security Management. Measurement. Moscow, Standartinform Publ., 2012. 56 p. (In Russian).
2. State Standard R ISO/IEC 27005–2010. Information Technology. Security Techniques. Information Security Risk Management. Moscow, Standartinform Publ., 2011. 47 p. (In Russian).
3. ISO/IEC 27005:2011. Information Technology. Security Techniques. Information Security Risk Management (second edition). Switzerland, ISO/IEC, 2011. 68 p.
4. ISO/IEC 27035:2011. Information Technology. Security Techniques. Information Security Incident Management. Switzerland, ISO/IEC, 2011. 78 p.
5. *The Center for Internet Security. The CIS Security Metrics.* 2009. Available at: https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf (accessed 28 September 2016).
6. Singhal A., Ou X. *Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs.* NIST Interagency Report 7788. Gaithersburg, National Institute of Standards and Technology, 2011. 24 p.
7. Chunlu W., Yancheng W., Yingfei D., Tianle Z. A Novel Comprehensive Network Security Assessment Approach. *Proc. of the IEEE International Conference on Communications*, Kyoto, 2011, IEEE, pp. 1–6.
8. Poolsappasit N., Dewri R., Ray I. Dynamic Security Risk Management using Bayesian Attack Graphs. *Proc. IEEE Transactions on Dependable and Security Computing*, 2012, vol. 9, no. 1, pp. 61–74.
9. Kheir N., Cuppens-Boulahia N., Cuppens F., Debar H. A Service Dependency Model for Cost-Sensitive Intrusion Response. *Proc. ESORICS'10*, 2010, pp. 626–642.
10. Wu Y.-S., Foo B., Mao Y.-C., Bagchi S., Spafford E. H. 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.
11. Manadhata P. K., Wing J. M. An Attack Surface Metric. *Proc. IEEE Transactions on Software Engineering*, 2010, pp. 371–386.
12. Cremonini M., Martini P. Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). *Proc. Fourth Workshop on the Economics of*

Information Security, 2005. Available at: http://www.infosecon.net/workshop/pdf/23.pdf (accessed 28 September 2016).
13. Kotenko I. V. and Doynikova E. V. Countermeasure Selection in Security Management Systems. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 3, pp. 60–69 (In Russian). doi:10.15217/issn1684-8853.2015.3.60
14. Mell P., Scarfone K. *A Complete Guide to the Common Vulnerability Scoring SystemVersion 2.0*. 2007. Available at: https://www.first.org/cvss/cvss-v2-guide.pdf (accessed 28 September 2016).
15. Frigault M., Wang L., Singhal A. and Jajodia S. Measuring Network Security Using Dynamic Bayesian Network. *Proc. 2008 ACM Workshop on Quality of Protection*, 2008, pp. 23–30.
16. *NVD website*. Available at: https://nvd.nist.gov/ (accessed 30 June 2016).
17. Fedorchenko A. V., Chechulin A. A., Kotenko I. V. Open Vulnerability Bases and their Application in Security Analysis Systems of Computer Networks. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2014, no. 5, pp. 72–79 (In Russian).
18. *Common Attack Pattern Enumeration and Classification (CAPEC)*. Available at: https://capec.mitre.org (accessed 30 June 2016).
19. Kotenko I. and Doynikova E. The CAPEC based Generator of Attack Scenarios for Network Security Evaluation. *Proc. IEEE 8th International Conference "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications" (IDAACS'2015)*, Warsaw, Poland, 2015, pp. 436–441.

Уважаемые авторы!

При подготовке рукописей статей необходимо руководствоваться следующими рекомендациями.

Статьи должны содержать изложение новых научных результатов. Название статьи должно быть кратким, но информативным. В названии недопустимо использование сокращений, кроме самых общепринятых (РАН, РФ, САПР и т. п.).

Объем статьи (текст, таблицы, иллюстрации и библиография) не должен превышать эквивалента в 20 страниц, напечатанных на бумаге формата А4 на одной стороне через 1,5 интервала Word шрифтом Times New Roman размером 13, поля не менее двух сантиметров.

Обязательными элементами оформления статьи являются: индекс УДК, заглавие, инициалы и фамилия автора (авторов), ученая степень, звание (при отсутствии — должность), полное название организации, аннотация и ключевые слова на русском и английском языках, электронные адреса авторов, которые по требованию ВАК должны быть опубликованы на страницах журнала. При написании аннотации не используйте аббревиатур и не делайте ссылок на источники в списке литературы.

Статьи авторов, не имеющих ученой степени, рекомендуется публиковать в соавторстве с научным руководителем, наличие подписи научного руководителя на рукописи обязательно; в случае самостоятельной публикации обязательно предоставляйте заверенную по месту работы рекомендацию научного руководителя с указанием его фамилии, имени, отчества, места работы, должности, ученого звания, ученой степени — эта информация будет опубликована в ссылке на первой странице.

Формулы набирайте в Word, не используя формульный редактор (Mathtype или Equation), при необходимости можно использовать формульный редактор; для набора одной формулы не используйте два редактора; при наборе формул в формульном редакторе знаки препинания, ограничивающие формулу, набирайте вместе с формулой; для установки размера шрифта никогда не пользуйтесь вкладкой Other…, используйте заводские установки редактора, не подгоняйте размер символов в формулах под размер шрифта в тексте статьи, не растягивайте и не сжимайте мышью формулы, вставленные в текст; в формулах не отделяйте пробелами знаки: + = −.

Для набора формул в Word никогда не используйте Конструктор (на верхней панели: «Работа с формулами» — «Конструктор»), так как этот ресурс предназначен только для внутреннего использования в Word и не поддерживается программами, предназначенными для изготовления оригинал-макета журнала.

При наборе символов в тексте помните, что символы, обозначаемые латинскими буквами, набираются светлым курсивом, русскими и греческими — светлым прямым, векторы и матрицы — прямым полужирным шрифтом.

Иллюстрации в текст не заверстываются и предоставляются отдельными исходными файлами, поддающимися редактированию:

— рисунки, графики, диаграммы, блок-схемы предоставляйте в виде отдельных исходных файлов, поддающихся редактированию, используя векторные программы: Visio 4, 5, 2002-2003 (*.vsd); Coreldraw (*.cdr); Excel (*.xls); Word (*.doc); AdobeIllustrator (*.ai); AutoCad (*.dxf); Matlab (*.ps, *.pdf или экспорт в формат *.ai);

— если редактор, в котором Вы изготавливаете рисунок, не позволяет сохранить в векторном формате, используйте функцию экспорта (только по отношению к исходному рисунку), например, в формат *.ai, *.esp, *.wmf, *.emf, *.svg;

— фото и растровые — в формате *.tif, *.png с максимальным разрешением (не менее 300 pixels/inch).

Наличие подрисуночных подписей обязательно (желательно не повторяющих дословно комментарии к рисункам в тексте статьи).

В редакцию предоставляются:

— сведения об авторе (фамилия, имя, отчество, место работы, должность, ученое звание, учебное заведение и год его окончания, ученая степень и год защиты диссертации, область научных интересов, количество научных публикаций, домашний и служебный адреса и телефоны, e-mail), фото авторов: анфас, в темной одежде на белом фоне, должны быть видны плечи и грудь, высокая степень четкости изображения без теней и отблесков на лице, фото можно представить в электронном виде в формате *.tif, *.png с максимальным разрешением — не менее 300 pixels/inch при минимальном размере фото 40×55 мм;

— экспертное заключение.

Список литературы составляется по порядку ссылок в тексте и оформляется следующим образом:

— для книг и сборников — фамилия и инициалы авторов, полное название книги (сборника), город, издательство, год, общее количество страниц;

— для журнальных статей — фамилия и инициалы авторов, полное название статьи, название журнала, год издания, номер журнала, номера страниц;

— ссылки на иностранную литературу следует давать на языке оригинала без сокращений;

— при использовании web-материалов указывайте адрес сайта и дату обращения.

Список литературы оформляйте двумя отдельными блоками по образцам lit.dot на сайте журнала (http://i-us.ru/paperrules) по разным стандартам: Литература — СИБИД РФ, References — один из мировых стандартов.

Более подробно правила подготовки текста с образцами изложены на нашем сайте в разделе «Оформление статей».

Контакты
Куда: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Кому: Редакция журнала «Информационно-управляющие системы»
Тел.: (812) 494-70-02
Эл. почта: ius.spb@gmail.com
Сайт: www.i-us.ru