УДК 004.056
doi:10.15217/issn1684-8853.2015.3.60

МЕТОДИКА ВЫБОРА КОНТРМЕР В СИСТЕМАХ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ И СОБЫТИЯМИ БЕЗОПАСНОСТИ

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

Цель: *ручная обработка информации, связанной с безопасностью, может привести к упущению важных факторов и, в конечном итоге, к выбору неэффективных защитных мер. Целью исследования является автоматизация процесса выбора защитных мер путем обработки данных по безопасности.* ***Результаты:*** *разработана методика выбора контрмер в процессе управления информацией и событиями безопасности, основанная на предложенной авторами комплексной системе показателей защищенности, отражающих ситуацию по безопасности в сети. Для выбора контрмер в систему показателей вводится дополнительный уровень поддержки принятия решений, базирующийся на показателях оценки эффективности применения контрмер. Основными особенностями предлагаемого подхода являются использование графов атак и зависимостей сервисов, применение предлагаемых модели контрмер и показателей защищенности, а также возможность предоставления решения по выбору контрмер в любой момент времени в соответствии с текущей информацией о состоянии защищенности и событиях безопасности.* ***Практическая значимость:*** *разработанная методика позволит повысить эффективность процесса принятия решений по выбору защитных мер в системах управления информацией и событиями безопасности.*

Ключевые слова *— инциденты безопасности, мониторинг, реагирование, показатели защищенности, выработка контрмер, графы атак, графы зависимостей сервисов.*

Введение

Современные информационные системы, как правило, содержат большое количество связанных между собой устройств и средств управления безопасностью, формирующих огромное количество информации и событий безопасности. Эту информацию необходимо обрабатывать в целях выявления возможных уязвимостей в защите, идентификации компьютерных атак и принятия контрмер.

Ручная обработка данной информации неэффективна по ряду причин: ограниченное время обработки, в результате чего время на противодействие компьютерной атаке может быть упущено; зависимость от уровня знаний эксперта, который может упустить важное сообщение или не связать между собой события, указывающие на атаку; возможность нанести системе еще больший ущерб в результате применения неэффективных контрмер или неправильной оценки уровня разрушительности атаки и несвоевременного реагирования на нее из-за сложных взаимосвязей между устройствами и сервисами системы.

Системы управления информацией и событиями безопасности (*Security Information and Events Management* — SIEM) создаются с целью решить эти проблемы и автоматизировать процесс обработки информации и событий безопасности [1, 2]. Функции SIEM-систем включают сбор записей о событиях из различных источников, их нормализацию, корреляцию, агрегацию, аналитическую обработку и составление отчетов.

Для повышения эффективности реагирования на компьютерные атаки в рамках исследований авторами в архитектуру SIEM-системы был добавлен компонент анализа защищенности на основе графов атак и зависимостей сервисов [1, 2]. Данный компонент дает возможность в результате анализа информации и событий безопасности сформировать ряд показателей защищенности, позволяющих сделать выводы об уровне защищенности системы и выбрать набор наиболее эффективных контрмер как для повышения общего уровня защищенности системы, так и для реагирования на отдельные атаки, выполняемые в реальном времени [3].

При разработке подхода, лежащего в основе работы компонента, учитывались особенности архитектуры SIEM-систем и особенности моделирования атак на компьютерные сети в виде графов атак [3].

Основными особенностями предлагаемого в статье подхода являются использование графов атак и зависимостей сервисов; применение введенной модели контрмер, базирующейся на стандартах «Общее перечисление защитных мер» (*Common Remediation Enumeration* — CRE) [4] и «Расширенная информация по защитным мерам» (*Extended Remediation Information* — ERI) [5]; использование предложенных показателей эффективности, стоимости и побочного ущерба контрмеры, а также возможность предоставления решения по выбору контрмер в любой момент времени в зависимости от текущей информации о состоянии защищенности и событиях безопасности в статическом и динамическом режимах

функционирования. Предлагаемый в работе подход позволит повысить защищенность информационных систем за счет автоматизации выбора обоснованных защитных мер.

Релевантные работы

Ранее авторы рассматривали вопросы вычисления различных показателей защищенности на основе графов атак и графов зависимостей сервисов [3]. В данной работе рассматриваются вопросы применения предложенных показателей, а также новых показателей уровня поддержки принятия решений для выбора контрмер. Подход учитывает и развивает модели и методы для расчета показателей, рассмотренные в работе [6].

При разработке подхода к выбору контрмер учитывались последние исследования в данной области [7, 8]. Вопросы автоматического выбора защитных мер представлены во многих работах, например в [9]. В ряде работ рассматривается аспект оценивания уровня риска на основе графов атак и графов зависимостей сервисов [6–8]. Некоторые авторы используют экономические индексы для оценивания возможных потерь и эффективности контрмер [10, 11]. Так, в работе [11] контрмеры оцениваются по трем параметрам, на основе которых определяется общий выигрыш от реализации k-й контрмеры:

$$Net\_Benefit_k = Benefit_k - Added\_Cost_k + \\ + Added\_Profit_k,\ \forall k = \{1, 2, 3, \ldots, l\},$$

где l — количество контрмер; $Benefit_k$ — выигрыш от реализации k-й контрмеры; $Added\_Cost_k$ — затраты на k-ю контрмеру; $Added\_Profit_k$ — дополнительная польза от реализации k-й контрмеры.

В работе [7] предлагается показатель выбора контрмер для реагирования на атаки на основе графов зависимостей сервисов — *показатель возврата инвестиций в реагирование* (*Return-On-Response-Investment* — RORI):

$$RORI = \frac{RG - (CD + OC)}{CD + OC},$$

где RG — эффективность реагирования; CD — побочные потери при реагировании; OC — затраты на контрмеры. Для реализации выбирается контрмера с наибольшим значением показателя RORI.

В статье [12] представлен модифицированный показатель RORI, учитывающий вариант отсутствия контрмер, а также размер инфраструктуры системы:

$$RORI = \frac{(ALE \times RM) - ARC}{ARC + AIV} \times 100,$$

где ALE — ожидаемые годовые потери (соответствуют последствиям негативного события в случае отсутствия контрмер), которые зависят от критичности и вероятности реализации атаки; RM — уровень снижения риска в случае реализации контрмеры; ARC — ожидаемые годовые затраты на реализацию контрмеры; AIV — годовые затраты на инфраструктуру (оборудование, поддержку) в случае реализации защитной меры.

Кроме того, следует учитывать существующие стандарты в области выбора контрмер. Вопросы выбора контрмер рассмотрены, например, в ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер». В этом стандарте риск используется для определения того, требуются ли защитные меры. В стандарте отмечено, что при выборе защитных мер важно сравнивать расходы по реализации защиты со стоимостью активов и оценивать возврат вложений с точки зрения снижения рисков. Кроме того, защитные меры не должны снижать функциональные возможности системы.

Настоящие исследования ориентированы на системы управления информацией и событиями безопасности. В этой области наиболее продвинутыми работами являются, например, [7, 12]. В статье предлагается развитие существующих подходов с использованием расширенного набора показателей и многоуровневого подхода, использующего, в том числе, семейство стандартов, применяемых в протоколе SCAP [13]. Авторами разработана методика выбора защитных мер, которая учитывает их влияние на угрозы, уязвимости и воздействия, а также общий уровень риска с учетом подхода к оценке защищенности системы на основе графов атак [3].

Описание подхода

Модель контрмер

Для учета контрмеры в общем подходе к поддержке принятия решений по реагированию на атаки необходимо сформировать модель контрмер.

Поскольку в данном исследовании используются стандарты протокола SCAP [13] для автоматизации оценки защищенности, рассмотрим соответствующие стандарты описания контрмер: стандарты CRE [4] и ERI [5]. Хотя стандарты еще находятся в процессе разработки и не сформирована полная база данных, использующая указанные стандарты, они подходят для создания модели контрмер.

Стандарт CRE является схемой определения и описания контрмер в формате XML [4]. Стандарт ERI содержит дополнительную информацию к CRE [5].

В настоящей статье в модель контрмеры (рис. 1) предполагается включить:

1) поля стандарта CRE: текстовое описание элемента (метод и действие контрмеры); платформу

Поля:

Название	Описание	CCE или CVE	Платформа	Влияние на граф атак	Влияние на работу	Эффективность	Стоимость

Пример значений полей

Запрет или перенаправление запросов	Запрет или перенаправление url запросов от подозрительных учетных записей	CVE-2010-1870	cpe:/a:apache:struts:2.0.0	Удаление связи	**CD** = = **[0 0 0.5]**	**CE** = = **[0.5 0.5 0.5]**	500 €

■ ***Рис. 1.*** Модель контрмеры

с использованием языка CPE Applicability Language 2.3, для которой применима данная контрмера;

2) поля стандарта ERI: индикаторы (ссылки на CCE [14] или CVE [15]); влияние на работу — отрицательное влияние на свойства безопасности активов, выражается показателем *уровень побочного ущерба* (*CollateralDamage* — CD) в виде трехмерного вектора $[\mathbf{CD}_c\ \mathbf{CD}_i\ \mathbf{CD}_a]$, где $\mathbf{CD}_c$, $\mathbf{CD}_i$, $\mathbf{CD}_a$ — соответственно ущерб для свойств конфиденциальности/целостности/доступности в результате реализации контрмеры; эти параметры принимают значения от 0 до 1;

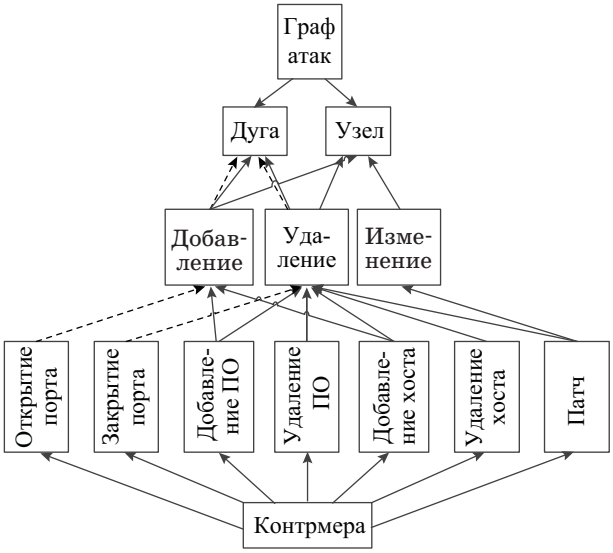
3) дополнительные поля: название контрмеры; тип влияния на граф атак — удаление, добавление или изменение связи в графе (поле принимает значения {REMOVE[CVE1-CVE2], ADD[CVE1-CVE2], MODIFY[CVE1-CVE2]});

4) показатели: *эффективность контрмеры* (*Countermeasure Effectiveness* — CE) — степень исправления свойства безопасности в виде трехмерного вектора $[\mathbf{CE}_c\ \mathbf{CE}_i\ \mathbf{CE}_a]$, где $\mathbf{CE}_c$, $\mathbf{CE}_i$, $\mathbf{CE}_a$ — соответственно значения эффективности исправления свойств конфиденциальности/целостности/доступности в результате реализации контрмеры; эти параметры принимают значения от 0 до 1; *стоимость контрмеры* (*Countermeasure Cost* — CC) — стоимость реализации контрмеры, измеряется в денежных единицах.

В качестве демонстративного примера рассмотрим следующие варианты контрмер: патч для уязвимости (информацию можно взять, например, из базы xForce [16, 17], которая содержит временные оценки CVSS, в том числе *уровень исправления*, который определяет наличие патча для уязвимости); удаление уязвимого программного обеспечения; закрытие порта; добавление дополнительных защитных средств (например, фаервола или антивируса).

Связь модели контрмер и графа атак

В основе методики принятия решений лежит граф атак. Граф атак представляет собой граф переходов состояний, в котором каждый узел соответствует успешной/неуспешной эксплуатации уязвимости, а дуга — возможности перехода от одного атакующего действия к другому [19]. Реализация контрмеры влияет на переходы состояний и, соответственно, изменяет граф атак (удаляя/добавляя узлы) и вероятности атак. Очевидно, что контрмера может повлиять на каждый из этих элементов тремя способами: удалением, добавлением, изменением (например, вероятности атак) (рис. 2). Пунктирными и сплошными стрелками выделены пути, соответствующие определенным контрмерам, например, открытие порта обусловливает добавление дуги, но не узла.



■ ***Рис. 2.*** Зависимости между контрмерами и объектами графа атак

Расширение таксономии показателей

В соответствии с работами [3, 19] для построения таксономии показателей используется комплексная иерархическая система показателей, позволяющих на разных уровнях (топологическом, графа атак, атакующего, событий и системы) и с учетом различных аспектов (основных показателей, показателей нулевого дня и стоимостных показателей) отразить текущий уровень защищенности.

Показатели топологического уровня определяются администратором на основе топологии системы (сети) [3].

На уровне графа атак для вычисления показателей защищенности используется информация, получаемая на основе графа атак. Данный уровень позволяет определить вероятность атаки и возможный ущерб с учетом всех путей атаки [3].

На уровне атакующего вводится зависимость от профиля атакующего (т. е. его положения в сети и навыков). Это позволяет сформировать так называемый профильный граф атак, который включает атаки, которые может реализовать именно данный атакующий [3].

Уровень событий соответствует динамическому режиму работы системы оценивания защищенности [3]. Он позволяет отслеживать развитие атаки и профиль атакующего по событиям безопасности. На основе поступающих событий корректируется позиция атакующего на графе атак и возможные пути продолжения атаки.

На уровне системы определяются общий уровень защищенности системы и поверхность атаки системы.

Основные показатели каждого уровня представлены на рис. 3, где пунктирными стрелками обозначены необязательные связи.

В соответствии с определенной моделью контрмер необходимо расширить таксономию показателей защищенности за счет введения дополнительных показателей в модель контрмер: стоимости контрмеры, эффективности контрмеры и уровня побочного ущерба.

Связь уровня принятия решений и остальных уровней таксономии

Рассмотрим ниже связь уровня принятия решений с четырьмя другими уровнями: топологическим, графа атак, атакующего и событий.

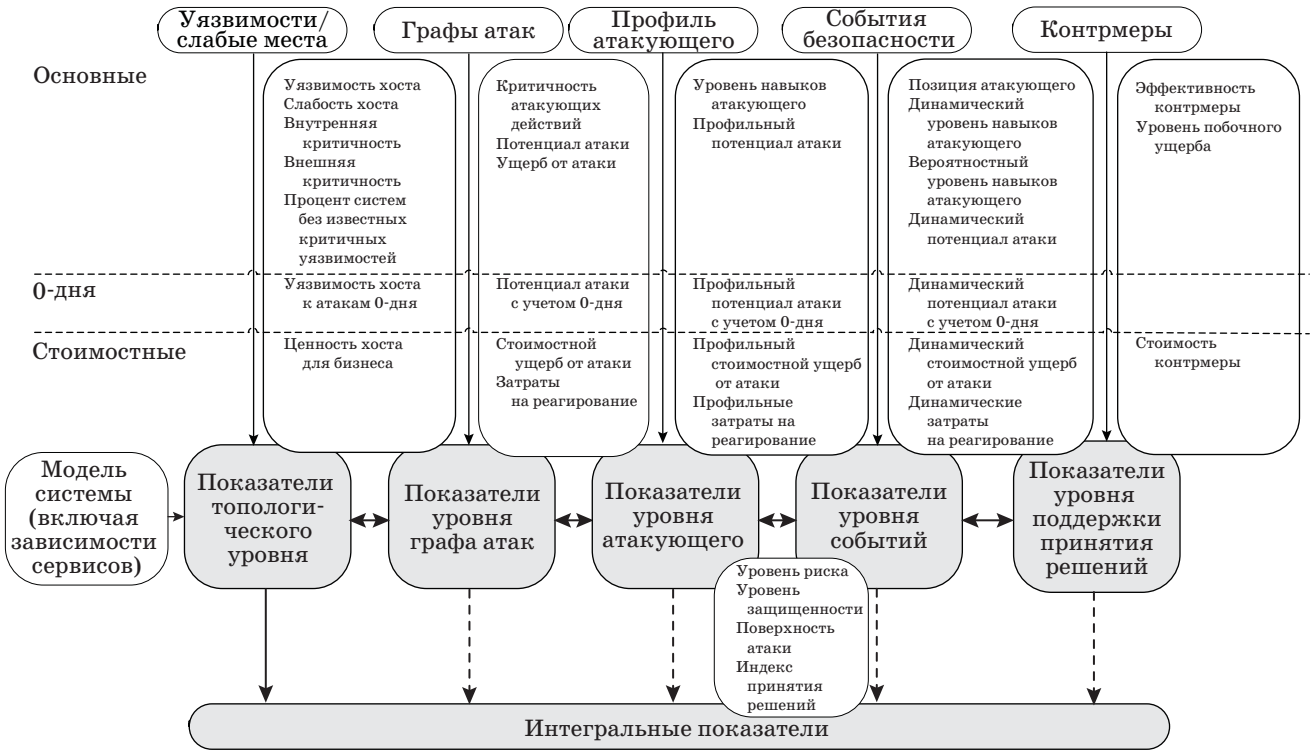
Топологический уровень

На данном уровне не рассматриваются многошаговые атаки, использующие множество уязвимостей. Как следствие, не учитывается влияние контрмер на граф атак. Поэтому принятие решений основано на использовании уровня риска для отдельных активов, который определяется при помощи контекстной оценки CVSS (от 0 до 10) [18]:

$$Risk = round\_to\_1\_decimal(AdjustedBase),$$

где $AdjustedBase=BaseScore$, в котором $BaseScore$ $Impact$ заменен на $AdjustedImpact$;

$$AdjustedBase = round\_to\_1\_dicimal\times$$
$$\times\left((0{,}6\,AdjustedImpact + 0{,}4\,Exploitability - 1{,}5)\times\right.$$
$$\left.\times\, f(AdjustedImpact)\right);$$
$$AdjustedImpact =$$
$$= \min\left(10;10{,}41\times\left(1-(1-ConfImpact\times ConfReq)\times\right.\right.$$
$$\times(1-IntegImpact\times IntegReq)\times$$
$$\left.\left.\times(1-AvailImpact\times AvailReq)\right)\right),$$



■ ***Рис. 3.*** Расширенная таксономия показателей защищенности

где *ConfImpact*, *IntegImpact*, *AvailImpact* — влияние на конфиденциальность, целостность и доступность; *ConfReq*, *IntegReq*, *AvailReq* — требования безопасности, которые в данном контексте рассматриваются как критичность актива, поэтому

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

где *Criticality*(*c*), *Criticality*(*i*) и *Criticality*(*a*) — критичность конфиденциальности, целостности и доступности актива соответственно. Значения определяются экспертами в зависимости от возможных потерь организации. Возможные значения показателей критичности: [0; 1,51];

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

где *AccessVector* — вектор доступа; *AccessComplexity* — сложность доступа; *Authentication* — аутентификация;

$$f(AdjustedImpact) = \begin{cases} 0, & \text{если } AdjustedImpact = 0 \\ 1{,}176, & \text{если } AdjustedImpact \neq 0 \end{cases}.$$

Методика выбора контрмер на данном уровне реализуется в несколько этапов.

1. Выявление активов с неприемлемым уровнем риска, т. е. «высокой» контекстной (environmental) CVSS-оценкой согласно системе CVSS (от 7,0 до 10,0).

2. Определение временной (temporal) CVSS-оценки на предмет того, не уменьшится ли значение риска с реализацией патча. Оценка определяется на основе временного уравнения CVSS, использующего только один дополнительный показатель — *уровень исправления* (*RemediationLevel*), который определяет наличие патча для уязвимости [18]: *TemporalScore* = *round_to_1_decimal*(*BaseScore* × *RemediationLevel*), где функция *round_to_1_decimal* выполняет округление аргумента до одного знака после запятой. Временная CVSS-оценка имеет значение от 0 до 10. Если уровень риска для актива становится ниже 7,0, то система рекомендует применить патчи для соответствующих уязвимостей.

3. Для активов с высокой оценкой уровня риска определяются четыре аспекта: риск нарушения конфиденциальности/целостности/доступности и получения привилегий нелегитимным пользователем (в соответствии с CVSS-данными по уязвимости, определившей оценку риска). Для этого используются показатели *ConfImpact*, *IntegImpact*, *AvailImpact* и *ConfReq*, *IntegReq*, *AvailReq* следующим образом: реализация контрмер необходима для обеспечения соответствующего свойства безопасности, если *ConfImpact*, *IntegImpact* или *AvailImpact* ≥ 0,275 (т. е. ущерб есть), и если требования *ConfReq*, *IntegReq*, *AvailReq* для этого свойства > 1,0 (т. е. критичность высокая). Необходимо перебрать все уязвимости с «высокой» оценкой риска, относящиеся к данному активу. В случае если уязвимость дает возможность получения привилегий, необходимо применять контрмеры.

4. В зависимости от того, какие аспекты безопасности могут быть нарушены, выбираются контрмеры для обеспечения соответствующих свойств безопасности (например, дополнительная аутентификация в случае риска нарушения конфиденциальности). В модели контрмер это заложено в оценках показателей эффективности [$\mathbf{CE}_c$ $\mathbf{CE}_i$ $\mathbf{CE}_a$]: если $\mathbf{CE}_c \neq 0$, то соответствующую контрмеру можно использовать против нарушения конфиденциальности; если $\mathbf{CE}_i \neq 0$ — против нарушения целостности; если $\mathbf{CE}_a \neq 0$ — против нарушения доступности.

5. Для выбора контрмер используется следующий подход. Интуитивно понятно, что необходимо увеличить выигрыш от реализации защитных мер при снижении затрат. Выигрыш определяется отношением риска до реализации защитных мер к риску после реализации защитных мер. Чем меньше будет риск после реализации защитных мер, тем больше будет данная величина. Затраты, нормализованные согласно шкале критичности, помещаются в знаменатель. Таким образом, с увеличением затрат данный показатель уменьшится, и наоборот. Показатель *индекс принятия решения* (*Countermeasure Index* — CI), используемый для выбора защитных мер, определим следующим образом:

$$CI = \frac{R_b}{R_a \times CC},$$

где R_b — риск в случае, если защитные меры не реализованы; R_a — риск в случае, если защитные меры реализованы.

Уровень графа атак, уровень атакующего и уровень событий

На уровне *графа атак* рассматриваются узлы графа атак с уровнем риска, превышающим приемлемый. Для таких узлов рассматривается возможность реализации защитных мер в соответствии с классификацией на рис. 2. На данном уровне применяются методы вычисления уровня риска, определенные для графа атак [3, 19, 20]. На *уровне атакующего* дополнительно учитываются возможности нарушителя.

На *уровне событий* контрмеры реализуются в зависимости от текущих и будущих (спрогнозированных) шагов нарушителя. При этом учитывается «глубина графа до критичного ресурса», которая определяется как количество узлов

графа до актива с высоким уровнем критичности. Если данная глубина превышает определенное значение, то система ждет нового события для уточнения своих оценок; если глубина меньше определенного значения, система предлагает контрмеру на основе имеющихся данных со степенью точности, соответствующей количеству уже выявленных релевантных событий.

Описание case study

Описание тестовой сети и возможных контрмер

Для демонстрации выбран фрагмент сети из сценария ATOS для проекта MASSIF [1]. Фрагмент тестовой сети представлен на рис. 4 [1].

■ Описание программного обеспечения

Хост	Программное обеспечение
Веб-сервер Accreditation (Massif-2)	Windows Server 2008 R2 (64 bits); JBoss AS 5.0.1; Snare agent; ApacheStruts2 framework
Веб-сервер Sport Entries (Massif-1)	Windows Server 2008 R2 (64 bits); JBoss AS 5.0.1; Snare agent; ApacheStruts2 Framework (cpe:/a:apache:struts:2.0.0)
Сервер аутентификации Authentication (Massif-3)	SUSE Enterprise Linux 11 SP1 (32 bits) (cpe:/o:novell:suse_linux:11:sp1:server)
	NetIQ eDirect server 8.8.7.1 (cpe:/a:netiq:edirectory:8.8.7.1)

В таблице [1] описано программное обеспечение тестовой сети. Структуру сервисов тестовой сети определим следующим образом: для аутентификации используется NetIQ eDirect, доступ к данным eDirect осуществляется по протоколу LDAP, инкапсулированному в SSL (порт 636); веб-приложения Accreditation и Sport Entries задействуют ApacheStruts2 framework (использует порт 8080 для доступа к веб-страницам), поддерживаемый JBoss AS (использует порт 443).

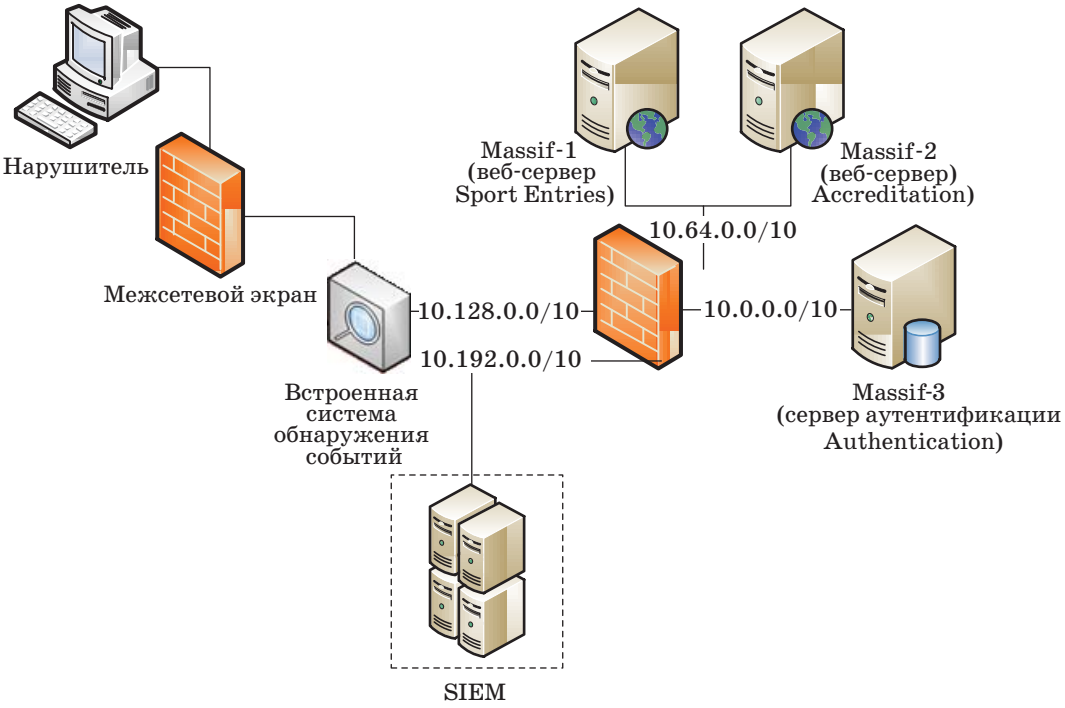
Граф зависимостей сервисов

Граф зависимостей сервисов (рис. 5) построен в соответствии с методикой, предложенной в работе [7]: зависимость определяется необходимостью доступности, целостности и конфиденциальности сервиса для обеспечения доступности, целостности и конфиденциальности другого сервиса. Сервисы предоставляются различными приложениями хостов системы или сетевыми устройствами.

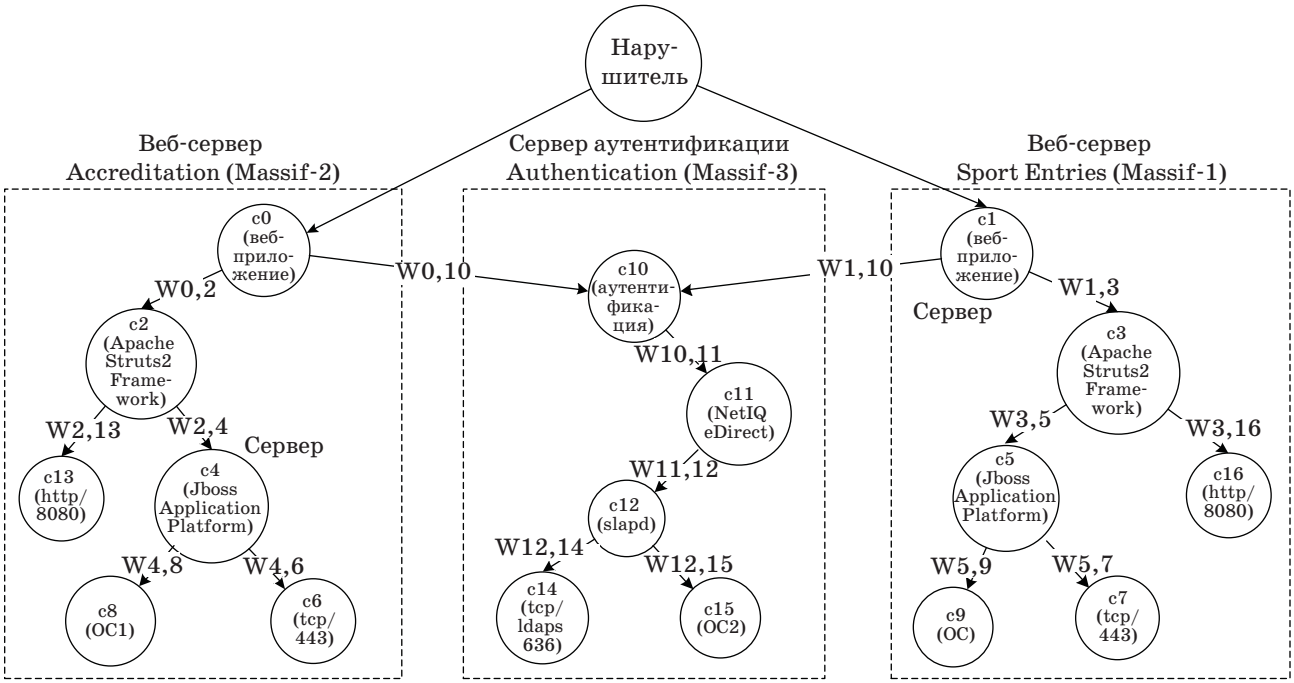
Для вычисления показателей необходимо задать весовые матрицы зависимостей (задаются экспертами).

Вычисление показателей для выбора контрмер

Для описанного фрагмента сети и атаки на веб-сервер Massif-2 определим *индекс принятия решения*. Для этого необходимо найти уровень риска до и после внедрения контрмер. Для упрощения вычислений выберем топологический уровень.



■ ***Рис. 4.*** Схема фрагмента тестовой сети



■ ***Рис. 5.*** Зависимости сервисов

На топологическом уровне риск атаки на веб-сервер Massif-2 до внедрения контрмер определим следующим образом. Вначале вычислим критичность активов (в данном случае, это информация на веб-серверах): *Criticality*(*c*) = 0,8, *Criticality*(*i*) = 0,8 и *Criticality*(*a*) = 0,8.

Далее необходимо оценить риск до внедрения контрмер в соответствии с формулой для топологического уровня, определенной выше. Например, для узла Massif-2 он будет определен в соответствии с максимальной CVSS-оценкой уязвимостей хоста — уязвимостью ApacheStruts2 Framework CVE-2013-4316 (10,0 H; AV:L/AC:L/Au:N/C:C/I:C/A:C).

Отметим, что хотя сам сервис ApacheStruts2 Framework не отмечен как критичный для системы, тем не менее сохранение его свойств безопасности необходимо для сохранения свойств безопасности веб-приложения в соответствии с весовой матрицей: $\mathbf{W}_{0,2} = \begin{bmatrix} 0,7 & 0,7 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$. Критичность ApacheStruts2 Framework будет определяться как *Criticality*(*c*) = 0,56, *Criticality*(*i*) = 0,8 и *Criticality*(*a*) = 0,8.

Уязвимость представлена с помощью идентификаторов CVE [15], базовой оценки CVSS по шкале от 1 до 10 и соответствующего качественного значения (H — высокая, M — средняя, L — низкая оценка критичности уязвимости) и базовых векторов CVSS: AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/ A:[N,P,C], где AV — вектор доступа к уязвимости (L — локальный, A — смежная сеть, N — удаленный); AC — сложность доступа к уязвимости (H — высокая, M — средняя, L — низкая); Au — показатель того, требуется ли дополнительная аутентификация (M — требуется пройти несколько процедур аутентификации, S — требуется пройти одну процедуру аутентификации, N — не требуется); C, I и A — ущерб, наносимый конфиденциальности, целостности и доступности в результате успешной эксплуатации уязвимости соответственно (N — нет, P — частичный, C — полный) [19].

Поскольку ущерб является полным, то согласно системе оценивания CVSS *ConfImpact* (C), *IntegImpact* (I) и *AvailImpact* (A) имеют значения 0,660. Тогда

$$AdjustedImpact =$$

$$= \min\left(10; 10,41 \times \left(1 - (1 - 0,660 \times 0,56) \times \right.\right.$$

$$\left.\left. \times (1 - 0,660 \times 0,8) \times (1 - 0,660 \times 0,8)\right)\right) = 8,948.$$

Вектор доступа определяется как локальный, что согласно системе оценивания CVSS соответствует значению 1,0; сложность доступа определяется как низкая, что соответствует значению 0,71; аутентификация не требуется, что соответствует значению 0,704. Таким образом:

$$Exploitability = 20 \times 1,0 \times 0,71 \times 0,704 = 9,9968,$$

$$f(AdjustedImpact) = 1,176;$$

$$AdjustedBase =$$
$$= round\_to\_1\_dicimal\big(((0{,}6\times 8{,}948)+$$
$$+(0{,}4\times 9{,}9968)-1{,}5)\times 1{,}176\big)=9{,}3;$$
$$Risk = AdjustedBase = 9{,}3.$$

Определим риск после внедрения контрмер. Для примера возьмем контрмеру 1 «блокировка подозрительных учетных записей» (в случае которой эффективность $\mathbf{CE}_{c1} = 0{,}75$ и стоимость $CC_1 = 0{,}0001$) и контрмеру 2 «активация многофакторной аутентификации» ($\mathbf{CE}_{c2} = 0{,}85$ и $CC_2 = 0{,}0001$):

$$AdjustedImpact_1 = 8{,}948,$$
$$AdjustedImpact_2 = 8{,}948;$$
$$Exploitability_1 =$$
$$= 20\times 1{,}0\times 0{,}71\times 0{,}704\times 0{,}75 = 7{,}4976,$$
$$Exploitability_2 = 8{,}4973;$$
$$f(AdjustedImpact_1) = 1{,}176,$$
$$f(AdjustedImpact_2) = 1{,}176;$$
$$AdjustedBase_1 =$$
$$= round\_to\_1\_dicimal\big(((0{,}6\times 8{,}948)+$$
$$+(0{,}4\times 7{,}4976)-1{,}5)\times 1{,}176\big)=8{,}1,$$
$$AdjustedBase_2 =$$
$$= round\_to\_1\_dicimal\big(((0{,}6\times 8{,}948)+$$
$$+(0{,}4\times 8{,}4973)-1{,}5)\times 1{,}176\big)=8{,}5;$$
$$Risk_1 = AdjustedBase_1 = 8{,}1,$$
$$Risk_2 = AdjustedBase_2 = 8{,}5.$$

Соответственно, коэффициенты выбора контрмер

$$CI_1 = \frac{R_b}{R_{a1}\times CC_1} = \frac{9{,}3}{8{,}1\times 0{,}0001} = 11\,481{,}5;$$
$$CI_2 = \frac{9{,}3}{8{,}5\times 0{,}0001} = 10\,941{,}2.$$

Максимальный коэффициент используется для выбора защитных мер. Таким образом, будет выбрана контрмера «блокировка подозрительных учетных записей».

Были проведены эксперименты для различных сетевых топологий и различных наборов входных данных. Эксперименты подтвердили, что благодаря дополнительной информации на каждом новом уровне можно выбрать более эффективные защитные меры (с меньшей стоимостью и позволяющие минимизировать ущерб).

Тем не менее индекс принятия решений имеет ряд ограничений. Так, например, он не применим в случае нулевой стоимости защитных мер и в случае нулевого риска после внедрения защитных мер. В дальнейшем планируется модифицировать индекс для устранения этого недостатка.

Заключение

Предложен подход к выбору контрмер в системах управления информацией и событиями безопасности, основанный на многоуровневой системе показателей защищенности. Для выбора контрмер применяются показатели оценки эффективности и целесообразности применения контрмер.

Особенностью предложенного подхода является возможность предоставления решения по выбору контрмер в любой момент времени в зависимости от имеющихся в наличии входных данных о текущей ситуации по уровню защищенности как в статическом, так и в динамическом режимах функционирования системы. Приведен пример применения подхода для простого сценария атаки на фрагменте тестовой сети.

В дальнейшем планируется продолжить серию экспериментов по определению эффективности предложенного подхода на различных компьютерных сетях при реализации различных атак.

Работа выполнена при финансовой поддержке РФФИ (13-01-00843, 14-07-00697, 14-07-00417, 15-07-07451) и программы фундаментальных исследований ОНИТ РАН (контракт № 1.5).

Литература

1. **MASSIF** FP7 Project. MAnagement of Security information and events in Service Infrastructures. http://www.massif-project.eu (дата обращения: 02.04.2015).
2. **Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А.** Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Тр. СПИИРАН. 2012. Вып. 1(20). С. 27–56.
3. **Kotenko I. and Doynikova E.** Security Assessment of Computer Networks based on Attack Graphs and Security Events // Proc. of the 2014 Asian Conf. on Availability, Reliability and Security, LNCS, 2014. P. 462–471.
4. **McGuire G. T., Waltermire D., Baker J. O.** Common Remediation Enumeration (CRE) Version 1.0 (Draft) // NIST Interagency Report 7831 (Draft). — National Institute of Standards and Technology, Dec. 2011. — 33 p.
5. **Johnson C.** Enterprise Remediation Automation // Proc. of the IT Security Automation Conf., Sept. 27–29, 2010. NIST. http://csap.nist.gov/events/2010/itsac/

presentations/day1/Automation_Specifications-Enterprise_Remediation_Automation.pdf (дата обращения: 02.04.2015).
6. **Kotenko I., Stepashkin M.** Attack Graph based Evaluation of Network Security // Proc. of the 10th IFIP Conf. on Communications and Multimedia Security (CMS'2006), Heraklion, Greece, 2006. P. 216–227.
7. **Kheir N.** Response Policies and Counter-Measures: Management Ofservice Dependencies and Intrusion and Reaction Impacts: PhD thesis. — Ecole Nationale Supérieure des Télécommunications de Bretagne, 2010. — 229 p.
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. **Balepin I., Maltsev S., Rowe J., Levitt K.** Using Specification-Based Intrusion Detection for Automated Response // Proc. of 6th Intern. Symp., RAID 2003, Pittsburgh, PA, USA, Sept. 8–10, 2003. Lecture Notes in Computer Science, 2003. P. 136–154.
10. **Cremonini M. and Martini P.** Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA) // Workshop on the Economics of Information Security (WEIS'05), 2005. http://infosecon.net/workshop/pdf/23.pdf (дата обращения 02.04.2015).
11. **Hoo K. J. S.** How Much is Enough? A Risk-Management Approach to Computer Security: PhD thesis. — Stanford University, June 2000. — 99 p.
12. **Grenadillo G. G., Debar H., Jacob G., Achemlal C. G. M.** Individual Countermeasure Selection Based on the Return on Response Investment Index // Lecture Notes in Computer Science. 2012. Vol. 7531. P. 156–170.
13. **Waltermire D., Quinn S., Scarfone K., Halbardier A.** The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2. Sept. 2011. http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf (дата обращения: 02.04.2015).
14. **Common** Configuration Enumeration (CCE): http://cce.mitre.org/ (дата обращения: 02.04.2015).
15. **Common** Vulnerabilities and Exposures (CVE): http://cve.mitre.org/ (дата обращения: 02.04.2015).
16. **X-Force:** http://xforce.iss.net/ (дата обращения: 02.04.2015).
17. **Федорченко А. В., Чечулин А. А., Котенко И. В.** Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных систем и сетей // Информационно-управляющие системы. 2014. № 5. С. 72–79.
18. **Mell P., Scarfone K.** A Complete Guide to the Common Vulnerability Scoring SystemVersion 2.0, 2007. — 23 p.
19. **Котенко И. В., Степашкин М. В., Дойникова Е. В.** Анализ защищенности автоматизированных систем с учетом социо-инженерных атак // Проблемы информационной безопасности. Компьютерные системы. 2011. № 3. С. 40–57.
20. **Котенко И. В., Новикова Е. С.** Визуальный анализ для оценки защищенности компьютерных сетей // Информационно-управляющие системы. 2013. № 3. С. 55–61.

UDC 004.056
doi:10.15217/issn1684-8853.2015.3.60

Countermeasure Selection in Security Management Systems

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

Purpose: Manual processing of security-related information can result in omitting important aspects and, finally, in taking inefficient countermeasures. The aim of this research is the automation of countermeasure selection by security-related information processing. **Results:** The technique is developed for countermeasure selection in the process of managing security information and events. This technique is based on a newly proposed integrated system of security metrics representing the security state of the system. For countermeasure selection, the system of security metrics is extended with an additional level of decision support. The new level is based on the metrics of countermeasure effectiveness. The key features of the proposed technique include using graphs of attacks and service dependencies, applying the suggested countermeasures and security metrics, and also the possibility to give a countermeasure decision at any time, according to the current information on security state and events. **Practical relevance:** The developed technique can help to improve the efficiency of decision-making in the systems of security information and event management.

Keywords — Security Incidents, Monitoring, Response, Security Metrics, Countermeasure Selection, Attack Graphs, Graphs of Service Dependencies.

References

1. *MASSIF FP7 Project. MAnagement of Security information and events in Service Infrastructures.* Available at: http://www.massif-project.eu (accessed 02 April 2015).
2. Kotenko I. V., Saenko I. B., Polubelova O. V., Chechulin A. A. Application of Security Information and Event Management Technology for Information Security in Critical Infrastructures. *Trudy SPIIRAN*, 2012, iss. 1(20), pp. 27–56 (In Russian).
3. Kotenko I. and Doynikova E. Security Assessment of Computer Networks based on Attack Graphs and Security

Events. *Proc. of the 2014 Asian Conf. on Availability, Reliability and Security, LNCS*, 2014, pp. 462–471.
4. McGuire G. T., Waltermire D., Baker J. O. Common Remediation Enumeration (CRE) Version 1.0 (Draft). *NIST Interagency Report 7831 (Draft)*, National Institute of Standards and Technology, December 2011. 33 p.
5. Johnson C. Enterprise Remediation Automation. *Proc. of the IT Security Automation Conf.*, September 27–29, 2010. NIST. Available at: http://csap.nist.gov/events/2010/itsac/resentations/day1/Automation_Specifications-Enterprise_Remediation_Automation.pdf (accessed 02 April 2015).
6. Kotenko I., Stepashkin M. Attack Graph based Evaluation of Network Security. *Proc. of the 10th IFIP Conf. on Communications and Multimedia Security (CMS'2006)*, Heraklion, Greece, 2006, pp. 216–227.
7. Kheir N. *Response Policies and Counter-Measures: Management Ofservice Dependencies and Intrusion and Reaction Impacts*. PhD thesis. Ecole Nationale Supérieure des Télécommunications de Bretagne, 2010. 229 p.
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, no. 1, pp. 61–74.
9. Balepin I., Maltsev S., Rowe J., Levitt K. Using Specification-Based Intrusion Detection for Automated Response. *Proc. of 6th International Symp., RAID 2003*, Pittsburgh, PA, USA, September 8–10, 2003. Lecture Notes in Computer Science, 2003, pp. 136–154.
10. Cremonini M. and Martini P. Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). *Workshop on the Economics of Information Security (WEIS'05)*, 2005. Available at: http://infosecon.net/workshop/pdf/23.pdf (accessed 02 April 2015).
11. Hoo K. J. S. *How Much is Enough? A Risk-Management Approach to Computer Security*. PhD thesis. Stanford University, June 2000. 99 p.
12. Grenadillo G. G., Debar H., Jacob G., Achemlal C. G. M. Individual Countermeasure Selection Based on the Return on Response Investment Index. *Lecture Notes in Computer Science*, Springer-Verlag, 2012, vol. 7531, pp. 156–170.
13. Waltermire D., Quinn S., Scarfone K., Halbardier A. *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*. September 2011. Available at: http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf (accessed 02 April 2015).
14. *Common Configuration Enumeration (CCE)*. Available at: http://cce.mitre.org/ (accessed 02 April 2015).
15. *Common Vulnerabilities and Exposures (CVE)*. Available at: http://cve.mitre.org/ (accessed 02 April 2015).
16. *X-Force*. Available at: http://xforce.iss.net/ (accessed 02 April 2015).
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. Mell P., Scarfone K. *A Complete Guide to the Common Vulnerability Scoring System Version 2.0*. 2007. 23 p.
19. Kotenko I. V., Stepashkin M. V., Doynikova E. V. Protection Analysis of Information Systems Taking into Account Social Engineering Attacks. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 2011, no. 3, pp. 40–57 (In Russian).
20. Kotenko I. V., Novikova E. S. Visual Analysis of Computer Network Security Assessment. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2013, no. 3, pp. 55–61 (In Russian).