Пескова Ольга Юрьевна – e-mail: poy@tgn.sfedu.ru; кафедра безопасности информационных технологий; к.т.н.; доцент.

Polovko Ivan Yur'evich – Southern Federal University; e-mail: i.y.polovko@gmail.com; 2, Chekhova street, Taganrog, 347928, Russia; phone: +78634371905; the department of security of information technologies; cand. of eng. sc.; assistant professor.

Peskova Olga Yur'evna – e-mail: poy@tgn.sfedu.ru; the department of security of information technologies; cand. of eng. sc.; associate professor.

УДК 004.056.57:004.056.53

Е.С. Абрамов, М.А. Кобилев, Л.С. Крамаров, Д.В. Мордвин

ИСПОЛЬЗОВАНИЕ ГРАФА АТАК ДЛЯ АВТОМАТИЗИРОВАННОГО РАСЧЕТА МЕР ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ

Представлены результаты разработки метода автоматизированного расчета мер противодействия угрозам информационной безопасности сети с использованием графа атак. Описывается алгоритм построения графа атак определенной структуры для оценки уязвимости сети и помощи в более качественном автоматизированном расчете мер противодействия данным уязвимостям. Предлагается алгоритм автоматизированного расчета контрмер, использующий модель сети и взаимодействие с администратором сети (экспертом), обладающим знаниями о специфике сети. Выделяются 11 векторов противодействия уязвимостям. Эксперт осуществляет выбор из предложенных контрмер, для которых предварительно рассчитываются результаты применения и влияние на общую защищённость. Таким образом, применение моделирования позволяет оптимально и с меньшим количеством ошибок распределить правила между межсетевыми экранами, а также скорректировать расположение самих экранов. В результате эксперт может сформировать инструкцию применения контрмер в реальной сети, которая должна стать частью документированной политики информационной безопасности.

Уязвимости; угрозы информационной безопасности; многостадийные атаки; сетевые атаки; контрмеры; межсетвые экраны; системы обнаружения вторжений; CVSS; CVE; IDS; IPS; firewall.

E.S. Abramov, M.A. Kobilev, L.S. Kramorov, D.V. Mordvin

DESIGN OF COUNTERMEASURES FOR SECURITY RISKS OF ENTERPRISE NETWORKS BY USING ATTACK GRAPHS

The article presents the results of the method for automated calculation of countermeasures for network information security threats using attack graph. It describes an algorithm for constructing the attack graph for network vulnerability assessment and for helping in higher quality automated calculation of countermeasures against these vulnerabilities. We propose an algorithm for automated analysis of countermeasures , using a network model and interaction with the network administrator (security executive council), who has knowledge about the specifics of the given network. Allocated 11 vectors counteract vulnerabilities. SEC carries a selection of proposed countermeasures with the pre- calculated results of its application and impact on the overall security. Thus, the use of simulation allows optimal and errorless firewall rules distribution between the firewalls. As a result, the expert can generate instruction of countermeasures in the real network, which should become part of a documented information security policy.

Vulnerabilities; threats to information security; multi-stage attacks; network attacks; countermeasures; intrusion detection systems; CVSS; CVE; IDS; IPS; firewall.

Введение. Компьютерные сети играют важную роль во многих областях. Успешные кибер-атаки приводят к значительным финансовым, имиджевым и иным убыткам и провоцируют рост числа потенциальных злоумышленников. Растущие требования приводят к усложнению структуры и увеличению размера сетей, что, в свою очередь, ведёт к росту сложности анализа их безопасности и запаздыванию применения контрмер. При этом, процесс анализа безопасности до сих пор основан преимущественно на экспертном подходе и носит субъективный характер, т.е. зависти от квалификации конкретного администратора безопасности, особенно в части выработки контрмер. Это делает актуальным продолжение исследований и практических разработок в области автоматизированного анализа защищенности компьютерных сетей.

Один из подходов к анализу безопасности сети состоит в моделировании атак и оценке воздействий вредоносного воздействия на основе графов атаки (деревьев атак) [1]. Атака представляется в виде графа, который содержит все возможные последовательности действий злоумышленника, приводящие к целям воздействия путём последовательной (многостадийной) эксплуатации уязвимостей. Построение полного графа атаки для сколь-нибудь большой сети (от нескольких сотен хостов), и , в особенности, его динамическое изменение, является задачей высокой вычислительной сложности, и делает эту технологию трудноприменимой для использования в системах обнаружения вторжений реального времени. В то же время, в задачах, не требующих мгновенного принятия решений, таких как прогнозирования и анализ защищённости, применение данной технологии представляется весьма перспективным.

Рамки статьи ограничены описанием предлагаемого метода автоматизированной генерации мер противодействия на основе разработанного метода расчёта графа атак. Рассмотрен также алгоритм оценки последствий применения контрмер. Такие важные вопросы, как собственно построение модели сети, метод построения графа атак, оптимизация расчёта графа атак, рассматриваются в других публикациях [1–4].

Статья организованна следующим образом. В первой части даны ключевые понятия анализа и катологизации уязвимостей программного обеспечения, а также принципы построения и использования графов атак. Вторая часть описывает методы использования модели сети для расчета контрмер и предлагаемые авторами вектора практических контрмер. В третьей части предлагается алгоритм автоматизированного расчета контрмер, использующий граф атак и взаимодействие с экспертом, осуществляющим выбор из предложенных контрмер, для которых предварительно рассчитываются результаты применения и влияние на общую защищённость. В разделе выводов дана краткая характеристика полученных результатов и основные направления будущей работы.

1. Уязвимости в сети. Граф атак, принципы построения. Для упорядоченного описания известных уязвимостей программного обеспечения используется система CVE [5]. Метрики для оценки последствий эксплуатации уязвимостей построены на основе «Общей системы оценки уязвимостей (CVSS)» [6]. Система оценки CVSS состоит из 3 метрик: базовая метрика, временна́я метрика и контекстная метрика. Каждая метрика представляет собой число (оценку) в интервале от 0 до 10 и вектор – краткое текстовое описание со значениями, которые используются для вывода оценки. Базовая метрика отображает основные характеристики уязвимости. Временная метрика соответствует таким характеристикам уязвимости, которые изменяются со временем, а контекстная метрика – характеристикам, которые уникальны для среды пользователя.

Использование CVSS предоставляет следующие возможности:

- Стандартизованная оценка уязвимостей. После нормализации оценок уязвимостей для всех программных и аппаратных платформ можно использовать единую политику управления уязвимостями.
- Открытость системы. Использование CVSS позволяет каждому увидеть индивидуальные особенности уязвимости, которые привели к указанной оценке.
- Приоритезация рисков. Как только для уязвимости вычислена контекстная метрика, оценка этой уязвимости становится зависимой от среды. Это означает, что полученная оценка отражает реальный риск от наличия этой уязвимости.

Граф атак (attack graph) – это граф, который представляет все возможные последовательности действий злоумышленника, приводящих его к поставленным целями. Эти многостадийные последовательности также называют трассами атак (attack traces). В данной работе мы предлагаем использовать предварительный расчет графа атак для последующей оптимизации расчета контрмер.

Граф атак в нашей системе – это направленный граф, который строится на основе модели сети, доступных уязвимостей и предусловий эксплуатации уязвимостей, рис. 1 [1, 7].

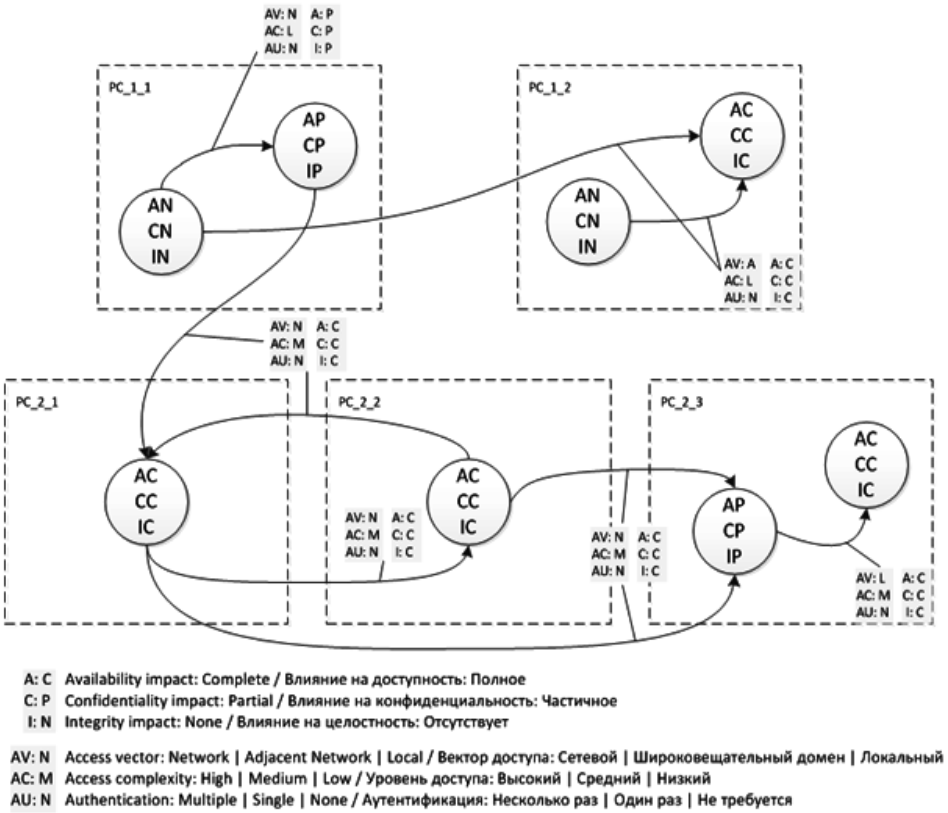

Рис. 1. Пример построения графа атак

Узлом графа является состояние отдельного хоста, возникающее в случае успешной эксплуатации уязвимости (*состояние опасности*). Состояние опасности представлено параметрами конфиденциальности, целостности и доступности. Один и тот же хост может присутствовать в графе несколько раз с разными со-

стояниями опасности. Это достигается путем эксплуатации различных уязвимостей сервисов хоста. Разные состояния опасности одного хоста могут достигать разными траекториями на графе.

Ребрами графа являются связи между исходным состоянием опасности одного хоста и целевым состоянием уязвимости (состоянием опасности) другого хоста. Исходное состояние опасности первого хоста является предусловием эксплуатации следующей уязвимости. Источниками в графе являются состояния нулевой опасности отдельных хостов. Эти узлы в графе необходимы для проведения ребер к узлам, образованным эксплуатацией уязвимостей, не имеющих предусловий состояния опасности источника атаки.

Граф атак строится для всей сети сразу, он учитывает реальную достижимость между сервисами в сети.

2. Использование модели сети для расчета контрмер. Использование компьютерного моделирования целевой сети может существенно упростить расчет и анализ защищенности сети, а также позволит произвести обоснованный расчет мер противодействия угрозам и уязвимостям сети. Модель сети строится на основе сканирования целевой сети или вручную администратором.

В модели сети, разработанной в рамках данного исследования, каждый сервис определяется его уникальным CPE-кодом. Такой подход позволяет для каждого сервиса (его конкретной версии) определить его уязвимости и их опасность. В разработке используется открытая база NVD [8], которая хранит информацию о большинстве практически используемых сервисов (CPE-код), их уязвимостях (CVE-коды) и их CVSS-метриках.

Модель карты сети включает связность, маршрутизацию, фильтрацию, возможность расчета доступа между узлами и сервисами [1, 7, 9, 10, 11].

Таким образом, на компьютерной модели может быть рассчитан и отображен доступ ко всем уязвимым сервисам. Какие-то уязвимости могут быть недоступны из недоверенных сегментов сети и, следовательно, будут нести меньшую опасность, при том, что у них будут высокие значения CVSS-метрик.

На модели сети можно автоматически посчитать общую опасность уязвимостей [12], оценить распределение уязвимостей между хостами и подсетями.

Возможность предварительного применения контрмер на модели позволяет:

- заранее оценить их влияние на общую защищенность сети;
- оптимально распределить правила между фильтрами в сети, а также само расположение фильтров;
- сформировать инструкцию применения контрмер в реальной сети, где все меры будут описаны последовательно, какие-то меры могут быть объединены в группы (новые списки фильтрации для всех фильтров).

Меры противодействия использованию уязвимостей

Контрмеры, направленные на сам сервис

1. *Удаление уязвимого сервиса*. Возможно, сервис, обладающий известной уязвимостью, на самом деле не используется и может быть удален. Эта самая простая ситуация, но её стоит учитывать в первую очередь.

2. *Установка обновлений для ликвидации уязвимости*. Возможно, уязвимость легко устранить при помощи установки обновлений для текущей версии сервиса. Наличие такого обновления можно проверить с помощью открытых баз данных.

3. *Замена сервиса на другую версию, без уязвимостей*. Наличие новой версии (или предыдущей) и наличие в ней уязвимостей можно проверить с помощью открытых баз данных. Но даже при наличии другой версии решение о её установке

должен принимать эксперт. Стабильная версия сервиса может не обладать обратной совместимостью или иной бизнес-спецификой, которая станет препятствием для замены. В этом случае стоит выбирать иную контрмеру для противодействия уязвимости сервиса.

4. *Замена сервиса на альтернативный, без уязвимостей*. Информацию о возможной взаимозаменяемости сервисов можно искать в открытых источниках или специально подготовить в собственной базе. Но аналогично вышеописанной контрмере, решение о применение такой меры может принять только администратор. Такая замена может быть возможно не всегда.

5. *Замена сервиса на другую версию с уязвимостью, эксплуатация которой приводит к состоянию меньшей опасности, чем текущая версия сервиса*. Альтернативная версия сервиса, пригодная для замены, может так же обладать уязвимостью. При этом уязвимость альтернативной версии может обладать меньшей опасностью, что можно оценить по открытым источникам.

6. Замена сервиса на альтернативный с уязвимостью, эксплуатация которой приводит к состоянию меньшей опасности, чем текущая версия сервиса.

Контрмеры, направленные на доступ к сервису

7. *Использование фильтрации, для ограничения доступа к сервису от всех узлов сети, от которых он является необязательным*. Возможно, доступ к уязвимому сервису открыт для большего количества источников, чем это действительно необходимо. Сократив доступ с помощью добавления межсетевого экрана или редактирования правил фильтрации, можно повысить общую защищенность сети.

8. *Перенастройка правил маршрутизации для ограничения доступа к сервису от всех узлов сети, от которых он является необязательным*. Изменением правил можно перенаправить отдельный трафик в обход уязвимых маршрутизаторов, подсетей.

9. *Использование NAT (DMZ), для ограничения доступа к сервису от всех узлов сети, от которых он является необязательным*.

Другие контрмеры

10. *Использование системы предотвращения вторжений (IPS).* При рассмотрении возможности использования IPS необходимо оценить возможность противодействия рассматриваемой уязвимости. Эту задачу можно решить, анализируя описания правил системы предотвращения вторжений. Так же существует задача оптимального расположения таких систем для минимизации их необходимого количества. Применение такой системы, вероятно, является самой дорогостоящей и сложной в реализации контрмерой, но, с другой стороны, такой подход не требует изменять сервисы.

11. Устранение противоречий между правилами фильтрации межсетевых экранов в сети [9–11].

В документе Национального института стандартов и технологий "Security and Privacy Controls for Federal Information Systems and Organizations" [12], предоставлен полный набор элементов управления и базовых функций обеспечения безопасности, а также руководство по адаптации этих рекомендаций для конкретных условий эксплуатации и применяемых технологий. Предлагаемые контрмеры покрывают следующие семейства требований:

- Access Control (AC-4, AC-17, AC-18, AC-19, AC-20, AC-21);
- Security Assessment and Authorization (CA-3);
- Configuration Management (CM-10, CM-11);
- Risk Assessment RA-1, RA-2, RA-3, RA-5;
- System and Communications Protection (SC-1, SC-3, SC-5, SC-7, SC-10, SC-11, SC-14);
- Risk Management Strategy (PM-9).

3. Применение графа для оценки эффекта выбранных контрмер. Использование граф атак позволяет улучшить расчет контрмер на модели сети.

Граф показывает все возможные пути атак, которые приводят к эксплуатации рассматриваемой уязвимости, а также атаки, которые возможны после эксплуатации рассматриваемой уязвимости.

С помощью графа учитываются только уязвимости, которые можно проэксплуатировать. Таким образом, показывается общее количество возможных атак. Граф атак позволяет оценивать защищенность сети, используя различные агрегированные метрики опасности на основе общего количества уязвимостей, их CVSS метрик, достижимости уязвимостей и т.д. [13].

Использование графа при расчете контрмер даёт следующие возможности:

- Можно не принимать во внимание те уязвимости, которые не могут быть проэксплуатированы в текущей конфигурации сети.
- Акцентировать внимание на тех уязвимостях, которые являются частью эксплуатации большего количества атак. Возможно, для таких уязвимостей стоит применить сложно реализуемые контрмеры, если простые в реализации отсутствуют (рассматривать возможность полного отказа от сервиса или его замену на альтернативный).
- При рассмотрении замены уязвимого сервиса на другой уязвимый (альтернативный или другой версии), можно увидеть, как такая замена отразится на графе атак. Возможно с альтернативным сервисом, даже с большей CVSS метрикой, но по-другому распределенными метриками целостности, конфиденциальности и доступности, граф уменьшится. Это произойдёт в том случае, если не будет выполнено предусловие состояния опасности для атаки, которая может быть продолжена с хоста с рассматриваемой уязвимостью.
- При применении новых правил фильтрации можно учитывать источники атак, которые содержит граф. Если можно заблокировать доступ к уязвимому сервису помощью фильтрации, то это будет легко реализуемая и надежная контрмера. То же самое касается маршрутизации. Это особенно актуально для публичных сервисов. Проанализировав пример на рис. 2 можно увидеть, что для решения проблемы уязвимости сервиса на хосте 10.1.2.1/24 достаточно будет с помощью нового правила фильтрации заблокировать доступ к сервису с хоста 10.1.3.1/24. Только проэксплуатировав уязвимость на этом хосте, злоумышленник получает возможность добраться до уязвимости 10.1.2.1/24. Стоит учесть, что запретить доступ можно, если это не противоречит бизнес правилам в сети.
- Граф позволяет выявить такие ситуации, когда на одном хосте содержатся несколько уязвимостей, которые эксплуатируются последовательно, развивая многостадийную атаку (например, локальная и сетевая уязвимости). Тогда возможно применение такой контрмеры, как разделение уязвимых сервисов по разным хостам. Такая мера прервет развитие сценария атаки и не позволит достичь конечной цели. На рис. 3 показана ситуация до и после применения контрмеры. Изначально хост 10.1.2.3/24 содержит одну сетевую и одну локальную уязвимость. Расчет графа показал, что эксплуатировать локальную уязвимость можно только после эксплуатации сетевой. Эксплуатация локальной уязвимости приводит хост в более опасное состояние. После применения контрмеры, локальный сервис был перенесен на другой хост, к которому нет доступа из источника атаки, и который не обладает другими уязвимостями. Повторный перерасчет графа показывает, что эксплуатация данной уязвимости стала невозможна.

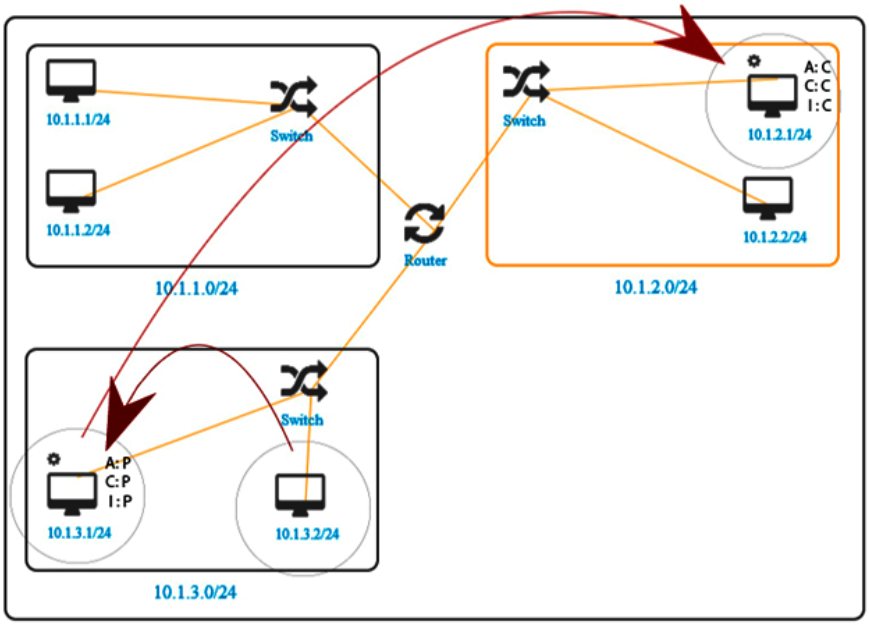

Рис. 2. Пример отображения части графа с многостадийной атакой до реализации контрмер

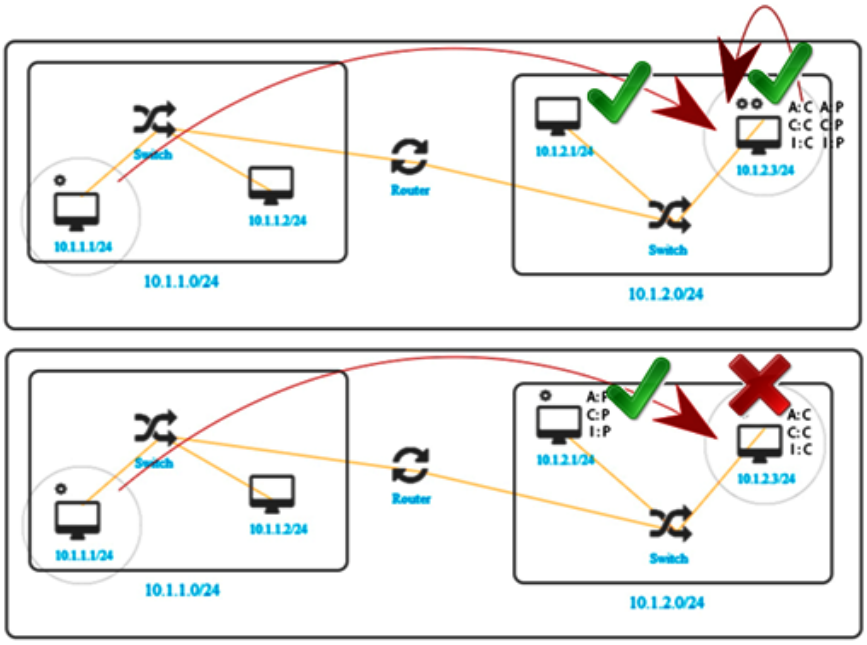

Рис. 3. Пример графа атак до и после применения контрмеры

Алгоритм автоматизированного расчета контрмер. Для разработанной системы предлагается следующий комплексный алгоритм.

1. Сбор информации о целевой сети.
2. Компьютерное моделирование сети.

3. Расчет достижимости между узлами в сети на основе маршрутизации и правил фильтрации.
4. Расчет графа атак в сети.
5. Последовательное отображение администратору уязвимых узлов, ранжированных по определенной метрике. Метрика учитывает опасность состояния на хосте после эксплуатации, количество атак в графе, которые приводят к эксплуатации данной уязвимости, количество атак, которые продолжаются после эксплуатации данной уязвимости.
6. Представление эксперту контрмер для рассматриваемой уязвимости для выбора оптимальной.

6.1. Если есть обновление для сервиса, устраняющее уязвимости, предлагается его применение.
6.2. Иначе предлагается удалить сервис.
6.3. Иначе предлагается замена сервиса на иную версию, если таковая есть, и у неё нет уязвимостей.
6.4. Иначе предлагается автоматическая доработка правил фильтрации для ограничения доступа источников атак, если между источниками и сервисом есть межсетевые экраны.
6.5. Иначе предлагается автоматическая доработка правил маршрутизации для ограничения доступа источников атак, если это возможно.
6.6. Иначе предлагается вынести сервис на отдельный хост (если на рассматриваемом хосте имеются еще уязвимости, а текущая уязвимость является предусловием для их эксплуатации).
6.7. Иначе предлагается добавить новый межсетевой экран в модель и применить на нем правила для ограничения доступа.
6.8. Иначе предлагается замена сервиса на аналог, если такой есть, и у него нет уязвимостей.
6.9. Иначе предлагается замена сервиса на другую версию, имеющую уязвимости, эксплуатация которых приводит к менее опасному состоянию.
6.10. Иначе предлагается замена сервиса на аналог, имеющий уязвимости, эксплуатация которых приводит к менее опасному состоянию.

Выводы. Даны ключевые понятия анализа и катологизации уязвимостей программного обеспечения, а также принципы построения и использования графов атак. Описаны методы использования модели сети для расчета контрмер и предлагаемые авторами вектора практических контрмер. Предложен алгоритм автоматизированного расчета контрмер, использующий граф атак и взаимодействие с экспертом, осуществляющим выбор из предложенных контрмер, для которых предварительно рассчитываются результаты применения и влияние на общую защищённость.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Абрамов Е.С., Андреев А.В., Мордвин Д.В.* Применение графов атак для моделирования сетевых воздействий // Известия ЮФУ. Технические науки. – 2012. – № 1 (126). – С. 165-174.
2. *Kotenko I.; Chechulin A.A.* Cyber Attack Modeling and Impact Assessment Framework. 5th International Conference on Cyber Conflict (CyCon), 2013. http://ieeexplore.ieee.org/xpl/abstractReferences.jsp?arnumber=6568374.
3. *Ingols K., Lippmann R. and Piwowarski K.* Practical attack graph generation for network defense // in ACSAC. IEEE Computer Society. – 2006. – P. 121-130.
4. *Williams L., Lippmann R. and Ingols K.* GARNET: A graphical attack graph and reachability network evaluation tool // in Visualization for Computer Security (VizSEC), ser. Lecture Notes in Computer Science, J.R. Goodall, G.J. Conti, and K.-L. Ma, Eds. – Springer, 2008. – Vol. 5210. – P. 44-59.
5. “Common Vulnerabilities and Exposures (CVE)” http://cve.mitre.org/, Feb. 2013.

6. *Mell P., Scarfone K., Romanosky S.* Common Vulnerability Scoring System (CVSS). http://www.first.org/cvss/cvss-guide.html, Feb. 2013.
7. *Andreev A.V., Mordvin D.V., Abramov E.S., Makarevich O.B.* Corporate networks security evaluation based on attack graphs // In Proceedings of the 4rd international conference on Security of information and networks (SIN '11). ACM, New York, NY, USA.
8. National Institute of Standards and Technology, "National Vulnerability Database, NVD", http://nvd.nist. gov, Feb. 2013.
9. *Mordvin D.V., Abramov E.S., Makarevich O.B.* Automated method for constructing of network traffic filtering rules // In Proceedings of the 3rd international conference on Security of information and networks (SIN '10). ACM, New York, NY, USA, http://doi.acm.org/10.1145/1854099.1854141. – P. 203-211.
10. *Абрамов Е.С., Андреев А.В., Мордвин Д.В*. Методы автоматизации построения правил фильтрации сетевого трафика // Информационное противодействие угрозам терроризма. – 2010. – № 14. – С. 121-127.
11. *Абрамов Е.С., Андреев А.В., Мордвин Д.В*. Метод и алгоритмы построения правил разграничения доступа между узлами сети // Информационное противодействие угрозам терроризма. – 2010. – № 14. – С. 127-132.
12. National Institute of Standards and Technology, "Security and Privacy Controls for Federal Information Systems and Organizations", http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf, Feb. 2013.
13. Anoop Singhal, Ximming Ou, NIST Interagency Report 7788 "Quantitative Security Risk Assessment of Enterprise Networks" http://csrc.nist.gov/publications/nistir/ir7788/NISTIR-7788.pdf, Feb. 2013.

Статью рекомендовал к опубликованию к.т.н. М.Н. Казарин.

Абрамов Евгений Сергеевич – Южный федеральный университет; e-mail: abramoves@sfedu.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634371905; кафедра безопасности информационных технологий; зав. кафедрой.

Кобилев Максим Андреевич – e-mail: mkobilev@gmail.ru; кафедра безопасности информационных технологий; студент.

Крамаров Леонид Сергеевич – e-mail: l.s.kramarov@gmail.com; кафедра безопасности информационных технологий; аспирант.

Мордвин Денис Валериевич – e-mail: denismordvin@sfedu.ru; кафедра безопасности информационных технологий; доцент.

Abramov Evgeny Sergeevich – Southern Federal University; e-mail: abramoves@sfedu.ru; 2, Chekhova street, Taganrog, 347928, Russia; phone: +78634371905; the department of security in data processing technologies; head of the department.

Kobilev Maxim Andreevich – e-mail: mkobilev@gmail.ru; the department of security in data processing technologies; student.

Kramarov Leonid Sergeevich – e-mail: l.s.kramarov@gmail.com; the department of security in data processing technologies; student.

Mordvin Denis Valerievich – e-mail: denismordvin@sfedu.ru; the department of security in data processing technologies; associate professor.