УДК 004.934.2

Л.Р. Тулиганова, И.А. Павлова, И.В. Машкина

РАЗРАБОТКА МОДЕЛЕЙ ОБЪЕКТА ЗАЩИТЫ И УГРОЗ НАРУШЕНИЯ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ, БАЗИРУЮЩЕЙСЯ НА ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ

Предлагается структурная вербальная модель, включающая в себя четыре вида ресурсов. Ставится и решается задача анализа и организации информации об инфраструктуре и сервисах виртуального сегмента информационной системы как объекте защиты. Разработана структурная вербальная модель угроз нарушения безопасности, реализующихся в виртуальном сегменте. Формат модели определяет сведения об объектах атак, источниках угроз, о структуре угрозы, пути ее распространения, возможных последствиях. Рассматриваются угрозы, которые приводят к перехвату управления в среде виртуализации за счет нарушения процедуры аутентификации субъектов доступа к виртуальной среде, несанкционированного доступа к средствам виртуализации, к образам виртуальных машин, к гипервизору, атак на виртуальное аппаратное обеспечение – со стороны пользователей физической сети информационной системы, пользователей виртуальной сети, работающих с экземплярами на одном и том же физическом сервере и на разных физических серверах.

Технология виртуализации; модель объекта защиты; структурная вербальная модель; моделирование угроз.

L.R. Tuliganova, I.A. Pavlova, I.V. Mashkina

DEVELOPMENT OF THE MODELS OF THE PROTECTION OBJECT AND SECURITY THREATS IN THE INFORMATION SYSTEM, BASED ON VIRTUALIZATION TECHNOLOGY

Offers structural verbal model that includes four types of resources. Pose and solve the problem of analysis and organization of information on the infrastructure and services virtual segment information system as the object of protection. Developed structural verbal model of security threats implemented in virtual segment. The model format specifies information about the objects of attacks, the threats, the structure of the threat, the ways of its distribution, the possible consequences. Discusses threats that lead to the seizure of control in a virtualization environment at the expense of: violations of the procedure of authentication of subjects of access to the virtual environment, unauthorized access to means of virtualization, virtual machine images, to the hypervisor, attacks on virtual hardware – user physical network information system, users of the virtual network, working with instances on the same physical server and on different physical servers.

Virtualization technology; model of the object of protection; structural verbal model; threat modeling.

В настоящее время в сфере информационных технологий наиболее эффективно развивается *технология виртуализации*. Эта инновационная технология используется компаниями не только для хранения данных, но и для обработки конфиденциальной информации в виртуальной инфраструктуре. Различные предприятия и организации внедряют технологию виртуализации в свои информационные системы, что позволяет обеспечить непрерывность бизнес процессов за счет повышения доступности информации.

Главная проблема использования технологии виртуализации – это защита информации. Существует необходимость учитывать риски использования механизмов виртуализации с учетом особенностей виртуальной среды. Это вызывает необходимость разработки модели объекта защиты – виртуального сегмента информационной системы (ВСИС) компании и разработки модели угроз нарушения

информационной безопасности. Решение этих задач позволит сделать адекватный выбор средств и механизмов защиты, оценить риски использования технологии виртуализации.

Моделирование является эффективным инструментом исследования характеристик сложных систем обеспечения информационной безопасности (СОИБ) на этапе их проектирования и при модернизации. Успех создания СОИБ в значительной мере зависит от адекватности модели объекта защиты и модели угроз. В первую очередь требуется наличие большого объема информации о самом объекте защиты – виртуальном сегменте информационной системы компании. Чем выше уровень организации информации об объекте защиты, тем меньше уровень неопределенности при разработке модели угроз, необходимой в ходе проектирования СОИБ.

В данной работе на основе нормативных документов (приказов №17, №21 ФСТЭК, проекта ГОСТ «Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации. Основные положения») приведены исследования по разработке структурных вербальных моделей сегмента виртуализации и угроз нарушения безопасности виртуальной среды.

Описание объекта защиты на профессиональном языке, создаваемое для определения и исследования его свойств, представляет *вербальную* модель, при этом в модели учитываются существенные элементы и связи объекта. Вербальная модель ВСИС как объекта защиты создается на основе целенаправленного накопления, анализа, организации информации и ее структурирования: это сведения о физической инфраструктуре сегмента и виртуальной инфраструктуре, сведения об используемых в процессе информационного взаимодействия операционных системах и приложениях. Для ВСИС характерно использование средств виртуализации, обеспечивающих динамическую масштабируемость вычислительных ресурсов и возможность самообслуживания потребителей. Использование средств виртуализации, как и других особенностей ВСИС, приводит к появлению новых потенциально возможных угроз нарушения информационной безопасности, которые будут являться специфическими для виртуальных сред [2].

Предлагаемая *структурная вербальная модель* ВСИС включает в себя четыре компонента, в соответствии с четырьмя типами ресурсов: средства вычислительной техники, информационные технологии, информационные ресурсы, аппаратуру, каналы и линии связи, – и позволяет наиболее полно описать объект защиты. В модели предлагается структурирование каждого типа ресурсов объекта защиты.

К элементам вычислительной системы относятся: рабочие станции администратора виртуализации и администратора безопасности; терминалы пользователей сегмента виртуализации; кластер выделенных физических серверов; физические серверы, на которых запускаются виртуальные машины; физические серверы, на которых запускается сервер хранения данных (Storage system server); другие аппаратные средства, используемые для реализации технологий виртуализации.

Ко второму типу ресурсов относятся элементы информационных технологий: гипервизоры; экземпляры виртуальных машин; виртуальные средства защиты информации; хостовые и гостевые операционные системы; системы управления базами данных; виртуальные серверы, виртуальные процессоры, виртуальные диски, виртуальная память; web-технологии; прикладное программное обеспечение; сетевые сервисы и протоколы; утилиты архивирования, резервирования; средства централизованного управления гипервизорами в рамках одной виртуальной инфраструктуры и другие.

Третий блок модели – элементы информационных ресурсов. К ним относятся: базы данных; образы виртуальных машин; тома виртуальных машин; резервные копии данных; текстовые, графические, табличные электронные документы; исходные коды программного обеспечения и другие.

В свою очередь элемент информационного ресурса может быть структурирован на элементы информации, содержащие конкретные сведения, которым присвоен тот или иной уровень конфиденциальности и метка бизнес-категоризации.

К элементам аппаратуры и линий связи относятся: маршрутизаторы и коммутаторы 3-го и 2-го уровней, а также виртуальное активное и пассивное сетевое оборудование.

При разработке модели ВСИС учитывались положения проекта ГОСТ [3], сведения о системах Amazone [5], VMWare [6] и другие.

Наличие уязвимостей компонентов виртуальной инфраструктуры может привести к нарушению изоляции гостевых операционных систем и экземпляров виртуальных машин (ВМ) друг от друга при обработке на одном и том же физическом сервере информации с различными метками бизнес-категоризации и разного уровня критичности, что повышает риски нарушения информационной безопасности. Сведения об уязвимостях компонентов инфраструктуры получены из международной базы данных уязвимостей National Vulnerability Database (NVD) [4].

Таким образом, для моделирования ВСИС как объекта защиты предложена следующая табличная форма, которая приведена с примерами заполнения.

Таблица 1

Модель виртуального сегмента информационной системы

№ ресурса	Тип ресурса				
1	Средства вычислительной техники				
№ элемента ресурса	Наименование элемента ресурса	Уровень физического доступа	Поддерживаемые LAN-протоколы	Встроенные сервисы безопасности	Месторасположение элемента ресурса
1.1	Терминалы пользователей виртуальных машин	Сотрудники соответствующего подразделения компании	Ethernet, стек протоколов TCP/IP	Access Control List (ACL), Active Directory (AD), антивирус (AB)	Соответствующие отделы компании
1.2	Web-сервер	Специалисты отдела информационных технологий, администратор безопасности	Ethernet, стек протоколов TCP/IP	ACL, AD, AB	Серверная
1.3	Рабочая станция администратора виртуализации	Администратор виртуализации	Ethernet, стек протоколов TCP/IP	ACL, AD, AB	Сегмент виртуализации
1.4	Физические серверы с запущенными виртуальными машинами (экземплярами)	Администратор безопасности, администратор виртуализации	Ethernet, стек протоколов TCP/IP	ACL, AD, AB	Серверная кластера виртуализации ИС

Продолжение табл. 1

№ ресурса	Тип ресурса				
1.5	Рабочая станция администратора безопасности	Администратор безопасности	Ethernet, стек протоколов TCP/IP	ACL, AD, AB	Сегмент рабочих серверов в сети ИС
1.7	Физический сервер хранения данных (Storage system server)	Администратор безопасности, администратор виртуализации	Ethernet, стек протоколов TCP/IP	ACL, AD, AB	Серверная кластера виртуализации ИС
1.8	Кластер выделенных физических серверов	Администратор безопасности	Ethernet, стек протоколов TCP/IP	ACL, AD, AB	Серверная ИС
2	Информационные технологии				

№ элемента ресурса	Наименование элемента ресурса ОИ		Уязвимости соответствующих прикладных программ	Уровень конфиденциальности		Ценность элемента ресурса	Субъект доступа	Месторасположение элемента ресурса
2.1. Системное ПО (примеры)								
2.1.1	Гипервизоры I типа	Amazone	Отсутствуют в базе данных NVD				Администратор виртуализации	Кластер виртуализации
		vSphere ESXi	CVE-2012-3496, CVE-2012-3494					На сервере VMWare
2.1.2	Хостовые ОС	Windows XP	CVE-2013-0662, CVE-2014-0506, CVE-2014-0323				Администратор безопасности	Физические серверы кластера виртуализации
		Windows 2010	CVE-2013-3906, CVE-2013-3129, CVE-2012-2520					
2.1.3	Гостевые ОС	Windows 7 Professionsl SP1	CVE-2014-0323, CVE-2014-0317				Администратор виртуализации	Пользователи
…								

Продолжение табл. 1

№ ресурса	Тип ресурса						
2.2. Прикладное ПО (примеры)							
2.2.1	Гипервизоры II типа	VMware Workstation 9.0.1	CVE-2014-1208, CVE-2013-1406			Администратор виртуализации	Инфраструктура сегмента виртуализации
2.3. Виртуальные средства безопасности (примеры)							
2.3.1	Виртуальный межсетевой экран					Администратор виртуализации	Периметр виртуальной инфраструктуры
2.3.1	Виртуальные системы обнаружения вторжений						
…							
3	Информационные ресурсы						
№ элемента ресурса	Наименование элемента ресурса	Уровень конфиденциальности	Субъект доступа	Месторасположение элемента ресурса			
3.1	Базы данных пользователей компании		Сотрудники-пользователи виртуальных машин	Хранилище данных SAN/Storage System Server			
3.2	Файлы образов и снимков виртуальных машин		Сотрудники-пользователи виртуальных машин, администратор виртуализации	Хранилище данных SAN/Storage System Server			
3.3	Служебная информация		Администратор виртуализации, администратор безопасности	Рабочая станция администратора виртуализации, администратора безопасности			
3.4	Резервные копии данных физического и виртуального пространства: - журналы событий гипервизора, - журналы событий виртуальных машин		Администратор виртуализации	Хранилище данных SAN/Storage System Server, рабочая станция администратора виртуализации			

Окончание табл. 1

№ ресурса	Тип ресурса			
3.5	Файлы параметров конфигурации (установки, запуска) аппаратных устройств обработки данных и системного ПО		Администратор безопасности	Выделенный сервер, рабочая станция администратора безопасности
3.6	Служебная информация виртуальных устройств		Сотрудники-пользователи виртуальных машин	Рабочая станция пользователя
…				
4	Аппаратура, каналы и линии связи (примеры)			
№ элемента ресурса	Наименование элемента ресурса ОИ	Реализуемая технология	Пропускная способность	Встроенные сервисы безопасности
4.1	Маршрутизаторы			
4.2	Коммутаторы 3-го уровня, 2-го уровня			
4.3	Виртуальные коммутаторы (Cisco Nexus 1000v)			
4.4	Одномодовый оптический кабель (LX)			
4.5	Медная витая пара категории 5 (TX)			
…				

Результаты анализа уязвимостей дают портрет состояния объекта защиты. К примеру, уязвимость CVE-2014-1208 гипервизора VMWare позволяет удаленному пользователю вызвать отказ в обслуживании, перехватывать и вносить изменения в трафик, а CVE-2014-1207 дает возможность считывать или изменять произвольные файлы за счет использования виртуальных машин опытным локальным пользователем или администратором.

Столбцы модели «ценность» заполняются значениями затрат, необходимых на восстановление работоспособности программы или информационного ресурса в случае, если они не являются конфиденциальными. Если используемая технология или актив являются критичными или имеют ограниченный уровень доступа, то в столбце указывается уровень возможного ущерба от потери свойства конфиденциальности.

Принципиальной особенностью проблемы защиты информации в сегменте виртуализации является требование абсолютной полноты выявления возможных угроз. В соответствии с методом декомпозиции системного анализа и алгоритмом проектирования СОИБ [7] методическое обеспечение должно обеспечивать выявление и *моделирование угроз* безопасности информационным ресурсам и технологиям виртуализации. Перед разработкой СОИБ необходимо определить, от чего, собственно, необходимо защищать информацию, т.е. построить модель угроз для данного конкретного ВСИС. Модель угроз должна включать в себя перечень потенциально возможных угроз (исходя из принятой политики безопасности), которые могут воздействовать на информацию в процессе ее обработки.

В работе при построении модели во внимание принимаются преднамеренные угрозы (компьютерные атаки), которые представляют собой целенаправленные действия нарушителя (злоумышленника) по поиску и использованию уязвимостей для нарушения безопасности информации в ВСИС. Создание модели угроз по существу является единственным методом достаточно полного исследования безопасности информации в ВСИС.

В настоящее время неизвестно, сколько реально существует методов атак – преднамеренных угроз. Это связано с тем, что до сих пор отсутствуют серьезные математические исследования в этой области. Можно привести работу Ф. Коэна, близкую по тематике исследований, в которой описываются математические основы вирусной технологии и приводится доказательство бесконечности числа вирусов. Очевидно, эти же результаты можно перенести на область атак, поскольку вирусы являются их подмножеством [8].

Поэтому при моделировании преднамеренных угроз необходимо стремиться к полноте описания всех возможных *путей* их проникновения, а не к описанию бесконечного множества возможных механизмов их реализации. В виртуальных средах это следующие специфические пути вторжения: локальное сетевое вторжение и удаленное вторжение из физической сети, из виртуальной инфраструктуры.

Разработана структурная вербальная модель угроз, реализуемых в информационной системе компании [9]. Очевидной является необходимость построения подобной структурной вербальной модели угроз, формат которой определяет сведения об объектах атак (источниках информации), источниках угроз, о структуре угрозы, путях их распространения в виртуальных средах.

В результате исследования особенностей виртуальных сред, изучения продуктов, реализующих технологию виртуализации, предлагается следующий формат модели (табл. 2)..

Таблица 2

Структурная вербальная модель угроз нарушения безопасности в ВСИС

№ п/п	Источник угрозы	Объект атаки	Ценность элемента ресурса	Уязвимость инфраструктуры	Возможные последствия	Вероятность угрозы
а) Угрозы несанкционированного доступа к средствам виртуализации						
1	Пользователь физической сети	Образы ВМ на диске Storage System		Уязвимость физических барьеров виртуального сегмента	Нарушение работоспособности информационной системы	
2	Пользователь физической сети	Экземпляр ВМ на физическом сервере виртуального сегмента		Уязвимость физических барьеров виртуального сегмента	Нарушение работоспособности виртуальной инфраструктуры. Получение доступа к ВМ со стороны не авторизованного пользователя	

Окончание табл. 2

№ п/п	Источник угрозы	Объект атаки	Ценность элемента ресурса	Уязвимость инфраструктуры	Возможные последствия	Вероятность угрозы
3	Пользователь физической сети	Гипервизор		Уязвимость физического барьера защиты виртуального сегмента. Уязвимость операционной системы, на которой установлен гипервизор	Получение контроля над виртуальным сегментом	
4	Пользователь виртуального сегмента	Образы ВМ на диске Storage System		Уязвимость виртуальных барьеров защиты	Нарушение изоляции пользовательских данных внутри ВМ Получение доступа к ВМ со стороны пользователя другой ВМ	
5	Пользователь виртуального сегмента	Экземпляр ВМ на физическом сервере виртуального сегмента		Уязвимость виртуальных барьеров защиты	Получение доступа к виртуальной машине со стороны пользователя другой виртуальной машины	
6	Пользователь виртуального сегмента	Гипервизор		Уязвимость физических барьеров защиты сервера виртуализации. Уязвимость ОС, на которой установлен гипервизор	Получение контроля над виртуальным сегментом	
б) Угрозы утечки информации						
7	Внутренний нарушитель, обладающий высокими привилегиями	Гипервизор		Уязвимость барьера безопасности виртуального серверного сегмента	Реализация трафика несанкционированным субъектам сети	

Безопасность информационной системы, функционирующей с использованием технологии виртуализации, зависит от безопасности механизмов виртуализации и виртуальной среды. Защита информации в информационной системе заключается в создании барьеров, учете уязвимостей на путях распространения потенциально возможных угроз. Для определения мест расположения барьеров должна быть построена модель угроз.

Моделирование угроз нарушения безопасности информации позволяет специалисту по защите информации получить достаточно убедительные доводы о наличии потенциальных угроз в конкретном ВСИС, что может способствовать финансированию проекта системы обеспечения информационной безопасности в необходимом объеме [10].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Ивонин П.В.* Безопасность в облаках в деталях // Безопасность информационных технологий. – 2013. – № 2. – С. 37-40.
2. *Демурчев Н.Г., Ищенко С.О.* Проблемы обеспечения информационной безопасности при переходе на облачные вычисления // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – 256 с.
3. ГОСТ Р XXXXX – 20XX (проект, первая редакция). Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации. Общие положения. URL: https://drive.google.com/file/d/0B5PXq-icGjzLbTd4LVln (дата обращения 03.04.2014).
4. National Vulnerability Database. URL: http://nvd.nist.gov/ (дата обращения 03.04.2014).
5. *Риз Д.* Облачные вычисления: Пер. с англ. – СПб.: БХВ-Петербург, 2011. – 288 с.
6. *Михеев М.О.* Администрирование VMware vSphere 5. – М.: ДМК Пресс, 2012. – 508 с.
7. *Тихонов В.А., Райх В.В.* Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. – М.: Гелиос АРВ, 2006. – 528 с.
8. *Корт С.С.* Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004. – 240 с.
9. *Машкина И.В.* Управление защитой информации в сегменте корпоративной информационной системы на основе интеллектуальных технологий: Дис. ... д-ра техн. наук. – Уфа, 2009. – 354 с.
10. *Торокин А.А.* Инженерно-техническая защита информации: Учебное пособие. – М.: Гелиос АРВ, 2005. – 960 с.

REFERENCES

1. *Ivonin P.V.* Bezopasnost' v oblakakh v detalyakh [Security in the cloud is in the details], *Bezopasnost' informatsionnykh tekhnologiy* [Information Technology Security], 2013, No. 2, pp. 37-40.
2. *Demurchev N.G., Ishchenko S.O.* Problemy obespecheniya informatsionnoy bezopasnosti pri perekhode na oblachnye vychisleniya [Problems of information security in the transition to cloud computing], *Materialy XI Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Informatsionnaya bezopasnost'»* [Proceedings of the XI International scientific-practical conference "Information security". Part 1. Taganrog: Izd-vo TTI YuFU, 2010, 256 p.
3. GOST R XXXXX – 20 XX (proekt, pervaya redaktsiya) «Zashchita informatsii. Trebovaniya po zashchite informatsii, obrabatyvaemoy s ispol'zovaniem tekhnologii virtualizatsii. Obshchie polozheniya» [State Standard R XXXXX – 20 XX. Protection of information. Requirements for the protection of information processed by using virtualization technology. General provisions]. Available at: https://drive.google.com/file/d/0B5PXq-icGjzLbTd4LVln (accessed 3 April 2014).
4. National Vulnerability Database. Available at: http://nvd.nist.gov/ (accessed 3 April 2014).
5. *Riz D.* Oblachnye vychisleniya [Cloud computing]: Per. s angl. St. Petersburg: BKhV-Peterburg, 2011, 288 p.
6. *Mikheev M.O.* Administrirovanie VMware vSphere 5 [Administering VMware vSphere 5]. Moscow: DMK Press, 2012, 508 p.
7. *Tikhonov V.A., Raykh V.V.* Informatsionnaya bezopasnost': kontseptual'nye, pravovye, organizatsionnye i tekhnicheskie aspekty [Information security: conceptual, legal, organizational and technical aspects]: Uchebnoe posobie [textbook]. Moscow: Gelios ARV, 2006, 528 p.
8. *Kort S.S.* Teoreticheskie osnovy zashchity informatsii [Theoretical basics of information security]: Uchebnoe posobie [textbook]. Moscow: Gelios ARV, 2004, 240 p.

9. *Mashkina I.V.* Upravlenie zashchitoy informatsii v segmente korporativnoy informatsionnoy sistemy na osnove intellektual'nykh tekhnologiy [Management of information security in the corporate information system based on intelligent technologies: Dr. of eng. sc. diss]. Ufa, 2009, 354 p.
10. *Torokin A.A.* Inzhenerno-tekhnicheskaya zashchita informatsii [Engineering and technical protection of information]: Uchebnoe posobie [textbook]. Moscow: Gelios ARV, 2005, 960 p.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Тулиганова Лилия Равилевна – Уфимский государственный авиационный технический университет; e-mail: tulegan@rambler.ru; 450000, Республика Башкортостан, г. Уфа, ул. К. Маркса, 12; тел.: +79374747997; кафедра вычислительной техники и защиты информации.

Павлова Ирина Александровна – e-mail: i_pavlova@list.ru; тел.: +79191489821; кафедра вычислительной техники и защиты информации.

Машкина Ирина Владимировна – e-mail: mashkina_vtzi@mail.ru; тел.: +79279277089; кафедра вычислительной техники и защиты информации.

Tuliganova Liliia Ravilevna – The Ufa State Aviation Technical University; e-mail: tulegan@rambler.ru; 12, K. Marx's street, Ufa, 450000, Russia; phone: +79374747997; the chair of computer facilities and information protection.

Pavlova Irina Aleksandrovna – e-mail: i_pavlova@list.ru; phone: +79191489821; the chair of computer facilities and information protection.

Mashkina Irina Vladimirovna – e-mail: mashkina_vtzi@mail.ru; phone: +79279277089; the chair of computer facilities and information protection.

УДК 004.056.57

Д.А. Катаргин

ОБНАРУЖЕНИЕ МУТАЦИИ УЯЗВИМОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ

Рассматривается методика обнаружения уязвимостей в программном обеспечении (ПО). Актуальность связана с необходимостью своевременного обнаружения уязвимостей в программных продуктах для предотвращения утечки или порчи пользовательских данных. В качестве объекта исследования выступает продукт «MS Office», так как уязвимости, присутствующие в нем, непосредственно влияют на личные документы пользователя. Для обнаружения мутаций уязвимости выявлены модули ПО, которые подвергаются наиболее частой эксплуатации. Для этого используется база уязвимостей NVD и классификаторы уязвимостей CWE. Но ссылки на классификаторы не всегда присутствуют в базе уязвимостей, поэтому была проведена оценка достаточности покрытия для дальнейшего исследования, которая показала, что классификаторы CWE присутствуют в базе для более чем 80 % уязвимостей, начиная с 2009 г. На основании полученных классификаторов из базы NVD была построена карта уязвимостей, из которой были получены векторы атаки: «вверх» – эксплуатация старой уязвимости в новой версии ПО; «вдоль» – эксплуатация уязвимости в смежном модуле, которая распространяется на смежные продукты; «вниз» – эксплуатация уязвимости из новой версии ПО на старой. Также к данным векторам приведены экспериментальные результаты, которые подтвердили положение методики к обнаружению уязвимостей в ПО с закрытым исходным кодом.

Уязвимость; мутация; программное обеспечение; карта уязвимостей.