УДК 004.77+372.862

Кадан А.М., Доронин А.К.

Гродненский государственный университет им. Я. Купалы, г. Гродно, Беларусь

ОБЛАЧНЫЕ ЛАБОРАТОРИИ ДЛЯ ЗАДАЧ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ*

АННОТАЦИЯ

В статье рассматриваются вопросы создания современной образовательной среды в рамках облачного кластера на платформе OpenNebula для подготовки специалистов в области компьютерной безопасности. В центре внимания авторов - создание виртуальных лабораторий для изучения методов тестирования на проникновение. Использование таких лабораторий позволяет сформировать у студентов практические навыки использования методов тестирования на проникновение на примерах объектов различных уровней сложности, а также обеспечивает возможность быстрого изменения инфраструктуры и свойств тестируемых объектов.

КЛЮЧЕВЫЕ СЛОВА

Облачные технологии; OpenNebula; образовательная среда; виртуальные лаборатории; защита информации; компьютерная безопасность; тестирование на проникновение.

Alexander Kadan, Alexey Doronin

Yanka Kupala State University of Grodno, Grodno, Belarus

CLOUD LABORATORIES FOR PROBLEMS PENETRATION TESTING

ABSTRACT

In the article the creation of a modern educational environment on the platform of the cloud cluster Open Nebula for the training of specialists in the field of information security and computer security is discussed. The creation of virtual laboratories for studies methods for penetration testing in center attention of authors. The use of such laboratories allows to teach students methods of penetration testing on examples of objects of different levels of difficulty, and also provides the possibility of rapid infrastructure changes and the properties of the research objects.

KEYWORDS

Cloud technologies; OpenNebula; educational environment; virtual laboratories; data protection; computer security; penetration testing.

Без должного внимания к вопросам обеспечения безопасности, последствия перехода к широкомасштабному использованию информационных технологий могут принимать драматический характер, что подтверждает нескончаемый поток публикаций в средствах массовой информации и специальных изданиях. Неправомерное уничтожение или разглашение информации, ее искажение или фальсификация, равно как и дезорганизация процессов обработки в информационных системах могут приводить, и уже приводят, к нанесению серьезных материальных, моральных и даже физических потерь как отдельным гражданам, так организациям и государствам.

К настоящему времени сравнительно молодая профессия специалиста по защите информации уже стала востребованной в республике. В то же время, в связи с появлением все новых угроз, ростом масштабов их проявлений, существенной проблемой процесса практической подготовки специалистов по защите компьютерной информации становится недостаточная оснащенность программно-технической базы учебных заведений.

Возможным выходом из этой ситуации представляется создание и использование в учебном процессе современных инфраструктурных решений, виртуальных лабораторий, возможностей облачных и кластерных архитектур.

* **Труды XI Международной научно-практической конференции «Современные информационные технологии и ИТ-образование» (SITITO'2016), Москва, Россия, 25-26 ноября, 2016**

Преступления в сфере информационных технологий или киберпреступность

Общественная опасность противоправных действий в области электронной техники и информационных технологий определяется тем, что они могут вступить в противоречие с положениями Закона РБ «Об информации, информатизации и защите информации» [1] в отношении личных данных и конфиденциальной информации, а также могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, нарушение работы компьютерных систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям.

Согласно УК РБ [2] преступлениями против информационной безопасности (глава 31 УК РБ) являются:

- несанкционированный доступ к компьютерной информации (ст. 349 УК РБ);
- модификация компьютерной информации (ст. 250 УК РБ);
- компьютерный саботаж (ст.251 УК РБ);
- неправомерное завладение компьютерной информацией (ст. 252 УК РБ);
- изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 253 УК РБ);
- разработка, использование либо распространение вредоносных программ (ст. 254 УК РБ);
- нарушение правил эксплуатации компьютерной системы или сети (ст. 255 УК РБ).

Зачастую совершение преступлений в сфере компьютерной информации сопряжено с совершением иных уголовно наказуемых деяний, в частности, таких как:

- нарушение тайны переписки (ст. 203 УК РБ);
- нарушение авторских, смежных, изобретательских и патентных прав (ст. 201 УК РБ);
- кража (ст. 205 УК РБ);
- причинение имущественного ущерба путем обмана или злоупотребления доверием (ст. 216 УК РБ);
- мошенничество (ст. 209 УК РБ);
- вымогательство (ст.208 УК РБ) и пр.

Методы оказания противодействия указанным противоправным действиям, многие из которых связаны с проблемами несанкционированного проникновения злоумышленника в инфраструктуру информационных систем, входят в сферу подготовки специалистов по защите информации.

Киберпреступления и задачи тестирования на проникновение

Незаконные действия, которые осуществляются людьми, использующими информационные технологии для преступных целей, относятся к категории преступлений в сфере информационных технологий или киберпреступности. Основные виды киберпреступлений связаны с несанкционированным использованием различных технических устройств и систем удаленного доступа; созданием и распространением вредоносного кода, взломом паролей, кражей реквизитов банковских карт; а также с распространением противоправной информации (клевета, материалы для разжигания межнациональной и межрелигиозной розни и т.п.) через информационно-коммуникационные сети [3].

Для снижения уровня опасности реализации киберперступлений, популярной во всем мире услугой в области информационной безопасности становится тестирование на проникновение. Суть его заключается в санкционированной попытке обойти существующий комплекс средств защиты информационной системы. В ходе тестирования на проникновение аудитор играет роль злоумышленника, мотивированного на нарушение информационной безопасности сети заказчика.

Тестирование на проникновение (сокращение от англ. — penetration testing, на сленге «пентест») - это поиск уязвимостей с практической проверкой возможностей их реализации. Цель тестирования на проникновение - оценка уровня защищенности, которая заключается в исследовании сети или веб-ресурса для выявления уязвимостей, которые могут быть использованы злоумышленником для реализации угроз информационной безопасности [4].

Очевидными достоинствами методов тестирования на проникновение являются:

- высокая достоверность сведений о выявленных уязвимостях благодаря фактическому подтверждению возможности их использования злоумышленником;
- достаточность результатов исследования для оценки критичности выявленных

уязвимостей; наглядность получаемых результатов.

К недостаткам методов тестирования на проникновение можно отнеси:

- способность исследователя воспроизводить только действия нарушителя, равного ему или уступающего по квалификации, и, как следствие, — высокие требования к квалификации исследователя и не высокая достоверность сведений об отсутствии уязвимостей;
- низкую степень автоматизации действий исследователя, и, как следствие, — высокие затраты по сравнению с другими способами оценки уровня защищенности.

Очевидно, что подготовка таких специалистов, способных проводить тестирование на проникновение по заказу организаций, предполагает не только наличие теоретических знаний, но и использование специализированных лабораторий со специально сконфигурированной инфраструктурой и программно-технической базой.

Выбор платформы для создания учебных лабораторий

В учебном процессе кафедры системного программирования и компьютерной безопасности ГрГУ им. Я. Купалы в качестве платформы для обучения методам исследования информационных систем на проникновение выбран облачный кластер Гродненского государственного университета [5]. Кластер используется в университете с 2012 года, работает на платформе на OpenSource-продукта OpenNebula [6], в качестве системы виртуализации использует KVM.

Выбор кластера для создания лабораторий обусловлен возможностью формирования профильных библиотек образов вычислительных машин (ВМ) с комплектами программного обеспечения (ПО) учебного назначения; возможностью быстрого пакетного развертывания, обновления, удаления однотипных виртуальных рабочих мест или лабораторий целиком; формированием, на основе набора ВМ, лабораторных макетов распределенных систем; возможностью подключения виртуальных машин к локальной сети университета.

Использование платформы OpenNebula также позволило реализовать ряд возможностей, необходимых для обучения методам защиты информации:

- тестирование в облаке антивирусного ПО без вероятности повреждения оборудования студентов;
- развёртывание ВМ с различными уязвимыми сетевыми сервисами, используемыми для обучения сканированию безопасности сети;
- развертывание фермы ВМ Linux и Windows для изучения отдельных уязвимостей операционных системы;
- развёртывание виртуальных машин для обучения технологиям защиты от утечек информации (использование DLP-систем, программных комплексов для анализа угроз и уязвимостей, систем защиты сетей и рабочих станций), связанных с обеспечение управления информационной безопасностью организаций [5].

Возможности облачного кластера на базе OpenNebula позволили эффективно использовать его также для организации соревнований по практической защите компьютерной информации различного формата и уровня. Например, существующая инфраструктура OpenNebula была выбрана в качестве базы при проведении очного тура по защите информации в рамках Республиканской олимпиады по криптографии и защите информации 2015 года.

В то же время нельзя не отметить и некоторые недостатки использования облачного кластера для обучения методам тестирования на проникновение:

- подготовка мастер-образов и шаблонов ВМ является весьма трудоемким процессом, требующим не только владения предметной областью, но и навыками системного администрирования Windows и Linux, а также знания особенностей облачной платформы;
- невозможность использования некоторых ОС семейства Windows (в частности, Windows XP SP3 и некоторых других, более старых версий) из-за несовместимости с используемым средством виртуализации KVM;
- требование наличия постоянного подключения к сети Интернет. Очевидно, что при обрыве соединения сеанс связи с облачной платформой будет прекращен. Продолжить работу можно будет только после восстановления подключения к Интернет.

Характеристика учебных лабораторий для тестирования на проникновение

В рамках развития концепции использования виртуальных лабораторий для задач тестирования на проникновение, развернуты три учебных лаборатории – начального, среднего и высокого уровня сложности.

Работа обучаемого в лабораториях осуществляется на основе методики «серый ящик»: перед началом исследования предоставляется информация об инфраструктуре в виде схемы и

описания деятельности виртуальной компании. Далее участникам будет предложено выполнить эксплуатацию различных уязвимостей, связанных с работой сетевых и веб-компонентов, криптографических механизмов, ошибками конфигурации и кода, а также с человеческим фактором.

Каждая из трёх лабораторий соответствует определённому уровню сложности («наименьшая», «средняя», «высокая»). Прохождение 1-го уровня открывает доступ к прохождению 2-го, и т.д. Полное прохождение третьего (последнего) уровня потребует от участника наивысших знаний и умений.

Система виртуальных облачных лабораторий интегрирована в образовательную онлайн-платформу университета для того, чтобы обеспечить обучаемым удобный доступ к необходимой теоретической информации.

Для автоматизации проверки результатов проведенного тестирования на проникновение, соответствия найденных токенов (флагов), отмечающих найденную в результате проникновения уязвимость, требуемым эталонам, в локальной сети университета развернута система Facebook CTF [7, 8].

Facebook CTF — это платформа для организации соревнований в формате CTF (Capture The Flag), а именно — двух его разновидностей:

- Jeopardy — классический CTF с набором заданий. Доступ к следующему заданию можно получить, лишь правильно решив предыдущее;
- King of the Hill — вид CTF, в котором нужно максимальное время удерживать контроль над взломанной системой; это связано с особенностью системы, которая периодически регенерирует состояние, «сбрасывая» участников с того уровня, на которого им удалось достичь.

Использование платформы Facebook CTF, как интерфейса управления процессом тестирования на проникновение, позволило активизировать учебный процесс, придав решению задач на проникновение соревновательный характер и эмоциональную окраску.

Приведем примеры лабораторий различного уровня сложности.

Пример 1. Лаборатория тестирования на проникновение (начальный уровень сложности)

Легенда. Терминальный узел компании «ИТ-Безопасность» был скомпрометирован (известен пароль от учётной записи одного из пользователей). Как следствие злоумышленник может подключится к терминальному серверу внутри локальной сети по протоколу SSH, используя скомпрометированные учетные данные: IP-адрес: 192.168.100.106, user: <…>, password: <…>

Примеры практических заданий для лаборатории начального уровня

1. Web-security.

Описание задачи: Необходимо исследовать web-приложение, найти уязвимость и проэксплуатировать ее. Решением задачи будет получение доступа к файловой системе сервера, где можно будет найти необходимый токен (рис.1).

Участвующее машины: 172.16.1.2 - машина с web-приложением.

2. Audit (windows).

Описание задачи: На машине Windows исследовать журнал событий. Выяснить, на какого пользователя совершалась атака.

Участвующее машины: 172.16.1.6 (Windows) - user: John; password: john

3. Audit (linux).

Описание задачи: Исследовать журналы аудита - выяснить, на какого пользователя совершалась атака.

Участвующее машины: (Debian) - user: labuser, password: pass4labuser

4. Network security.

Описание задачи: Необходимо исследовать маршрутизатор Cisco, найти уязвимость и проэксплуатировать ее.

Участвующее машины: 172.16.1.100

4.1. Network security 1.

Описание задачи: Необходимо исследовать маршрутизатор Cisco, найти открытый порт. (Найденный открытый порт будет означать решение задания и является токеном)

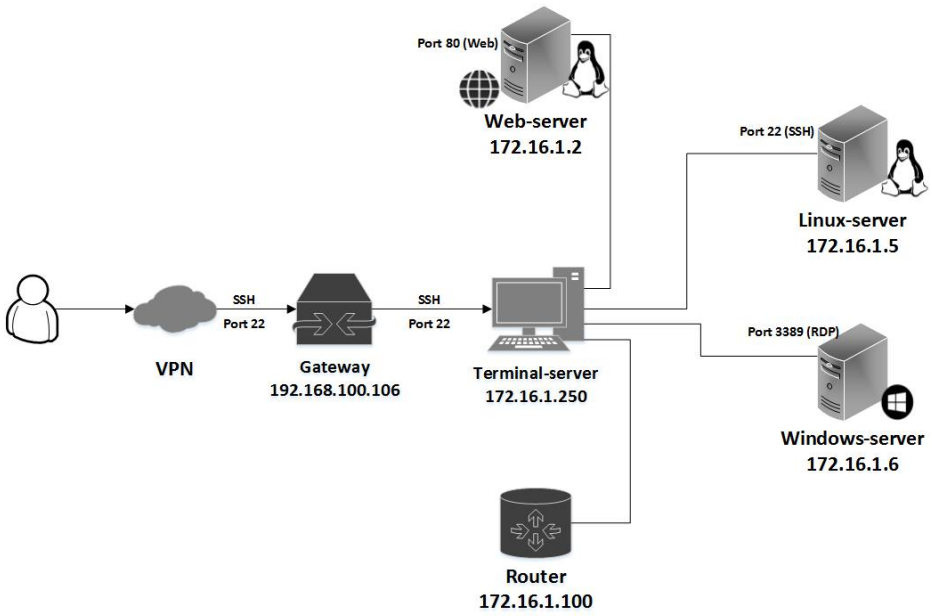

Рис.1. Примерная схема лаборатории начального уровня сложности

4.2 Network security 2.

Описание задачи: Необходимо найти уязвимость маршрутизатора Cisco и проэксплуатировать её. (Получение зашифрованного пароля enable будет означать решение задания и является токеном)

4.3. Network security 3.

Описание задачи: Необходимо расшифровать пароль от enable. (Полученный расшифрованный пароль enable является токеном; получение данного токена также открывает доступ к задачам уровня №2).

Пример 2. Лаборатория тестирования на проникновение (средний уровень сложности)

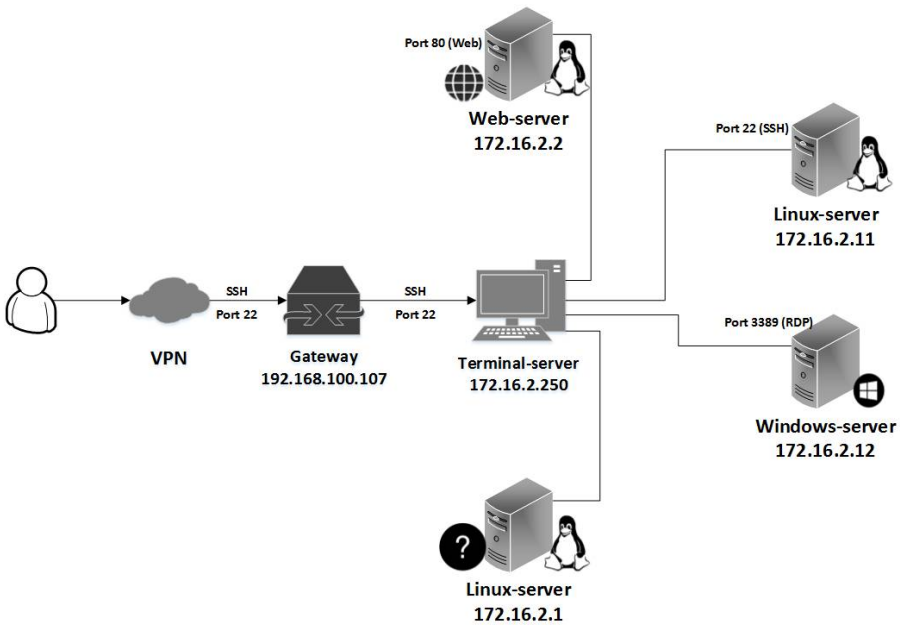

Рис.2. Примерная схема лаборатории среднего уровня сложности

Примеры практических заданий

1. Сетевая безопасность.

Описание задачи: Необходимо исследовать сервер, найти все открытые порты, определить сервис и найти токен.

Участвующее машины: 172.16.2.1

2. Безопасность Web-приложений.

Описание задачи: Необходимо исследовать web-приложение, найти уязвимость и проэксплуатировать ее. После эксплуатации можно будет найти необходимый токен. (Получение токена также открывает доступ к задачам уровня №3).

Участвующее машины: 172.16.2.2

3. Обнаружение атак.

Легенда. Машина бухгалтерии компании находится под управлением linux по адресу 172.16.2.11. Также имеется машина Windows по адресу 172.16.2.12, с которой работают те же пользователи.

3.1 Audit 1 (linux).

Описание задачи: На Linux машине определите какой из уволенных сотрудников ответственен за утечку данных.

Участвующее машины: 172.16.2.11 (linux) - user: labuser, password:labuser

3.2 Audit 2 (linux).

Описание задачи: Какой из пользователей пытался получить права пользователя root?

Участвующее машины: 172.16.2.11 (linux) - user: labuser, password: labuser

3.3. Audit 3 (Windows).

Описание задачи: На Windows-машине найдите пользователя, который удалил файл ImportantFile.txt.

Участвующее машины: 172.16.2.12 (windows) - user: John(AdministratorUser), password: john

3.4. Audit 4 (Windows).

Описание задачи: Кто последний получал доступ к файлу ImportantFile.txt перед его удалением (исключая удалившего файл пользователя)?

Участвующее машины: 172.16.2.12 (windows) - user: John(AdministratorUser), password: john

Пример 3. Лаборатория тестирования на проникновение (высокий уровень сложности)

Условия прохождения лаборатории №3 максимально приближены к реальным: участнику сообщается только схематичное изображение виртуальной компании (рис. 3) без дополнительной информации об уязвимых узлах и токенах. Уровень задач данного уровня является максимально сложным и требует глубокого понимания предметной области. Получение доступа к машине администратора (192.168.2.1) является целевой задачей (дополнительные подсказки к данному заданию будут даваться участнику по мере нахождения токенов).

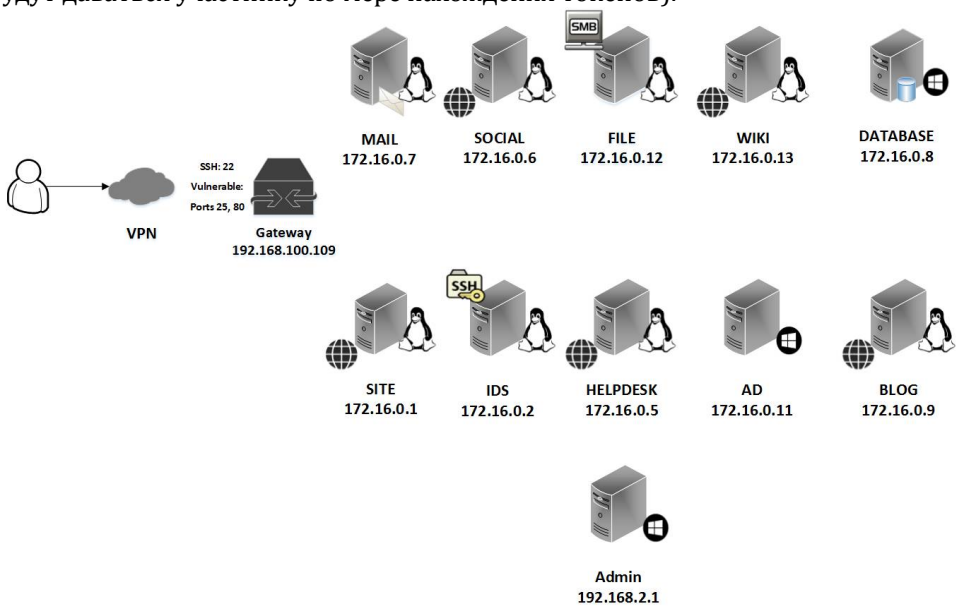

Рис.3. Схема проекта лаборатории высокого уровня сложности

Выводы

Использование облачных лабораторий для задач тестирования на проникновение продемонстрировало адекватность предложенного подхода поставленной цели - формированию и совершенствованию навыков обучаемых при решении задач по тестированию сетевой

инфраструктуры на проникновение извне. Основная сложность, с которой пришлось столкнуться разработчикам – это подготовка множества поэтапных заданий.

Опыт работы показал, что организация виртуальных облачных лабораторий для тестирования на проникновение является перспективным направлением в организации учебного процесса; может рассматриваться как содержательная квинтэссенция различных учебных дисциплин; является одним из немногих действительно эффективных способов подготовки специалистов с практическими навыками тестирования на проникновение.

Литература

1. Об информации, информатизации и защите информации: Закон Республики Беларусь от 10 ноября 2008 г. N 455-З // Консультант Плюс : Беларусь. Технология 3000 [Электронный ресурс] / ООО ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2016. – Дата доступа: 16.09.2016.
2. Уголовный кодекс Республики Беларусь: с изменениями и дополнениями от 5 января 2016 г. – Изд.: НЦПИ РБ. – 2016. – 320 с.
3. Киберпреступность [Электронный ресурс] / SecurityLab.ru - информационный портал по безопасности. – М.: Positive Technologies. - Режим доступа: http://www.securitylab.ru/news/tags/Киберпреступность/ (дата обращения. 27.03.2016).
4. Тестирование на проникновение [Электронный ресурс] / Портал по информационной безопасности. ООО «ПентестИТ», 2016. – Режим доступа: https://www.pentestit.ru/audit/penetration-testing (дата обращения: 27.09.2016).
5. Кадан А.М. Облачные инфраструктурные решения на платформе OpenNebula в подготовке специалистов по защите информации // Современные информационные технологии и ИТ-образование. Т. 1 (№ 11), 2015. — С.178-182.
6. OpenNebula [Электронный ресурс] // Сайт проекта OpenNebula. – Режим доступа:: http://opennebula.org/ (дата обращения: 27.03.2016).
7. Facebook выложил на Гитхаб свою платформу для проведения CTF [Электронный ресурс] / Сообщество IT-специалистов. ООО «Хабр», 2016. – Режим доступа: https://habrahabr.ru/post/283380/ (дата обращения: 29.09.2016).
8. Страница проекта Facebook CTF [Электронный ресурс] / Сайт GitHub. – Режим доступа: https://github.com/facebook/fbctf (дата обращения: 29.09.2016).

References

1. Ob informatsii, informatizatsii i zashchite informatsii: Zakon Respubliki Belarus' ot 10 noyabrya 2008 g. N 455-Z // Konsul'tant Plyus : Belarus'. Tekhnologiya 3000 [Elektronnyy resurs] / OOO YurSpektr», Nats. tsentr pravovoy inform. Resp. Belarus'. – Minsk, 2016. – Data dostupa: 16.09.2016.
2. Ugolovnyy kodeks Respubliki Belarus': s izmeneniyami i dopolneniyami ot 5 yanvarya 2016 g. – Izd.: NTsPI RB. – 2016. – 320 s.
3. Kiberprestupnost' [Elektronnyy resurs] / SecurityLab.ru informatsionnyy portal po bezopasnosti. – M.: Positive Technologies. Rezhim dostupa: http://www.securitylab.ru/news/tags/Kiberprestupnost'/ (data obrashcheniya. 27.03.2016).
4. Testirovanie na proniknovenie [Elektronnyy resurs] / Portal po informatsionnoy bezopasnosti. OOO «PentestIT», 2016. – Rezhim dostupa: https://www.pentestit.ru/audit/penetration-testing (data obrashcheniya: 27.09.2016).
5. Kadan A.M. Oblachnye infrastrukturnye resheniya na platforme OpenNebula v podgotovke spetsialistov po zashchite informatsii // Sovremennye informatsionnye tekhnologii i IT-obrazovanie. T. 1 (№ 11), 2015. — S.178-182.
6. OpenNebula [Elektronnyy resurs] // Sayt proekta OpenNebula. – Rezhim dostupa:: http://opennebula.org/ (data obrashcheniya: 27.03.2016).
7. Facebook vylozhil na Gitkhab svoyu platformu dlya provedeniya CTF [Elektronnyy resurs] / Soobshchestvo IT-spetsialistov. OOO «Khabr», 2016. – Rezhim dostupa: https://habrahabr.ru/post/283380/ (data obrashcheniya: 29.09.2016).
8. Stranitsa proekta Facebook CTF [Elektronnyy resurs] / Sayt GitHub. – Rezhim dostupa: https://github.com/facebook/fbctf (data obrashcheniya: 29.09.2016).

Поступила: 10.10.2016

Об авторах:

Кадан Александр Михайлович, заведующий кафедрой системного программирования и компьютерной безопасности Гродненского государственного университета им. Я. Купалы, г. Гродно, Беларусь, кандидат технических наук, kadan@mf.grsu.by;

Доронин Алексей Константинович, магистрант факультета математики и информатики Гродненского государственного университета им. Я. Купалы, г. Гродно, Беларусь, doronin_ak@mf.grsu.by.