Третьим вопросом является ситуация, когда нагрузка создаётся запросами, которые не повторяют обращений к одним и тем же несуществующим страницам, либо количества обращений и запросов к страницам недостаточно, чтобы преодолеть минимально необходимый лимит. В таком случае на автоматизированную систему можно возложить функцию анализа взаимосвязи ошибочных запросов и отправителя [3]. Простейшим случаем будет блокировка запросов с определённых адресов, от которых пришло достаточно весомое количество ошибочных запросов за некий промежуток времени.

Реализация динамической блокировки в начале атаки и снятие блокировки после в данном случае не является сложной задачей, поскольку автоматизированная система может просто обновлять конфигурации межсетевых экранов в части блокировок. Ситуация отличается от предыдущей с использованием межсетевых экранов тем, последним нет необходимости держать в конфигурациях всю базу актуальных адресов, а лишь достаточно адресов, подвергающихся блокировке.

Таким образом, применяя комплекс перечисленных мер, есть возможность сократить нагрузку от специально сгенерированных ошибочных запросов на значительную величину (касательно тестового сервера, использовавшегося для исследования, сокращение нагрузки при реализации подобной схемы защиты в идеальных условиях составило бы до 9 %, т.е. более чем на половину).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК.

1. *Максимов А.М., Тищенко Е.Н.* Особенности использования носителей информации в защищённых информационных системах // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 238-244.
2. *Ciesielski V., Anand L.* Data mining of web access logs from an academic web site. Design and application of hybrid intelligent systems // IOS Press Amsterdam. – 2003. – С. 1034-1043.
3. *Тищенко Е.Н., Шарыпова Т.Н.* Формализация выбора различных вариантов системы защиты информации от несанкционированного доступа в среде электронного документооборота // Вестник Ростовского государственного экономического университета (РИНХ). – 2010. – № 32. – С. 226-233.

Статью рекомендовал к опубликованию д.т.н., профессор П.Н. Башлы.

**Максимов Алексей Михайлович** – Ростовский Государственный Экономический Университет (РИНХ); e-mail: ironmanpc@rambler.ru; 344002, г. Ростов-на-Дону, ул. Б. Садовая, 69, к. 211, 306а; тел.: 88632613858; аспирант.

**Maximov Alexey Mikhailovich** – Rostov State University of Economics; e-mail: ironmanpc@rambler.ru; 69, B. Sadovaya streeet, room 211, 306a, Rostov-on-Don; 344002, Russia; phone: +78632613858; postgraduate student.

УДК 004.054

**А.Г. Богораз, О.Ю. Пескова**

## МЕТОДИКА ТЕСТИРОВАНИЯ И ОЦЕНКИ МЕЖСЕТЕВЫХ ЭКРАНОВ*

*Рассмотрены основные российские и зарубежные методики оценки защищенности информационных систем в приложении к анализу межсетевых экранов. Показана необходимость разработки методологии тестирования межсетевых экранов как на стендах, так и в реальной системе. Был выполнен анализ следующих методик тестирования инфор-*

* Работа поддержана грантом РФФИ 13-07-00244-а.

*мационной безопасности организации: OSSTMM – The Open Source Security Testing Methodology Manual, NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment, ISSAF – Information System Security Assessment Framework. Также анализировались следующие методики проведения тестов на проникновение: методика Positive Technology, методика Digital Security, BSI – Study A Penetration Testing Model, PTES – Penetration Testing Execution Standard – Technical Guidelines.Описаны основные шаги методик, проведено их сравнение по различным показателям. Представлена авторская методика тестирования и оценки межсетевых экранов. Приведен перечень уязвимостей, которые могут быть обнаружены с помощью разработанной методики.*

*Межсетевой экран; тестирование межсетевых экранов; тесты на прочность; пентестинг; методики тестирования информационной безопасности.*

**A.G. Bogoras, O.Yu. Peskova**

## METHODOLOGY FOR TESTING AND ASSESSMENT OF FIREWALLS

*In article the main Russian and foreign techniques of an assessment of security of information systems in the annex to the analysis of firewalls are considered. The necessity of developing the methodology of testing firewalls both in the laboratory and in the real system is shown. Analysis was performed for the following test methods for information security: OSSTMM – The Open Source Security Testing Methodology Manual, NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment, ISSAF – Information System Security Assessment Framework. In addition, we analyzed the following methods of penetration testing: methods of Positive Technology, technique Digital Security, BSI - Study A Penetration Testing Model, PTES – Penetration Testing Execution Standard – Technical Guidelines. The basic steps of techniques are described, comparison on various indicators is carried out them. The author's technique of testing and assessment of firewalls is presented. The list of vulnerabilities that can be found by means of the developed technique is provided.*

*Firewall; firewall testing; pretesting; security assessment techniques.*

**Введение.** При современном уровне развития информационно-вычислительных сетей (и зачастую их главенствующей роли в технологической цепочке обработки информации) вопросы обеспечения сетевой безопасности являются критически важными для работоспособности всей информационной системы. Одним из основных средств защиты от внешних воздействий являются межсетевые экраны (МЭ), предназначенные для контроля и фильтрации трафика, проходящего через них.

Межсетевые экраны подразделяются на различные типы по своим функциональным возможностям, поддерживаемым протоколам, видам фильтрации и так далее. Но вне зависимости от типа МЭ существует большое количество решений различных производителей, и потребителю бывает трудно выбрать систему, наиболее адекватно и эффективно решающую задачи по защите конкретной сети от несанкционированного доступа. Информация о межсетевых экранах, доступная непосредственно от производителя, чаще всего представляет собой рекламу, преувеличивающую достоинства и скрывающую недостатки. Для осознанного выбора желательно получить четкое (стандартизированное) описание качественных характеристик продукта, его достоинств и недостатков, надежности и уязвимых мест.

На данный момент не существует методологии, нацеленной именно на специализированное тестирование межсетевых экранов. Для оценки качества МЭ приходится пользоваться более общими методиками.

Классифицируем рассматриваемые методики по двум типам: методики тестирования информационной безопасности организации и методики проведения тестов на проникновение.

Был выполнен анализ следующих методик тестирования информационной безопасности организации:

- OSSTMM – The Open Source Security Testing Methodology Manual;
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment;
- ISSAF – Information System Security Assessment Framework.

Также анализировались следующие методики проведения тестов на проникновение:

- методика Positive Technology;
- методика Digital Security;
- BSI – Study A Penetration Testing Model;
- PTES – Penetration Testing Execution Standard – Technical Guidelines.

**1. Российские методики анализа защищенности**

***1.1. Методика Positive Technology.*** Следует отметить, что российские методики, по большей части, являются копиями зарубежных методик. Единственная методика, полностью разработанная в России – методика Positive Technology [1].

При планировании тестов определяются границы и режимы проведения тестов. Проведение тестов может быть как с уведомлением персонала объекта, так и без него. Тесты разбиваются на 2 фазы: внешнюю, при которой аудиторы работают с минимальными знаниями о системе, и их целью является «пробить периметр», и внутреннюю, когда периметр успешно «пробит», аудиторы начинают оценку защищенности сети, уже координируя свои действия с администраторами системы.

В компании определены три вида тестов на проникновение: технологический, социотехнический, комплексный. Для оценки критичности обнаруженных уязвимостей используется методика Common Vulnerability Scoring System (CVSS), что позволяет использовать результаты тестирования на проникновение в качественных и количественных методиках анализа риска.

Данную методику можно применять на этапе оценки продукта для возможности использования на предприятии.

***1.2. Методика Digital Security***. Методика Digital Security – методика NSA INFOSEC, доработанная специалистами фирмы Digital Security [2], которая включает в себя этапы:

1. Утверждение с заказчиком режима тестирования. Определяется уровень информированности исполнителя о тестируемой системе и уровень информированности Заказчика о проведение теста на проникновение.

2. Подписание договора.

3. Выполнение теста на проникновение. В рамках теста на проникновение аудиторы проводят полный анализ всех деталей исследуемого объекта, выбирают подходящие сценарии атак, с учетом человеческого фактора, возможно, разрабатывают уникальное для каждого конкретного случая программное обеспечение для попытки проникновения в информационную систему.

Помимо технологических проверок в процессе внешнего теста на проникновение проводится тестирование возможности проникновения в информационную систему с использованием методик социальной.

По результатам проведения тестирования на проникновение создается отчет, содержащий детальное описание проведенных работ, все выявленные уязвимости системы и способы их реализации. Отчет также содержит конкретные рекомендации по устранению данных уязвимостей.

Данную методику также можно применять на этапе оценки продукта для возможности использования на предприятии.

**2. Зарубежные методики анализа защищенности**

***2.1. OSSTMM – The Open Source Security Testing Methodology Manual [3].*** Является достаточно формализованным и хорошо структурированным документом для тестирования сети. Документ имеет так называемую «Карту безопасно-

сти» – визуальный показатель безопасности. На карте указываются основные области безопасности, которые включают в себя наборы элементов, которые должны быть протестированы на соответствие методике:

1. Информационная безопасность.
2. Тестирование процесса безопасности.
3. Тестирование технологии интернет-безопасности.
4. Тестирование безопасности каналов связи.
5. Тестирование безопасности беспроводных технологий.
6. Тестирование физической безопасности.

В документе присутствует подпункт «Методология» / «Тестирование технологии интернет-безопасности» / «Обзор сети» / «Тестирование МЭ», где перечислена ожидаемая информация, которую может получить взломщик в результате удачной атаки или отсутствия нужной функции у средства защиты. В методике указано, что МЭ должен обладать конкретными функциями и возможностями, и перечислено свыше 30 типов тестов для их контроля. Также описываются конкретные корректные реакции сети на атаки и их наличие, например, измерение времени отклика на пакет или проверка наличия потерь пакетов на маршруте к цели.

Минусами методики считается формализованность и отсутствие дополнительного описания к требованиям.

Данную методику можно использовать как на этапе оценки продукта для возможности использования на предприятии, так и на этапе разработки для проверки отдельных возможностей и функций. Также методику можно использовать как шаблон разработки, — какие стандартные функции должны обязательно присутствовать в конечном продукте.

***2.2. NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment [4], [5].*** Создана и поддерживается подразделением NIST — CSRC, центром по компьютерной безопасности, объединяющий специалистов федеральных служб, университетов, крупнейших ИТ-компаний США.

В документе присутствуют такие разделы как:

- обзор тестирования и экспертизы безопасности;
- обзор методов;
- определение цели и техники анализа;
- техники оценки уязвимостей цели;
- планирование оценки безопасности;
- выполнение оценки безопасности;
- пост-тестовые мероприятия.

В разделе «Техники оценки уязвимостей цели», в качестве одной из техник описываются Тесты на проникновение, а именно Фазы и Логистика тестов. По данному документу тесты на проникновение, в дополнение к стандартным их возможностям, можно применять для определения:

- насколько хорошо система переносит реально существующие модели атак;
- примерного уровня сложности, который необходимо преодолеть атакующему;
- дополнительных мер противодействия, которые могли бы ослабить угрозы в адрес системы;
- способности защищающего систему на обнаружение атак и обеспечение соответствующей реакции на них.

Выделяются следующие фазы тестов на проникновение:

1. *Планирование.* На данном этапе определяются правила, утверждается и документируется управление, определяются тестируемые цели. Задается основа для успешного тестирования на проникновение.

2. *Исследование.* Данный этап включает в себя 2 части. Первая часть – старт тестирования и сохранение собираемой и сканируемой информации. Для идентификации потенциальных целей проводится определение сетевых портов и сервисов. Вторая часть – анализ уязвимостей. Производится сравнение сервисов, приложений, ОС сканируемого хоста с базами уязвимостей (автоматический процесс для сканеров уязвимостей) и с собственными знаниями аудитора об уязвимостях. Аудитор может использовать свои собственные базы – или открытые базы уязвимостей – для ручного определения уязвимостей. Ручная обработка позволяет выявить новые уязвимости, но существенно замедляет процесс.
3. *Атака.* Этап проверки ранее определенных уязвимостей путем их эксплоитирования. Если атака удачна, то уязвимость проверяется и определяются меры понижения угроз безопасности.
4. *Отчет.* Производится во время 3 вышеописанных фаз. Во время фазы «Планирование» разрабатывается план оценки. Во время фаз «Исследование» и «Атака» сохраняются лог-файлы и создаются периодические отчеты для системных администраторов или менеджмента. В заключение теста, создается отчет, как правило, для описания уязвимостей, указания оценок рисков и представления указаний по смягчению обнаруженных недостатков.

В главе «Логистика тестов» описываются различные рекомендации по типам тестирования.

Также существует отдельный документ, регулирующий методологию работы с МЭ – NIST SP 800–41 Guideline on Firewalls and Firewall Policy. В пункте «Тесты» документа приводится достаточно подробный список аспектов оценки МЭ

Данную методику можно использовать как на этапе оценки продукта для возможности использования на предприятии, так и на этапе разработки для проверки отдельных возможностей и функций. Также методику можно использовать как шаблон разработки — какие стандартные функции должны обязательно присутствовать в конечном продукте.

***2.3. BSI – Study A Penetration Testing Model [6].*** Разработан германским подразделением «Federal Office for Information Security». В документе описывается проведение корректных испытаний системы на прочность. Подробно описываются не только сама методология тестов, но и необходимые требования, правовые аспекты применения методологии и процедуры, которые необходимо выполнить для успешного проведения тестов. Присутствуют такие разделы, как:

- Введение и объекты обучения.
- IT-безопасность и тесты на проникновение.
- Классификация и объекты тестов на проникновение.
- Правовые вопросы.
- Общие требования.
- Методология тестов на проникновение.
- Выполнение тестов на проникновение.

Согласно этому документу, существует 3 типа методов, с помощью которых можно нанести IT-системе вред или подготовить атаку: атаки через сеть, социальная инженерия, обход физических мер безопасности.

Определены 5 процедур, которые необходимо выполнить для проведения тестов на прочность:

- поиск информации о целевой системе;
- сканирование целевой системы на предмет наличия сервисов;
- идентификация системы и приложений;

- ♦ исследование уязвимостей;
- ♦ эксплоитирование уязвимостей.

Приводится классификация тестов на прочность и определены ее критерии. В приложениях содержатся описание ПО, которое можно использовать для тестирования объектов, описанных в методике.

Данную методику рекомендуется использовать для тестирования конечного продукта. Она является достаточно подробной и старается предусмотреть все аспекты тестов на прочность, как технические, организационные, так и правовые.

***2.4. ISSAF – Information System Security Assessment Framework [7].*** Разработан OISSG (Open Information Systems Security Group) для следующих инструментов менеджмента и внутренних контрольных проверок:

а) Оценка политик и процедур информационной безопасности организации для отчетности об их соответствии индустриальным IT-стандартам, применимым законам, а также нормативным требованиям;

б) Выявление и оценка зависимости бизнеса от инфраструктуры IT-услуг;

в) Проведение оценки уязвимостей и тестов на проникновение для выделения уязвимостей в системе, которые могут привести к потенциальным рискам информационных активов;

г) Указание моделей оценки по доменам безопасности;

1) Нахождение и устранение неправильных конфигураций;

2) Идентификация и решение рисков, связанных с технологиями;

3) Идентификация и решение рисков, связанных с персоналом или бизнес–процессами;

4) Усиление существующих процессов и технологий;

5) Предоставление лучших практик и процедур для поддержки инициатив непрерывности бизнеса.

Документ охватывает огромное количество вопросов, связанных с информационной безопасностью. Присутствуют главы, описывающие оценку безопасности МЭ, роутеров, антивирусных систем и много другого.

Также присутствует глава «Оценка безопасности МЭ», где описывается, какие бывают МЭ, каким функциями они должны обладать и защиту от чего они не могут предоставить.

Непосредственно методология включает в себя 4 этапа:

1. Определение МЭ.
2. Определение общих неправильных конфигураций.
3. Тестирование общих атак на МЭ.
4. Тестирование продукта по специфическим вопросам.

Также в главе прилагается подробные рекомендации по тестированию. Описаны не только утилиты, которыми можно провести тестирование, но и указания по их использованию и какие реакции можно получить в результате тестирования с определенными параметрами.

Данную методику рекомендуется применять для проверки конечного продукта или проверки общей надежности сети.

***2.5. PTES – Penetration Testing Execution Standard – Technical Guidelines [8].*** Стандарт, разработанный для объединения как бизнес требований, так и возможностей служб безопасности, и масштабирования тестов на проникновение. На первом подготовительном этапе подробно рассматриваются устанавливаемые каналы коммуникаций, правила взаимодействия и контроля, конкретные способы реагирования и мониторинга инцидентов.

Далее выделены следующие этапы:

1. Сбор информации.

2. Моделирование угроз.

3. Методы анализа уязвимостей.

4. Эксплоитация – обеспечение обхода контрмер и обнаружение наилучшего пути атаки.

5. Пост-эксплоитация – анализ инфраструктуры, последующее проникновение в инфраструктуру, зачистка и живучесть.

Определена структура отчетов, составляемых по результатам тестирования.

***2.6. Результаты сравнения методик.*** В целом, результаты сравнения методологий по фазам тестов на прочность можно проиллюстрировать следующей картой (рис. 1)

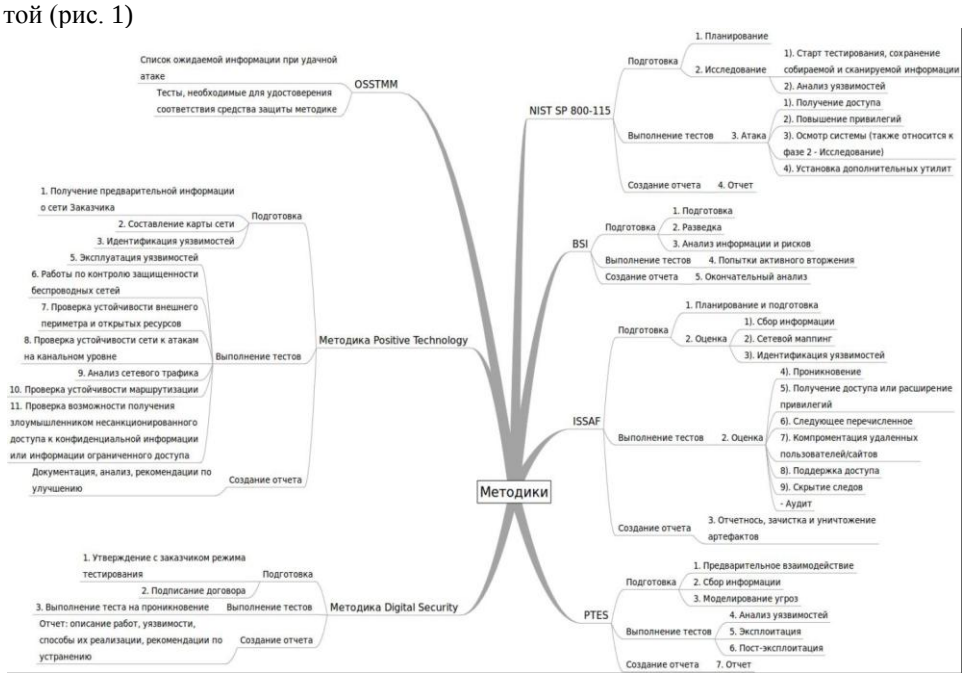


*Рис. 1. Сравнение методологий по фазам тестов на прочность*

**4. Разработанная методика тестирования межсетевых экранов**

По результатам анализа данных методик была предложена авторская методика тестирования, назначением которой является оценка уровня защиты, предоставляемой межсетевым экраном. Методика предназначена для стендового тестирования, однако может использоваться для тестирования в рабочей системе заказчика.

Методика состоит из следующих фаз:

1. **Планирование.** Эта фаза подразумевает активную работу с Заказчиком. Обсуждаются цели и условия предстоящего тестирования, подписываются документы и подтверждается эксплоитирование выявленных уязвимостей.
2. **Подготовка.** На данной фазе начинается подготовка набора ПО, необходимого для тестирования. Также производится сборка испытательного стенда и настройка тестовой среды под условия тестирования, определенные в фазе планирования.
3. **Разведка**. Данная фаза позволяет начать пассивные и активные исследования тестируемого объекта. На этапе пассивных исследований производится поиск информации, которая может помочь в работе аудитора. Активный этап подразумевает начало скрытого исследования тестируемого МЭ.

4. **Анализ уязвимостей.** С помощью этой фазы производится автоматическое и ручное определение уязвимостей тестируемого МЭ. Производится классификация найденных уязвимостей, а также определяются потенциальные риски системе при эксплоитировании этих уязвимостей.
5. **Активное вторжение.** Пятая фаза позволяет начать работу по эксплоитированию уязвимостей, выявленных в ходе фазы «4.Анализ уязвимостей», и определения их возможного использования для проникновения в целевую систему.
6. **Поддержка и зачистка.** После успешного вторжения в целевую систему, аудитор оставляет в системе скрытые закладки для дальнейшего облегченного проникновения в целевую систему. Также аудитор зачищает все следы своего пребывания для уменьшения возможности обнаружения своего успешного вторжения.
7. **Отчет**. Во время работы всех остальных фаз производится подробное документирование всех шагов тестирования для составления максимально полного и детального отчета.

Для корректного соблюдения процедуры тестирования необходимо соблюсти определенные требования, которые должны быть выполнены перед тестированием в обязательном порядке. Требования представлены в общем порядке для 2 типов тестирований: частная и независимая оценка продукта на стендовом оборудовании, и частная независимая оценка продукта в условиях среды Заказчика. Основным отличием данных типов является возможность эмулировать фактически любые условия работы среды в случае тестирования на стендовом оборудовании. В случае тестирования продукта на оборудовании Клиента, аудитор может быть жестко привязан к среде, и некоторые обязательные требования могут быть невыполнимы вследствие обстоятельств.

Методика подробно описывает основные и вспомогательные функции различных уровней и классов (как для защиты сети, так и для собственной защиты), которыми должны обладать МЭ и которые должны оцениваться в ходе выполнения методики.

С помощью разработанной методики можно обнаружить следующий перечень уязвимостей:

1. Недостатки конфигурирования.
2. Недостатки кода ядра.
3. Переполнение стека.
4. Недостаточная проверка ввода – многие приложения не проверяют информацию, введенную пользователем, полностью.
5. Символьные ссылки – файлы, указывающие на другие файлы.
6. Атаки на дескриптор файла – Файловый дескриптор – неотрицательное целое число, используемое системой для отслеживания файлов, вместо отслеживания их имен. Когда привилегированная программа предоставляет несоответствующий дескриптор файла, то этот файл – скомпроментированный.
7. Условие «гонки» – Условие, когда программа включилась в привилегированный режим, но еще не выключилась из него. Пользователь может воспользоваться этим моментом, для получения доступа к программе или процессу.
8. Некорректный доступ к файлам и каталогам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Positive Technologies – безопасность, консалтинг, compliance management [Электронный ресурс] // Positive Technologies [сайт]. URL: http://www.ptsecurity.ru/services/pen/ technological (дата обращения 20.10.2013).
2. Digital Security: N1 в аудите безопасности [Электронный ресурс]. // Digital Security [сайт]. URL: http://dsec.ru/consult/test/#why (дата обращения 20.10.2013).
3. *Herzog P.* OSSTMM – The Open Source Security Testing Methodology Manual. – USA, New York, 13.12.2006. –129 p. URL: http://www.isecom.org/research/osstmm.html (дата обращения: 20.10.2013).
4. *Scarfone K., Hoffmann P.* NIST Special Publications 800-41 Guidelines on Firewall and Firewall Policy. – USA, Gaithersburg, 09.2009. – 48 p. URL: http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf (дата обращения 20.10.2013).
5. *Scarfone K., Souppaya M., Cody A., Orebaugh A.* NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment. – USA, Gaithersburg, 09.2008. – 80 p. URL: http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf (дата обращения 20.10.2013).
6. BSI – Study A Penetration Tesing Model / Germany, Bonn. – 111 p. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile (дата обращения: 20.10.2013).
7. *Rathore B. и др.* ISSAF – Information System Security Assesment Framework. – 30.04.2006. – 1264 p. URL: http://www.oissg.org/issaf02/issaf0.1-5.pdf (дата обращения 20.10.2013).
8. *Nickerson C. и др.* The Penetration Testing Execution Standard. – 30.04.2012 [Электронный ресурс] // Penetration Testing Execution Standarts [сайт]. URL: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines (дата обращения 20.10.2013).

Статью рекомендовал к опубликованию д.т.н., профессор Н.И. Витиска.

**Пескова Ольга Юрьевна** – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail poy@tgn.sfedu.ru; 347922, г. Таганрог, ул. Чехова, 2; тел./факс: 88634371905; кафедра безопасности информационных технологий; к.т.н.; доцент.

**Богораз Антон Григорьевич** – e-mail bogoraz.a.g@gmail.com; кафедра безопасности информационных технологий; аспирант.

**Peskova Olga Yur'evna** – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University"; e-mail poy@tgn.sfedu.ru; 2, Chekhov street, Taganrog, 347922, Russia; phone/fax: +78634371905; the department of security in data processing technologies; cand. of eng. sc.; associate professor.

**Bogoras Anton Grigor'evich** – e-mail bogoraz.ag @ gmail.com; the department of security in data processing technologies; postgraduate student.