УДК 004.056

Анализ стандартов и методик тестирования на проникновение

Макаренко С. И., Смирнов Г. Е.

Актуальность. *В настоящее время вопросы безопасности информационных систем объектов критической информационной инфраструктуры приобретают важное значение. Вместе с тем текущие задачи аудита информационной безопасности (ИБ) объектов критической информационной инфраструктуры, как правило, ограничиваются проверкой их на соответствие требованиям по ИБ. Однако при таком подходе к аудиту, зачастую, остается неясным устойчивость данных объектов к реальным атакам злоумышленников. Для проверки такой устойчивости объекты подвергают процедуре тестирования, а именно – тестированию на проникновение. Анализ отечественных публикаций в этой области показывает, что в отечественной практике отсутствует какой-либо системный подход к проведению тестирования на проникновение. В связи с этим актуальным является анализ и систематизация лучших зарубежных подходов и практик к проведению тестирования.* ***Целями работы*** *является сравнительный анализ существующих зарубежных и отечественных методик и стандартов тестирования на проникновение.* ***Результаты.*** *В статье представлены результаты анализа следующих зарубежных стандартов и методик: OSSTMM, ISSAF, OWASP, PTES, NIST SP 800-115, BSI, PETA, PTF, а также отечественной методики Positive Technologies.* ***Элементами новизны работы*** *являются выявленные особенности, достоинства, недостатки и рамки применимости существующих стандартов и методик тестирования на проникновение.* ***Практическая значимость.*** *Материал статьи может использоваться для формирования исходных данных, последовательности этапов и их содержания, при практическом аудите безопасности информационных систем объектов критической инфраструктуры путем тестирования на проникновение.*

Ключевые слова: *тестирование на проникновение, стандарт, методика, аудит, информационная безопасность, критическая инфраструктура, информационно-техническое воздействие, информационно-психологическое воздействие, OSSTMM, ISSAF, OWASP, PTES, NIST SP 800-115, BSI, PETA, PTF, Positive Technologies.*

Введение

В 2017 г. в России был принят федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Данный закон устанавливает перечень объектов и субъектов, относящихся к критической информационной инфраструктуре (КИИ) РФ, а также обязует специальные службы разработать комплекс мер направленных на аудит состояния информационной безопасности (ИБ) объектов КИИ и обеспечения ее защищённости.

В подавляющем числе случаев аудит ИБ объектов КИИ проводиться на основе сравнительного анализа с нормативно-правовой документацией, регламентирующей обеспечение ИБ, или на основе анализа рисков. Вместе с тем, в предыдущих работах авторов [1, 2] указывается на необходимость формирования еще одного типа практического подхода к аудиту, а именно – аудита на основе экспериментальных исследований системы или ее прототипа. Данный тип

Библиографическая ссылка на статью:
Макаренко С. И., Смирнов Г. Е. Анализ стандартов и методик тестирования на проникновение // Системы управления, связи и безопасности. 2020. № 4. С. 44-72. DOI: 10.24411/2410-9916-2020-10402.

Reference for citation:
Makarenko S. I., Smirnov G. E. Analysis of penetration testing standards and methodologies. *Systems of Control, Communication and Security*, 2020, no. 4, pp. 44-72 (in Russian). DOI: 10.24411/2410-9916-2020-10402.

аудита, проводится с применением против системы средств или способов информационных воздействий с целью практической проверки эффективности технических или организационных мер защиты, а также выявления новых уязвимостей системы. В некоторых работах, например, таких как [3-9], для такого подхода используется термин «тестирование на проникновение» (в англоязычной литературе – «penetration testing»), а также другие термины «активный аудит», «инструментальный аудит» и др., но при этом суть подобного практического подхода к аудиту не меняется.

Таким образом, можно говорить о том, что одним из перспективных направлений практического аудита ИБ объектов КИИ является реализации в отношении них тестов на проникновение – воздействие на объект тестовых информационно-технических воздействий (ИТВ) и тестовых информационно-психологических воздействий (ИПВ), аналогичных реальным ИТВ и ИПВ, которые с высокой степенью вероятности могут использоваться злоумышленниками. Несмотря на то, что такое тестирование представляет собой достаточно адекватный и максимально приближенный к реальности подход к оценке защищенности, он не получил широкого распространения. Основными причинами этого, на взгляд авторов, является отсутствие единой общепризнанной методики проведения тестирования на проникновение, критериев выбора ИТВ и ИПВ, для такого тестирования, а также критериев оценки его результатов.

Целью статьи является: сравнительный анализ существующих методик и стандартов тестирования на проникновение, их особенностей, достоинств, недостатков и рамок применимости.

Результаты представленного в статье анализа, в дальнейшем, авторы планируют использовать для разработки теоретических основ тестирования на проникновение, критериев оценки эффективности тестов, моделей уязвимости объектов КИИ к тестовым ИТВ и ИПВ.

1. Базовая терминология и классификация тестовых воздействий

Введем базовую терминологию, которую будем использовать в дальнейшем.

Объект – информационная система, информационно-телекоммуникационная сеть, автоматизированная система управления, в отношение которых проводится аудит ИБ.

Тестирование – проверка выполнения требований к объекту при помощи наблюдения за его работой в конечном наборе специально выбранных ситуаций [2].

Тест – отдельное мероприятие по исследованию объекта или способ изучения процессов его функционирования [2].

Информационно-техническое воздействие – воздействие на информационный ресурс, информационную систему, информационную инфраструктуру, на технические средства или на программы, решающие задачи формирования, передачи, обработки, хранения и воспроизведения информации, с целью вызвать заданные структурные или функциональные изменения [2].

Тестовое информационно-техническое воздействие – воздействие на информационный ресурс, информационную систему, информационную инфраструктуру, на технические средства или на программы, решающие задачи фор-

мирования, передачи, обработки, хранения и воспроизведения информации, с целью выявить уязвимости объекта на которое производится воздействие [2].

Информационно-психологическое воздействие – информационное, психотронное или психофизическое воздействие на психику человека или группы людей, оказывающее влияние на восприятие ими реальной действительности, в том числе на их поведенческие функции, а, в некоторых случаях, и на функционирование органов и систем человеческого организма [2].

Тестовое информационно-психологическое воздействие – информационное, психотронное или психофизическое воздействие на психику человека или группы людей, оказывающее влияние на восприятие ими реальной действительности, в том числе на их поведенческие функции, а, в некоторых случаях, и на функционирование органов и систем человеческого организма, с целью выявить уязвимости объекта на которое производится воздействие [2].

Тестирование на проникновение – экспериментальная проверка с целью оценивания состояния ИБ и выявления уязвимостей объекта тестирования (тестируемой системы) путем интегрального и целенаправленного применения против него специальных средств и способов ИТВ и ИПВ [2].

Ущерб – эквивалентная стоимость всех видов потерь (финансовых, репутационных, материальных и пр.), которые понесет объект или его владелец в результате инцидента.

Инцидент – факт нарушения свойств ИБ в процессах формирования, передачи, обработки, хранения и воспроизведения информации на объекте и/или прекращение функционирования объекта, в том числе произошедшее в результате воздействия ИТВ или ИПВ.

Уязвимость – недостаток объекта, эксплуатация которого делает возможным реализацию инцидента, нанесение объекта повреждений любой природы, либо снижение эффективности его функционирования.

Эксплойт – потенциально безвредный набор данных или последовательности действий, которые некорректно обрабатывается информационной системой, вследствие ошибок в ней. Результатом некорректной обработки такого набора данных или последовательности действий может быть переход объекта в уязвимое состояние.

Общая классификация мероприятий, способов и средств ИТВ и ИПВ, которые могут быть использованы при тестировании на проникновение, представлены на рис. 1-2.

В рамках тестирования на проникновение должны реализовываться сценарии поэтапного интегрального применения средств и способов ИТВ и ИПВ, которые с высокой степенью вероятности будут применяться реальными злоумышленниками, что позволит провести всеобъемлющий анализ уязвимостей тестируемых объектов, а также сформировать предложения по совершенствованию системы защиты.

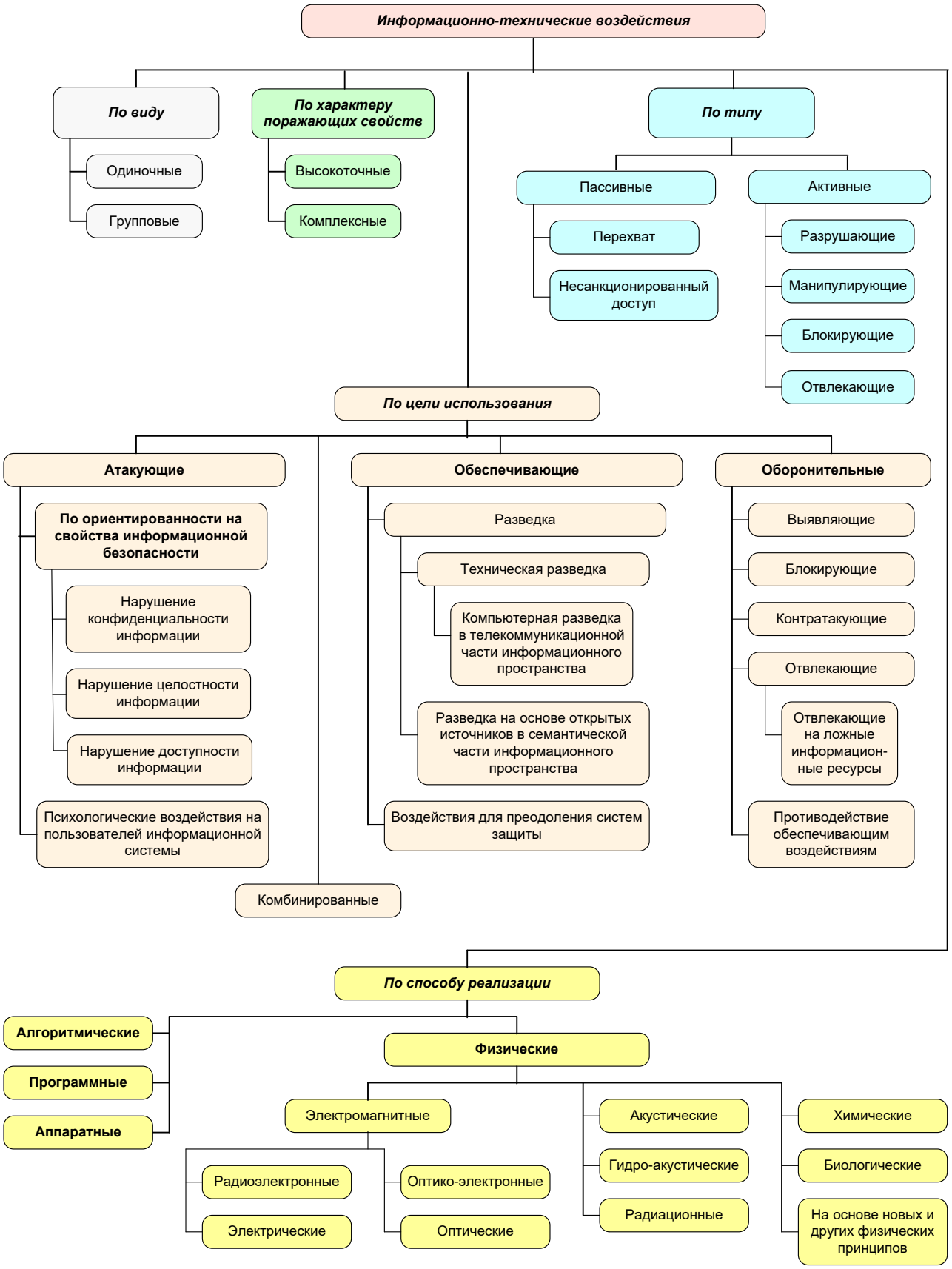

Рис. 1. Классификация ИТВ, которые могут быть использованы при тестировании на проникновение [2]

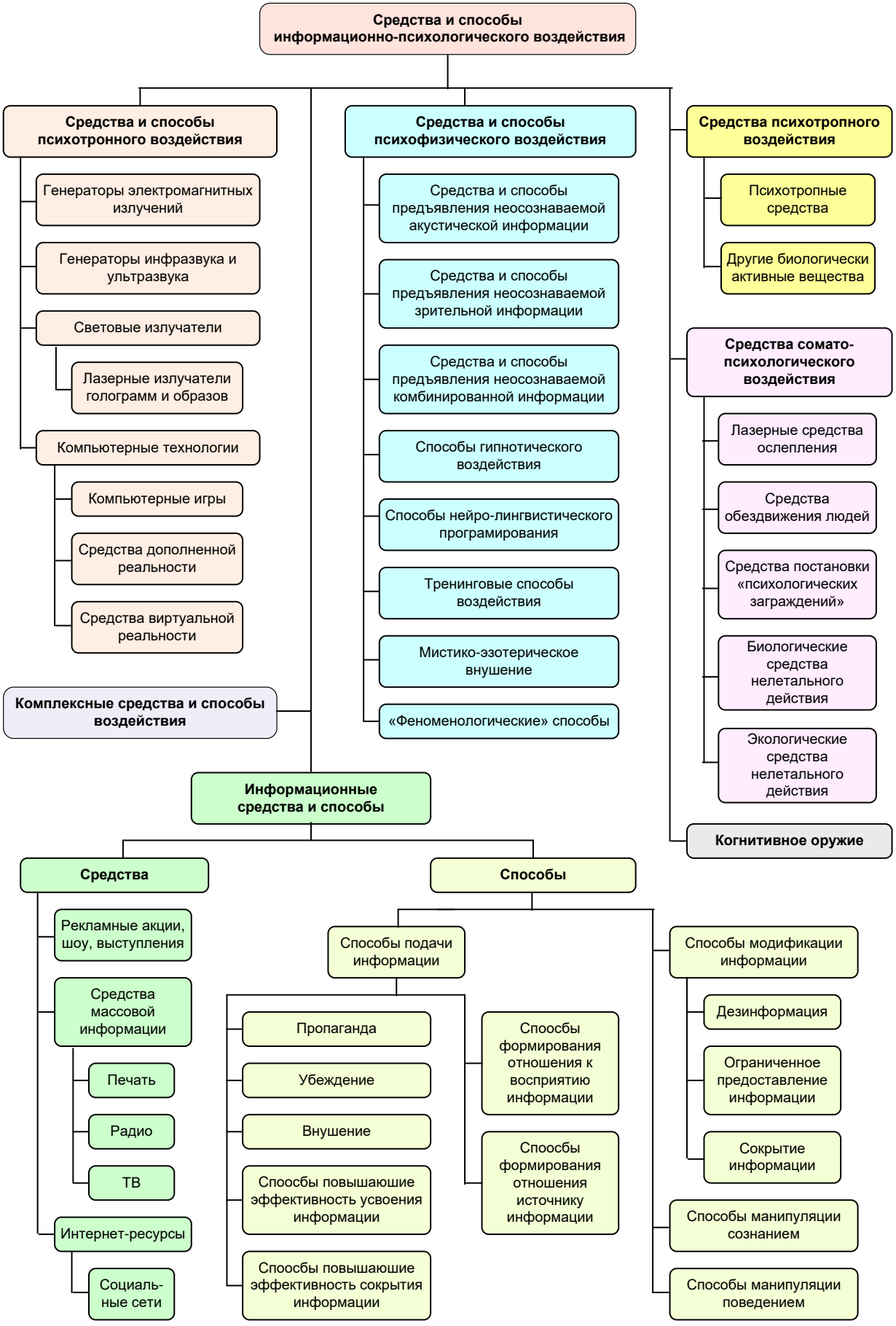

Рис. 2. Классификация ИПВ, которые могут быть использованы при тестировании на проникновение [2]

2. Анализ актуальных отечественных работ в области тестирования на проникновение

Практическим вопросам оценки состояния ИБ объектов путем их тестирования посвящены отечественные работы Климова С. М. [11, 12], Петренко А. А., Петренко С. А. [13], Маркова А. С., Цирлова В. Л., Барабанова А. В. [4], Скабцова Н. [5], Бойко А. А. [14-16], Храмова В. Ю. [15-17], Щеглова А. В. [16, 17], Дьяковой А. В. [14, 15], Макаренко С.И. [1, 2]. Теоретическим вопросам развития тестирования, как средства контроля состояния ИБ объектов посвящены работы Пакулина Н. В., Шнитмана В. З., Никешина А. В. [18], Аветисяна А. И., Белеванцева А. А., Чукляева И. И. [41] и Макаренко С.И. [2].

В работах Барановой Е.К. [19, 20], Бегаева А.Н., Бегаева С.Н., Федотова В.А. [21], Богораза А. Г., Песковой О. Ю. [22], Дорофеева А. [23], Умницына М. Ю. [24], Бородина М. К., Бородиной П. Ю. [25], Полтавцевой М. А., Печенкина А. И. [26], Кадана А. М., Доронина А. К. [27], Еременко Н. Н., Кокоулина А. Н. [28], Туманова С. А. [29], Кравчука А. В. [30], Горбатова В. С., Мещерякова А. А. [31], рассматриваются именно такие практические способы оценивания защищённости информационных систем, как тестирование на проникновение или «penetration testing». В некоторых работах, такой тип тестирования указан под наименованием «инструментальный аудит».

Анализ вышеуказанных работ показал следующее. Работы, посвященные вопросам экспериментального тестирования реальных информационных систем, рассматривают такие способы и сценарии исключительно как «тестирование на проникновение» или как «инструментальный аудит», при этом проведение такого типа аудита в отечественной практике не регламентируется какими-либо общепринятыми руководящими документами или методиками тестирования. В некоторых отечественных работах по тестированию на проникновение рекомендуется делать акцент на необходимости выявления наиболее «зрелищных» уязвимостей или тех уязвимостей устранение которых принесет максимальные экономические выгоды компании, выполняющий аудит.

Таким образом, можно сделать вывод, что дальнейшее развитие отечественной теории и практики тестирования на проникновение должно опираться на уже известные методики и стандарты проведения подобного типа тестирования, которые уже разработаны, преимущественно, за рубежом.

3. Анализ стандартов и методик в области тестирования на проникновение

В международной практике, проведение тестов на проникновение регламентируется стандартами и методиками, которые регламентируют этапы тестирования, порядок испытаний тестируемых объектов, порядок взаимодействия аудитора с заказчиком и т.д. К широко распространенным зарубежным стандартам и методикам относятся:

1) методика OSSTMM – The Open Source Security Testing Methodology Manual [32];
2) методика ISSAF – Information System Security Assessment Framework [33];

3) методика OWASP – Open Web Application Security Project [34];
4) стандарт PTES – Penetration Testing Execution Standard [35];
5) стандарт NIST SP 800-115 – Technical Guide to Information Security Testing and Assessment [36];
6) методика BSI – Study a Penetration Testing Model [37];
7) методика PETA – Methodology of Information Systems Security Penetration Testing [38];
8) методика PTF – Penetration Testing Framework [39].

К наиболее проработанным, среди оригинальных отечественных методик тестирования на проникновение, относится методика от Positive Technologies [40].

Отметим, что среди отечественных публикаций уже имеется работа [22], в которой ранее уже был представлен анализ методик тестирования на проникновение. Данная работа была использована авторами в качестве первоосновы изложенного ниже анализа, который был существенно дополнен и расширен.

3.1. Методика OSSTMM

Методика OSSTMM – The Open Source Security Testing Methodology Manual [32] разработана институтом ISECOM (Institute for Security and open Methodologies), который является открытым сообществом ученых и практиков в области ИБ.

Методика OSSTMM является в высокой степени формализованным и хорошо структурированным документом регламентирующем практически все аспекты тестирования на проникновение, ориентирована на тестирование преимущественно компьютерных сетей. Методика периодически обновляется. Из недостатков стоит отметить малое количество информации по практическим действиям и инструментарию тестирования.

Методика OSSTMM содержит следующие разделы:

1) первичные сведения о документе;
2) определение тестирования на проникновение, рамок тестирования, ролей и процессов;
3) анализ безопасности объекта;
4) показатели (метрики) безопасности объекта;
5) анализ социальных процессов в персонале объекта тестирования;
6) процесс тестирования;
7) тестирование устойчивости персонала к ИПВ и социальной инженерии;
8) тестирование безопасности физической инфраструктуры;
9) тестирование безопасности беспроводных технологий;
10) тестирование безопасности телекоммуникационных технологий;
11) тестирование безопасности данных;
12) рекомендации по следованию национальным стандартам и соглашениям;
13) подготовка отчета о тестировании.

Методика OSSTMM определяет, так называемую «карту безопасности» – визуальное отображение основных категорий ИБ, которые оцениваются в процессе тестирования:

- информационная безопасность;
- безопасность социальных процессов;
- безопасность информационных процессов;
- безопасность Интернет-технологий;
- безопасность каналов связи;
- безопасность беспроводных технологий;
- безопасность физической инфраструктуры.

Как таковой, классификации уязвимостей в этой методике нет. Понятие «уязвимость» в методике вводится как ограничение безопасности – это дефект или ошибка, которая запрещает доступ авторизованным пользователям или процессам к информационным ресурсам или позволяет несанкционированный доступ (НСД) неавторизованных пользователей или процессов к ресурсам.

Эту методику можно использовать как на этапе предварительной оценки защищенности объектов в интересах проверки возможности их использования в составе какой-либо информационной системы, так и на этапе разработки объектов для проверки отдельных возможностей и функций ИБ.

3.2. Методика ISSAF

Методика ISSAF – Information System Security Assessment Framework [33] разработана консорциумом OISSG (Open Information Systems Security Group) в качестве стандарта внутреннего аудита организаций этого консорциума. При данном аудите выполняется оценка следующих аспектов ИБ:

- оценка политик и процедур ИБ организации, а также степень их соответствия ИТ-стандартам и требованиям нормативных документов в области ИБ;
- выявление и оценка «зависимости» бизнес-процессов организаций от ИТ-инфраструктуры;
- проведение оценки уязвимостей и тестов на проникновение для выделения уязвимостей в системе, которые могут привести к потенциальным рискам информационных ресурсов;
- указание моделей оценки по доменам безопасности;
- нахождение и устранение неправильных конфигураций аппаратно-программных средств;
- идентификация и снижение рисков, связанных с ИТ;
- идентификация и снижение рисков, связанных с персоналом или бизнес-процессами;
- усиление безопасности существующих процессов и технологий;
- внедрение лучшего опыта обеспечения ИБ в практику и процедуры бизнес-процессов.

Методика ISSAF включает в себя большое количество вопросов, связанных с тестированием ИБ, а материал методики организован в виде двух частей:

– рекомендации для менеджмента;
– рекомендации по тестированию.

Материал методики ISSAF декомпозирован на 14 подразделов.

1. Управление проектом по тестированию.
2. Основные принципы и лучшие практики в проведении тестирования.
3. Схема процесса тестирования.
4. Обзор политики безопасности и способов повышения ИБ.
5. Методология оценки рисков.
6. Тестирование технических аспектов ИБ:
   а) тестирование криптоустойчивости паролей;
   б) тестирование безопасности операционной системы (ОС) Unix/ Linux;
   в) тестирование безопасности ОС Windows;
   г) тестирование безопасности ОС Novell Netware;
   д) тестирование безопасности баз данных (БД);
   е) тестирование безопасности беспроводных сетей и коммуникаций;
   ж) тестирование безопасности коммутаторов;
   з) тестирование безопасности маршрутизаторов;
   и) тестирование безопасности брандмауэров;
   к) тестирование безопасности систем обнаружения вторжений;
   л) тестирование безопасности частных виртуальных сетей VPN;
   м) тестирование безопасности антивирусных систем;
   н) тестирование безопасности распределенных систем хранения данных;
   о) тестирование безопасности Интернет-коммуникаций;
   п) тестирование безопасности пользователей;
   р) тестирование безопасности исходного кода;
   с) тестирование безопасности бинарного кода.
7. Тестирование социально-психологических аспектов ИБ.
8. Тестирование физической инфраструктуры.
9. Анализ инцидентов.
10. Отчетность по результатам аудита и тестирования.
11. Обеспечение непрерывности бизнес-процессов и восстановление после инцидентов.
12. Повышение полноты мониторинга и обучение в области ИБ.
13. Аутсорсинг проведения тестирования и обеспечения ИБ.
14. База знаний:
    а) правовые аспекты тестирования и аудита ИБ;
    б) рекомендации по составлению договора о неразглашении информации;
    в) рекомендации по составлению договора на тестирование и аудит;
    г) шаблоны типовых документов;
    д) контрольный список проверки ОС Windows;
    е) контрольный список проверки ОС Linux;
    ж) контрольный список проверки ОС Solaris;
    з) порты по умолчанию у брандмауэров;
    и) порты по умолчанию у систем обнаружения вторжений;

к) ссылки на другие документы и ресурсы;
л) рекомендации по программному обеспечению (ПО), которое можно использовать для проведения тестирования.

В методике ISSAF представлены 3 этапа, которые необходимо реализовать для корректного проведения тестов на проникновение.

1. Планирование и подготовка. Получение начальной исходной информации об объекте тестирования, планирование и подготовка к тестам. Перед тестированием сторонам необходимо будет подписать формальное соглашение, которое обеспечит основу для проведения тестирования и взаимную правовую защиту. В нем также будет указан порядок взаимодействия, точные даты, длительность тестирования, способы проведения тестирования и т.д.
2. Оценка. На этом этапе производится выполнение тестирования. Предусмотрены следующие подэтапы проведения тестирования:
   а) сбор информации. Для сбора информации в методике ISSAF рекомендуется использовать Интернет. При этом получаемая информация делится на две группы: техническая (DNS/WHOIS) и нетехническая (поисковые системы, группы новостей и т.д.). Данный этап позволяет выделить «точки уязвимости», которые будут использоваться в дальнейшем;
   б) сетевое картографирование. Применение специальных технических средств для определения структуры сети и ее ресурсов;
   в) идентификация уязвимостей. Перед этой стадией, аудитор определяет уязвимые объекты и способы их тестирования. В процессе тестирования методикой ISSAF предполагается выполнение следующих мероприятий:
      – идентификация уязвимостей почтовых сервисов;
      – выполнение углубленного сканирования сетевых информационных ресурсов и сетевых сервисов на предмет поиска известных уязвимостей. Информация об известных уязвимостях берется из открытых баз данных уязвимостей;
      – верификация полученной информации об уязвимостях путем сравнения и проверки информации об уязвимостях, полученных из различных источников или различными способами;
      – документирование обнаруженных уязвимостей;
      – классификация найденных уязвимостей;
      – определение сценариев ИТВ и сценариев использования эксплойтов.

Отметим, что в методике ISSAF для уязвимостей определяется два типа рисков: технический риск и бизнес-риск. В свою очередь каждый из них делится на 3 уровня: низкий, средний, высокий.

3. Непосредственно тестирование на проникновение.

4. Получение доступа или расширение привилегий. Получение минимальных привилегий доступа возможно через доступ к непривилегированным аккаунтам с помощью следующих способов:
   а) подбор комбинаций логин/пароль путем атаки со словарем;
   б) поиск пустых или стандартных паролей в системных аккаунтах;
   в) выявление эксплойтов в стандартных настройках сетевого оборудования;
   г) поиск публичных сервисов, допускающих определенные операции в системе (запись/создание/чтение файлов).

Конечной целью аудитора на данном этапе является получение доступа к аккаунту администратора сети. Часто в сети разрешены только аккаунты с минимальным количеством привилегий. В этом случае выполняется составление карты локальных уязвимостей, производится разработка или получение корректного эксплойта, затем он тестируется в изолированной среде и применяется к компрометированной системе.

5. Дополнительные тесты, например, получение зашифрованных паролей для их последующего взлома в режиме off-line, перехват трафика и его анализ и т.д.
6. Компрометация удаленных пользователей, информационных ресурсов, объектов сети.
7. Поддержка несанкционированного доступа к сети.
8. Сокрытие следов работы.

Методика ISSAF является наиболее подробной, из рассматриваемых в данной статье, методикой тестирования на проникновение как в теоретическом, так и в практическом плане. Эту методику можно использовать как на этапе предварительной оценки защищенности объектов сети в интересах проверки возможности их использования в составе какой-либо информационной системы, так и на этапе разработки объектов для проверки отдельных возможностей и функций ИБ.

3.3. Методика OWASP

Методика OWASP – Open Web Application Security Project [34] создана сообществом OWASP в 2004 г. и развивается по настоящее время международной группой независимых экспертов-энтузиастов. Методика ориентирована на тестирование веб-приложений. Организация OWASP зарегистрирована в США и Бельгии (OWASP Europe VZW). Методика подробно описывает тестирование веб-приложений и фактически является единственной подобной методикой, узко ориентированной именно на веб-приложения.

В 2020 г. вышла промежуточная версия руководства OWASP Web Security Testing Guide v. 4.1. В руководстве по тестированию имеется ссылка на перечень мероприятий по тестированию на проникновение (checklist), а также раскрывается содержимое этих мероприятий.

Методика OWASP содержит следующие разделы:

1) введение;
2) руководство по тестированию OWASP;

3) тестирование на проникновение веб-приложений;
4) руководство по составлению отчётов.

В разделе 4 «тестирование на проникновение веб-приложений» описан набор тестов, ориентированным на проверку следующих аспектов ИБ:

– сбор информации;
– тестирование управления конфигурацией и развертыванием;
– тестирование управления идентификацией;
– тестирование аутентификации;
– тестирование авторизации;
– тестирование управления сессиями;
– тестирование проверки ввода;
– тестирование обработки ошибок;
– тестирование на криптографическую устойчивость;
– тестирование бизнес-процессов;
– тестирование клиентской стороны.

Методику OWASP можно использовать как на этапе предварительной оценки защищенности веб-приложений в интересах проверки возможности их использования в составе какой-либо информационной системы, так и на этапе разработки веб-приложений для проверки отдельных возможностей и функций ИБ.

3.4. Стандарт PTES

Стандарт проведения тестирования на проникновение PTES – Penetration Testing Execution Standard [35] разработана в 2009 г. международной группой независимых экспертов-энтузиастов в области ИБ. PTES качестве стандарта официально зарегистрирована только в США. С момента появления стандарт получил развитие в виде версии 1.1 в 2017 г.

Стандарт PTES предусматривает 7 основных этапов проведения тестирования на проникновение, описанных в соответствующих разделах:

1) этап первоначального общения;
2) сбор информации;
3) моделирование угроз;
4) анализ уязвимостей;
5) эксплуатация;
6) постэксплуатация;
7) отчетность.

К данному стандарту прилагается техническое руководство (PTES Technical Guidelines) подробно излагающее основные технические аспекты тестирования:

1) инструментарий тестирования:
    а) ОС и ПО;
    б) аппаратные средства;
    в) радиотехнические средства;
2) сбор информации об объекте тестирования:
    а) разведка по открытым источникам (OSINT);

б) использование ИПВ и социальной инженерии;
в) анализ социальных сетей и контактов;
г) анализ email и телефонных контактов;
д) сканирование сети;
е) анализ используемого ПО и ОС;
ж) анализ периметра безопасности;
з) анализ физической инфраструктуры;

3) анализ уязвимостей:
   а) анализ уязвимостей ОС и ПО;
   б) анализ уязвимостей БД;
   в) анализ уязвимостей VPN;
   г) анализ уязвимостей транспортной сети и сетевых протоколов;
   д) анализ уязвимостей беспроводной сети;
   е) анализ уязвимостей Интернет-подключений;
   ж) анализ уязвимостей аутентификации и криптоустойчивости паролей;
   з) формирование целевых ИТВ компьютерной разведки;
4) эксплуатация уязвимостей (формирование обеспечивающих и атакующих ИТВ, ориентированных на проникновеннее за защищаемый периметр организации за счет эксплуатации выявленных уязвимостей):
   а) атаки на ОС и ПО;
   б) атаки на аутентификацию по стандартным паролям;
   в) атаки на сетевые протоколы;
   г) атаки на VPN;
   д) DOS-атаки;
   е) атаки на протоколы семейства WEP и WPA беспроводных сетей;
   ж) атаки на шлюзы с сетью Интернет;
   з) ИПВ и социальная инженерия;
   и) атаки на инфраструктуру контроля периметра (видеонаблюдение, пропускная система, учет передвижений персонала и т.д.);
5) постэксплуатация (формирование атакующих ИТВ, ориентированных на расширение привилегий и несанкционированные действия после проникновения за защищаемый периметр организации):
   а) эксплуатация уязвимостей ОС, ПО и БД;
   б) формирование закладок и уязвимостей для последующей эксплуатации;
   в) получение доступа и работа с системными файлами;
   г) получение доступа к важным файлам;
   д) получение доступа к информации авторизации пользователей;
   е) обход внутренних средств защиты;
6) отчетность.

Данные этапы охватывают практически все действия, связанные с тестом на проникновение – от первоначального общения и обоснования задания на тестирование до этапа формирования отчёта, в котором весь процесс фиксируется

наиболее эргономичным для заказчика образом, а также формируются рекомендации по повышению защищённости тестируемой системы.

Этот стандарт можно использовать как на этапе предварительной оценки защищенности объектов в интересах проверки возможности их использования в составе какой-либо информационной системы, так и на этапе разработки объектов для проверки отдельных их возможностей и функций ИБ.

3.5. Стандарт NIST SP 800-115

Стандарт NIST SP 800-115 – Technical Guide to Information Security Testing and Assessment [36] разработан и поддерживается в актуальном состоянии одним из подразделений национального института стандартизации США NIST (National Institute of Standards and Technology), а именно – центром по компьютерной безопасности CSRC (Computer Security Resource Center), объединяющим специалистов федеральных служб, университетов и крупнейших ИТ-компаний США.

Материал данного стандарта организован в виде последовательности следующих разделов:

1) обзор тестирования и экспертизы безопасности;
2) обзор методов;
3) определение цели и техники анализа;
4) техники оценки уязвимостей объектов;
5) планирование оценки безопасности;
6) выполнение оценки безопасности;
7) пост-тестовые мероприятия.

В разделе «техники оценки уязвимостей объектов», в качестве одной из техник описываются типовые тесты на проникновение, а именно их этапы и логика проведения. В соответствии с этим стандартом, тесты на проникновение рекомендуется проводить в следующих случаях:

- для определения устойчивости и защищенности объекта к реально существующим ИТВ;
- для определения трудоемкости преодоления периметра защиты объекта;
- для выяснения уязвимостей существующих мер и средств защиты;
- для определения способности системы защиты объекта, своевременно обнаруживать реальные ИТВ и адекватно реагировать на них.

В соответствии со стандартом NIST SP 800-115, в тестировании на проникновение выделяют следующие этапы.

1. Планирование. На данном этапе определяются правила тестирования, утверждаются и документируется управление тестированием, определяются цель и частные задачи тестирования.
2. Исследование. Данный этап включает в себя два подэтапа:
   - компьютерная разведка объекта тестирования в интересах сбора доступной информации об объекте тестирования, защищаемом периметре и т.д.;

- анализ уязвимостей в интересах формирования перечня перспективных уязвимостей которые могут использоваться в качестве целей для тестовых ИТВ.

3. Атака. Реализация ИТВ на ранее определенные уязвимости. Если ИТВ оканчивается инцидентом, то уязвимости присваивается статус «актуальная» и в дальнейшем определяются меры по ее устранению.
4. Отчет. В соответствии с методикой, формирование отчетных документов производится на всех вышеуказанных этапах. Во время этапа «планирование» разрабатывается план тестирования. Во время этапа «исследование» и «атака» сохраняются лог-файлы, создаются периодические отчеты для системных администраторов и специалистов-аналитиков. В заключение теста, создается итоговый отчет, который, как правило, содержит описания выявленных уязвимостей, оценки рисков, указаний по устранению уязвимостей и модернизации системы защиты.

Стандарт NIST SP 800-115 можно использовать как на этапе предварительной оценки защищенности объектов в интересах проверки возможности их использования в составе какой-либо информационной системы, так и на этапе разработки объектов для проверки отдельных возможностей и функций ИБ. Также этот стандарт можно использовать как шаблон для разработки – какие стандартные функции обеспечения ИБ должны присутствовать в разрабатываемом объекте.

Недостатком стандарта NIST SP 800-115 является то, что он был принят в 2008 г. и в настоящее время не в полной мере отражает современные подходы к тестированию на проникновение.

3.6. Методика BSI

Методика BSI – Study a Penetration Testing Model [37] разработана немецкой государственной организацией Federal Office for Information Security. В этой методике описывается проведение испытаний объекта на устойчивость к ИТВ, при этом подробно описываются не только последовательность проведения тестовых ИТВ, но и необходимые требования по ИБ, а также правовые аспекты тестирования на проникновение.

Материал методики BSI организован в следующие разделы:

1) ИТ-безопасность и тесты на проникновение;
2) объекты тестов на проникновение и их классификация;
3) правовые вопросы;
4) общие требования;
5) методика проведения тестов на проникновение;
6) выполнение тестов на проникновение.

Согласно методике BSI, выделяется три основных типа воздействий:

1) ИТВ через сеть;
2) ИПВ и социальная инженерия;
3) обход физических мер безопасности.

При этом в методике BSI определены следующие основные этапы тестирования объекта.

1. Подготовка к тестированию. Заказчик определяет объекты тестирования. Определяются ресурсы, риски, проверяемые требования по ИБ. Обсуждаются правовые аспект. Составляется договор о проведении тестирования.
2. Разведка. Это этап пассивного тестирования, цель которого получить как можно более полную информацию об объекте, установленных операционных системах (ОС) и программном обеспечении (ПО), данные о потенциальных целях атакующих ИТВ, а также об известных недостатках ИБ. Данный этап включает в себя ряд подэтапов:
   – поиск информации об объекте тестирования;
   – использование обеспечивающих ИТВ для проведения компьютерной разведки объекта;
   – определение операционной системы и приложений;
   – выявление уязвимостей объекта.
3. Анализ информации и рисков. Для успешной, прозрачной и эффективной процедуры тестирования, собранная информация должна быть проанализирована перед началом этапа тестирования атакующими ИТВ. Анализ должен включать в себя определение целей ИТВ, потенциальные риски для объекта, вероятность причинения ущерба объекту, время, необходимое для проведения тестирования атакующими ИТВ, их ориентированность на выявленные на предыдущем этапе уязвимости объекта.
4. Попытки активного вторжения. Тестирование и анализ возможностей эксплуатации уязвимостей объекта, выявленных на этапе разведки, путем реализации атакующих ИТВ.
5. Анализ результатов. Конечный отчет должен содержать оценку уязвимостей объекта в виде формуляров потенциальных рисков, а также рекомендации по устранению уязвимостей и рисков. Отчет также должен гарантировать прозрачность тестов и раскрытие уязвимостей.
6. Документирование. Это не отдельный этап, а постоянная процедура, предполагающая журналирование, запись, обработка и выработка рекомендаций во время всех вышеописанных этапов.

В приложениях методики BSI содержатся описание ПО, которое можно использовать для тестирования объектов, описанных в методике.

Данную методику рекомендуется использовать для тестирования конечного продукта. Методика BSI является достаточно подробной, а ее разработчики старались предусмотреть все аспекты тестирования на проникновение: технические, организационные, правовые.

3.7. Методика PETA

Методика PETA – Methodology of Information Systems Security Penetration Testing [38] является примером проектного подхода к организации тестирова-

ния информационных систем. Данная методика предлагает следующую последовательность этапов тестирования на проникновение.

1. Планирование:
   - формирование заказчиком требований к результатам тестирования;
   - формирование договоренностей о проведении тестирования между заказчиком и аудитором;
   - формирование команды менеджеров проекта;
   - определение области тестирования;
   - определение правил тестирования;
   - формирование группы тестирования;
   - описание ролей;
   - проведение брифингов и обсуждений стратегии тестирования.
2. Тестирование:
   - сбор информации об тестируемом объекте;
   - анализ периметра защиты тестируемого объекта;
   - проникновение за периметр;
   - анализ сети (использование обеспечивающих ИТВ);
   - анализ уязвимостей (использование обеспечивающих ИТВ);
   - закрепление за периметром, расширение полномочий (использование атакующих ИТВ);
   - получение доступа к целевым информационным ресурсам, проведение несанкционированных действий в системе (использование атакующих ИТВ);
   - использование ИПВ и методов социальной инженерии;
   - поддержание несанкционированного доступа в актуальном состоянии;
   - сокрытие следов.
3. Формирование отчета:
   - возвращение тестируемой системы в исходное состояние, удаление последствий ИТВ;
   - анализ полученной в ходе тестирования информации;
   - формирование итогового отчета заказчику;
   - представление результатов тестирования заказчику, итоговая приемка им результатов.

Вышеуказанные этапы в данной методике формализованы в виде процессной модели, которая, однако расписаны не очень подробно. Методика является достаточно обзорной и определяет только самые общее подходы к проведению тестирования на проникновение, оставляя выбор конкретных целей тестирования, используемых тестовых ИТВ, и прочие параметры тестирования на усмотрение заказчика и аудитора.

3.8. Методика PTF

Методика PTF – Penetration Testing Framework, судя по материалам сайта [39] является детальным техническим руководством по проведению тестирования на проникновение в технической части. Данное руководство не содержит

общетеоретической информации, подобно методикам OSSTMM или ISSAF, однако предоставляет практически исчерпывающий перечень уязвимостей объекта подлежащих проверке, в некоторых случаях, с указанием рекомендуемой порядка проведения тестирования и инструментария для него.

Материал методики PTF организован в виде следующих разделов:

1) разведка (рекогносцировка) – сбор информации об объекте за счет проведения активного и пассивного мониторинга, поиска информация в сети Интернет, с использованием ИПВ и способов социальной инженерии;
2) анализ ОС и ПО объекта;
3) анализ портов сети;
4) проверка паролей;
5) проверка уязвимостей:
   - уязвимости удаленного доступа;
   - уязвимости внутреннего доступа;
   - уязвимости bluetooth;
   - уязвимости телекоммуникационного оборудования Cisco;
   - уязвимости системы Citrix;
   - уязвимости транспортных сетей;
6) Непосредственно тестирование на проникновение – использование выявленных уязвимостей для реализации таргетированных ИТВ в отношении объекта тестирования. При этом отдельно рассмотрены:
   - проникновение на сервера;
   - оценка устойчивости VoIP-инфраструктуры;
   - проникновение через беспроводные сети;
   - безопасность физической инфраструктуры.
7) Формирование итогового отчета.

Необходимо отметить, что методика PTF, фактически является частным проектом специалиста по ИБ K. Orrey. Вместе с тем, данная методика получила большое число положительных отзывов специалистов по тестированию на проникновение, которые использовали данную методику как первооснову для разработки своего варианта тестирования. В связи с этим данная методика была включена в настоящий обзор.

3.9. Методика Positive Technologies

Методика Positive Technologies [40] разработана одной из ведущих российских компаний в области ИБ. Компания специализируется на комплексном аудите ИБ, оценке защищенности прикладных систем и веб-приложений, тестировании на проникновение и внедрении процессов мониторинга ИБ.

В качестве целей проведения тестов на проникновение в данной методике указываются:

- обоснование необходимости проведения работ по повышению уровня защищенности информационной системы;

– получение независимой оценки уровня безопасности информационной системы.

При планировании определяются области тестирования и режимы проведения тестов. Проведение тестов может проводиться как с уведомлением персонала объекта, так и без него.

Методика предусматривает три варианта тестов на проникновение, различающихся между собой акцентом на различных типах уязвимостях.

1. Технический тест:

– получение предварительной информации о сети заказчика. Используются те же источники информации, которые доступны злоумышленникам (Интернет, новости, конференции);
– анализ сети, определение типов устройств, ОС, ПО по реакции на внешние ИТВ;
– выявление уязвимостей сетевых служб и ПО;
– анализ веб-приложений заказчика, проверка следующих уязвимостей: внедрение операторов SQL (SQL Injection); межсайтовое исполнение сценариев (Cross-Site Scripting); подмена содержимого (Content Spoofing); выполнением команд ОС (OS Commanding); уязвимостей, связанных с некорректной настройкой механизмов аутентификации и авторизации и пр.;
– эксплуатации выявленных уязвимостей;
– анализ защищенности беспроводных сетей;
– анализ устойчивости внешнего периметра объекта и открытых ресурсов к ИТВ на сетевом уровне типа (DDOS-атаки);
– анализ устойчивости сети к ИТВ на канальном уровне (ИТВ, ориентированные на нарушение функционирования протоколов канального уровня: STP, VTP, CDP, ARP);
– анализ сетевого трафика на предмет выявления утечек и фактов хранения и передачи важной информации (пароли пользователей, конфиденциальные документы и пр.);
– анализ устойчивости сетевой маршрутизации путем реализации ИТВ направленных на фальсификацию маршрутов и проведения DDOS-атак против используемых протоколов маршрутизации;
– анализ возможности получения НСД к конфиденциальной информации или информации ограниченного доступа, путем проверки прав доступа к различным информационным ресурсам с привилегиями, полученными на различных этапах тестирования;
– документирование полученной в ходе тестирования информации, ее анализ с целью выработки рекомендаций по улучшению защищенности сети.

2. Социотехнический тест:

- рассылка сообщений от имени анонимных пользователей и сотрудников организации, содержащих ссылки на веб-ресурсы с исполняемым кодом, содержащие исполняемый код в теле письма, содержащие просьбу сменить пароли, переслать пароли или свою персональную информацию и пр.;
- выборочная проверка исполнения политики «чистого стола» (стикеры с паролями, незаблокированные в отсутствие пользователя консоли, наличие конфиденциальных документов в офисе, доступных посетителям, оставленные без присмотра сотовые телефоны и пр.);
- звонки пользователям от имени персонала ИТ и ИБ отделов с просьбами получения/смены пароля, пересылки конфиденциальных документов и пр.;
- выбор целевых групп пользователей и определение ИПВ для тестирования каждой из групп;
- использование полученных в результате предыдущих этапов привилегий для получения НСД к ресурсам тестируемого объекта;
- документирование полученной в ходе тестирования информации, ее анализ с целью выработки рекомендаций по улучшению защищенности сети.

3. Комплексный тест. Комплексный тест на проникновение, в соответствии с методикой Positive Technology, наиболее близок к реальным действиям злоумышленников. Используя различные вышеуказанные мероприятия технического и социоинженерного тестов, аудиторы пытаются обойти существующие защитные механизмы с целью выполнения поставленных заказчиком задач.

Данную методику рекомендуется использовать для тестирования конечного продукта, уже введенного в эксплуатацию.

4. Результаты сравнительного анализа стандартов и методик

Обобщенные результаты анализ вышеуказанных методик тестирования на проникновение по различным частным критериям представлены в таблице 1.

Отметим, что наиболее проработанной методикой тестирования на проникновение как в теоретическом, так и в практическом плане является методика ISSAF. Методики OSSTMM, PETA и стандарты NIST SP 800-115, BSI носят в большей степени теоретический характер, при этом NIST SP 800-115 и BSI фактически являются стандартами стран-разработчиков, которых необходимо придерживаться, проводя тестирование на проникновение в этих странах. Стандарт PTES и методика PTF являются практико-ориентированными и содержат широкий набор технических рекомендаций и конкретных уязвимостей, которые необходимо проверять в ходе тестирования на проникновение.

Таблица 1 – Результаты сравнительного анализа стандартов и методик тестирования на проникновение

Характеристика	OSSTMM	ISSAF	OWASP	PTES	NIST SP 800-115	BSI	PETA	PTF	Positive Technologies
Рекомендации по обсуждению с заказчиком целей и задач тестирования	+	+	+	+	±	+	–	–	–
Рекомендации по подготовке договора на тестирование	+	+	–	±	±	±	–	–	–
Законодательные аспекты тестирования	±	+	–	–	+	+	–	–	–
Рекомендации по сборе информации об объекте тестирования	+	+	+	+	+	+	±	+	+
Подробные рекомендации по анализу и оценке уязвимостей	±	+	+	+	±	+	–	+	±
Рекомендации по этапам тестирования и их содержанию	+	+	+	+	+	+	+	+	+
Отдельные рекомендации по тестированию телекоммуникационных сетей	+	+	±	+	+	–	–	+	+
Отдельные рекомендации по тестированию беспроводных сетей	+	+	–	+	+	–	–	+	+
Отдельные рекомендации по тестированию веб-приложений	±	±	+	+	–	–	–	±	±
Отдельные рекомендации по проверке безопасности физической инфраструктуры	+	+	–	+	–	–	–	+	–
Отдельные рекомендации по проверке безопасности паролей	–	+	±	+	+	–	–	+	±
Отдельные рекомендации по проверке безопасности баз данных	–	+	±	–	–	–	–	–	–
Отдельные рекомендации по проверке безопасности исходного кода программ	–	+	±	–	–	–	–	–	–
Подробные рекомендации по использованию конкретных ИТВ для тестирования	–	+	+	+	±	±	–	+	±
Подробные рекомендации по использованию конкретных ИПВ и социальной инженерии для тестирования	±	+	–	+	±	–	–	–	±
Рекомендации по конкретному ПО, используемому для тестирования	–	+	±	+	–	±	–	±	–
Рекомендации по формированию отчета о тестировании	+	+	+	+	–	+	–	+	–
Анализ и рекомендации по устранению найденных уязвимостей	–	+	–	–	+	+	–	–	–

Примечание: «+» – имеется в полном объеме; «±» – имеется в кратком изложении или упоминается; «–» – данный материал отсутствует, либо изложен таким образом, что не представляет ценности для аудитора.

При этом отметим, что в стандарте PTES достаточно подробно изложены вопросы проверки безопасности беспроводных и телекоммуникационных сетей. Однако, нужно отметить, что подробность изложения технических аспектов, к сожалению, быстро устаревает с развитием ИТ-индустрии, выпуском новых программных и аппаратных платформ. В связи с этим вышеуказанные технические методики со временем быстро устаревают, а разработчики не всегда успевают поддерживать их в актуальном состоянии. Методика OWASP, по сравнению с другими методиками и стандартами, является узко-ориентированной на тестирование веб-приложений. Методика Positive Technology, в отличие от других методик, представлена в весьма сжатом и сокращенном виде, в связи с чем провести ее полный глубокий анализ затруднительно.

Заключение

В статье, представлены результаты сравнительного анализа существующих методик и стандартов тестирования на проникновение, их особенностей, достоинств, недостатков и рамок применимости.

Результаты представленного в статье анализа, в дальнейшем, авторы планируют использовать для разработки теоретических основ тестирования на проникновение, критериев оценки эффективности тестов, моделей уязвимости объектов КИИ к тестовым ИТВ и ИПВ.

Отдельные результаты исследования получены в ходе выполнения работ в рамках госбюджетной темы НИР СПИИРАН № 0073-2019-0004.

Литература

1. Макаренко С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. С. 1-29. DOI: 10.24411/2410-9916-2018-10101.

2. Макаренко С. И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. – СПб.: Наукоемкие технологии, 2018. – 122 с.

3. Кашаев Т. Р. Алгоритмы активного аудита информационной системы на основе технологий искусственных иммунных систем. Автореф. дис. … канд. техн. наук: 05.13.19. – М., 2008. – 19 с.

4. Марков А. С., Цирлов В. Л., Барабанов А. В. Методы оценки несоответствия средств защиты информации / под ред. А.С. Маркова. – М.: Радио и связь, 2012. – 192 с.

5. Скабцов Н. Аудит безопасности информационных систем. – СПб.: Питер, 2018. – 272 с.

6. Penetration Testing. Procedures & Methodologies. – EC-Council Press, 2011. – 237 p.

7. Kennedy D., O'Gorman J., Kearns D., Aharoni M. Metasploit. The Penetration Tester's Guide. – San Francisco: No Starch Press, 2011. – 299 p.

8. Makan K. Penetration Testing with the Bash shell. – Birmingham: Pact Publishing, 2014. – 133 p.

9. Cardwell K. Building Virtual Pentesting Labs for Advanced Penetration Testing. – Birmingham: Pact Publishing, 2016. – 518 p.

10. Краковский Ю.М., Курчинский Б.В., Лузгин А.Н. Интервальное прогнозирование интенсивности кибератак на объекты критической информационной инфраструктуры // Доклады Томского государственного университета систем управления и радиоэлектроники. 2018. Т. 21. № 1. С. 71-79.

11. Климов С. М. Имитационные модели испытаний критически важных информационных объектов в условиях компьютерных атак // Известия ЮФУ. Технические науки. 2016. № 8 (181). С. 27-36.

12. Климов С. М., Сычёв М. П. Стендовый полигон учебно-тренировочных и испытательных средств в области обеспечения информационной безопасности // Информационное противодействие угрозам терроризма. 2015. № 24. С. 206-213.

13. Петренко А. А., Петренко С. А. Киберучения: методические рекомендации ENISA // Вопросы кибербезопасности. 2015. № 3 (11). С. 2-14.

14. Бойко А. А., Дьякова А. В. Способ разработки тестовых удаленных информационно-технических воздействий на пространственно распределенные системы информационно-технических средств // Информационно-управляющие системы. 2014. № 3 (70). С. 84-92.

15. Бойко А. А., Дьякова А. В., Храмов В. Ю. Методический подход к разработке тестовых способов удаленного информационно-технического воздействия на пространственно распределенные системы информационно-технических средств // Кибернетика и высокие технологии XXI века XV Международная научно-техническая конференция. – Воронеж: НПФ «САКВОЕЕ», 2014. – С. 386-395.

16. Бойко А. А., Обущенко Е. Ю., Щеглов А. В. Особенности синтеза полного множества тестовых способов удаленного информационно-технического воздействия на пространственно распределенные системы информационно-технических средств // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2017. № 2. С. 33-45.

17. Щеглов А. В., Храмов В. Ю. Способ разработки тестовых удаленных информационно-технических воздействий на пространственно-распределенные системы информационно-технических средств // Сборник студенческих научных работ факультета компьютерных наук ВГУ ФГБОУ ВО «Воронежский государственный университет». – Воронеж, 2016. – С. 203-210.

18. Пакулин Н. В., Шнитман В. З., Никешин А. В. Автоматизация тестирования соответствия для телекоммуникационных протоколов // Труды Института системного программирования РАН. 2014. Т. 26. № 1. С. 109-148.

19. Баранова Е. К., Худышкин А. А. Особенности анализа безопасности информационных систем методом тестирования на проникновение // Моделирование и анализ безопасности и риска в сложных системах. Труды международной научной школы МАБР - 2015. – С. 200-205.

20. Баранова Е. К., Чернова М. В. Сравнительный анализ программного инструментария для анализа и оценки рисков информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. 2014. № 4. С. 160-168.

21. Бегаев А. Н., Бегаев С. Н., Федотов В. А. Тестирование на проникновение. – СПб: Университет ИТМО, 2018. – 45 с.

22. Богораз А. Г., Пескова О. Ю. Методика тестирования и оценки межсетевых экранов // Известия ЮФУ. Технические науки. 2013. № 12 (149). С. 148-156.

23. Дорофеев А. Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? // Защита информации. Инсайд. 2010. № 6 (36). С. 72-73.

24. Умницын М. Ю. Подход к полунатурному анализу защищенности информационной системы // Известия Волгоградского государственного технического университета. 2018. № 8 (218). С. 112-116.

25. Бородин М. К., Бородина П. Ю. Тестирование на проникновение средства защиты информации VGATE R2 // Региональная информатика и информационная безопасность. – СПб., 2017. – С. 264-268.

26. Полтавцева М. А., Печенкин А. И. Интеллектуальный анализ данных в системах поддержки принятия решений при тестировании на проникновение // Проблемы информационной безопасности. Компьютерные системы. 2017. № 3. С. 62-69.

27. Кадан А. М., Доронин А. К. Инфраструктурные облачные решения для задач тестирования на проникновение // Ученые записки ИСГЗ. 2016. Т. 14. № 1. С. 296-302.

28. Еременко Н. Н., Кокоулин А. Н. Исследование методов тестирования на проникновение в информационных системах // Master's Journal. 2016. № 2. С. 181-186.

29. Туманов С. А. Средства тестирования информационной системы на проникновение // Доклады Томского государственного университета систем управления и радиоэлектроники. 2015. № 2 (36). С. 73-79.

30. Кравчук А. В. Модель процесса удаленного анализа защищенности информационных систем и методы повышения его результативности // Труды СПИИРАН. 2015. № 1 (38). С. 75-93.

31. Горбатов В. С., Мещеряков А. А. Сравнительный анализ средств контроля защищенности вычислительной сети // Безопасность информационных технологий. 2013. Т. 20. № 1. С. 43-48.

32. Herzog P. OSSTMM – The Open Source Security Testing Methodology Manual. – New York: 2006. – 129 с. – URL: https://www.isecom.org/OSSTMM.3.pdf (дата обращения: 20.09.2020).

33. ISSAF - Information System Security Assesment Framework. – 2006. – 1264 с. – URL: http://www.oissg.org/issaf02/issaf0.1-5.pdf (дата обращения 20.09.2020).

34. OSWAP Testing Guide. Version 4. – 2014. – URL: https://www.owasp.org/index.php/OWASP_Testing_Project (дата обращения: 20.09.2020).

35. PTES – The Penetration Testing Execution Standard // Penetration Testing Execution Standarts [Электронный ресурс]. 30.04.2012. – URL: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines (дата обращения 20.09.2020).

36. NIST Special Publications 800-115. Technical Guide to Information Security Testing and Assessment. – USA, Gaithersburg: 2008. – 80 с. – URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (дата обращения 20.09.2020).

37. BSI – Study A Penetration Tesing Model. – Germany, Bonn, 2008 – 111 с. – URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf (дата обращения: 20.09.2020).

38. Klíma T. PETA: Methodology of information systems security penetration testing // Acta Informatica Pragensia. 2016. Т. 5. № 2. С. 98-117.

39. Orrey K. Penetration Test Framework // Vulnerability Assessment [Электронный ресурс]. 2014. – URL: http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html (дата доступа: 20.09.2020).

40. Тесты на проникновение // Positive Technologies [Электронный ресурс]. 2018. – URL: https://www.ptsecurity.com/ru-ru/services/pentest/ (дата обращения: 20.09.2020).

41. Аветисян А. И., Белеванцев А. А., Чукляев И. И. Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности. 2014. № 3 (4). С. 20-28.

References

1. Makarenko S. I. Audit of Information Security - the Main Stages, Conceptual Framework, Classification of Types. *Systems of Control, Communication and Security*, 2018, no. 1, pp. 1-29 (in Russian). DOI: 10.24411/2410-9916-2018-10101.

2. Makarenko S. I. *Security audit of critical infrastructure with special information impacts. Monograph*. Saint Petersburg, Naukoemkie tehnologii, 2018. 122 p. (in Russian).

3. Kashaev T. R. *Algoritmy aktivnogo audita informatsionnoi sistemy na osnove tekhnologii iskusstvennykh immunnykh sistem. Avtoreferat dis.* [Algorithms for active audit of information system based on artificial immune systems. Abstract D.Ph. thesis]. Moscow, 2008. 19 p. (in Russian).

4. Markov A. S., Tsirlov V. L., Barabanov A. V. *Metody otsenki nesootvetstviia sredstv zashchity informatsii* [Methods of compliance of information security]. Moscow, Radio i Sviaz Publ., 2012. 192 p. (in Russian).

5. Skabtsov N. *Audit bezopasnosti informatsionnykh system* [Security audit of information systems]. Saint Petersburg, Piter Publ., 2018. 272 p. (in Russian).

6. *Penetration Testing. Procedures & Methodologies*. EC-Council Press, 2011. 237 p.

7. Kennedy D., O'Gorman J., Kearns D., Aharoni M. *Metasploit. The Penetration Tester's Guide*. San Francisco, No Starch Press, 2011. 299 p.

8. Makan K. *Penetration Testing with the Bash shell*. Birmingham, Pact Publishing, 2014. 133 p.

9. Cardwell K. *Building Virtual Pentesting Labs for Advanced Penetration Testing*. Birmingham, Pact Publishing, 2016. 518 p.

10. Krakovsky Y. M., Kurchinsky B. V., Luzgin A. N. Cyber-attack intensity interval forecasting on objects of critical information infrastructure. *Proceedings of Tomsk State University of Control Systems and Radioelectronics*, 2020, vol. 21, no. 1, pp. 71-79 (in Russian).

11. Klimov S. M. Imitating models of testing the critically important information objects in the conditions of computer attacks. *Izvestiya SFedU. Engineering Sciences*, 2016, vol. 181, no. 8, pp. 27-36 (in Russian).

12. Klimov S. M., Sychev M. P. Poster polygon for training and testing facilities in the field of information security. *Information counteraction to the terrorism threats*, 2015, no. 24, pp. 206-213 (in Russian).

13. Petrenko A. A., Petrenko S. A. Cyber education: methodical recommendations ENISA. *Voprosy kiberbezopasnosti*, 2015, vol. 11, no. 3, pp. 2-14 (in Russian).

14. Boyko A. A., Djakova A. V. Method of Developing Test Remote Information-Technical Impacts on Spatially Distributed Systems of Information-Technical Tools. *Informatsionno-upravliaiushchie sistemy*, 2014, vol. 70, no. 3, pp. 84-92 (in Russian).

15. Boyko A. A., Djakova A. V. Hramov V. Ju. Metodicheskij podhod k razrabotke testovyh sposobov udalennogo informacionno-tehnicheskogo vozdejstvija na prostranstvenno raspredelennye sistemy informacionno-tehnicheskih sredstv [Methodological approach to the development of test methods for remote information technology impact on spatially distributed systems of information technology tools]. *Kibernetika i vysokie tehnologii XXI veka XV Mezhdunarodnaja nauchno-tehnicheskaja konferencija* [*Cybernetics and high technologies of the XXI century XV international scientific and technical conference*]. Voronezh, SAKVOEE, 2014. pp. 386-395 (in Russian).

16. Boyko A. A., Obushenko E. Y., Shcheglov A. V. About synthesis of a full set of test methods of remote information-technical impacts on spatially distributed systems of information-technical tools. *Proceedings of Voronezh State University. Series: Systems analysis and information technologies*, 2017, no. 2, pp. 33-45 (in Russian).

17. Shcheglov A. V., Hramov V. Ju. Sposob razrabotki testovyh udalennyh informacionno-tehnicheskih vozdejstvij na prostranstvenno-raspredelennye sistemy informacionno-tehnicheskih sredstv [Method for developing test remote information technology impacts on spatially distributed information technology systems]. *Sbornik studencheskih nauchnyh rabot fakul'teta komp'juternyh nauk «Voronezhskij gosudarstvennyj universitet»* [*Collection of student research papers of the faculty of*

computer science of Voronezh state University]. Voronezh, 2016, pp. 203-210 (in Russian).

18. Pakulin N. V., Shnitman V. Z., Nikeshin A. V. Avtomatizatsiia testirovaniia sootvetstviia dlia telekommunikatsionnykh protokolov [Automation of compliance testing for telecommunication protocols]. *Proceedings of the Institute for System Programming of the RAS*, 2014, vol. 26, no. 1, pp. 109-148 (in Russian).

19. Baranova E. K., Hudyshkin A. A. Osobennosti analiza bezopasnosti informacionnyh sistem metodom testirovanija na proniknovenie [Features of information system security analysis by penetration testing]. *Modelirovanie i analiz bezopasnosti i riska v slozhnyh sistemah. Trudy mezhdunarodnoj nauchnoj shkoly MABR – 2015* [*Modeling and analysis of security and risk in complex systems. Proceedings of the international scientific school MABR - 2015*], 2015, pp. 200-205 (in Russian).

20. Baranova E. K., Chernova M. V. Comparative analysis of programming tools for cybersecurity risk assessment. *Information Security Problems. Computer Systems*, 2014, no. 4, pp. 160-168 (in Russian).

21. Begaev A. N., Begaev S. N., Fedotov V. A. *Testirovanie na proniknovenie* [*Penetration testing*]. Saint Petersburg, Saint Petersburg National Research University of Information Technologies, Mechanics and Optics Publ., 2018. 45 p. (in Russian).

22. Bogoras A. G., Peskova O. Y. Methodology for testing and assessment of firewalls. *Izvestiya SFedU. Engineering Sciences*, 2013, vol. 149, no. 12, pp. 148-156 (in Russian).

23. Dorofeev A. Testirovanie na proniknovenie: demonstracija odnoj ujazvimosti ili obektivnaja ocenka zashhishhennosti? *Zasita informacii. Inside*, 2010, vol. 36, no. 6, pp. 72-73 (in Russian).

24. Umnitsyn M. Y. Approach to semi-natural security evaluation of information system. *Izvestia VSTU*, 2018, vol. 218, no. 8, pp. 112-116

25. Borodin M. K., Borodina P. Ju. Testirovanie na proniknovenie sredstva zashhity informacii VGATE R2 [VGATE R2 information security penetration testing]. *Regional'naja informatika i informacionnaja bezopasnost* [*Regional Informatics and information security*], Saint Petersburg, 2017, pp. 264-268 (in Russian).

26. Poltavtseva M. A., Pechenkin A. I. Data mining methods in penetration tests decision support system. *Information Security Problems. Computer Systems*, 2017, no. 3, pp. 62-69 (in Russian).

27. Kadan A. M., Doronin A. K. Cloud infrastructure solutions for penetration testing. *Uchenye zapiski ISGZ*, 2016, vol. 14, no. 1, pp. 296-302 (in Russian).

28. Eremenko N. N., Kokoulin A. N. Research of methods of penetration testing in information systems. *Master's Journal*, 2016, no. 2, pp. 181-186 (in Russian).

29. Tumanov S. A. Penetration testing tools for information systems. *Proceedings of Tomsk State University of Control Systems and Radioelectronics*, 2015, vol. 36, no. 2, pp. 73-79 (in Russian).

30. Kravchuk A. V. The model of process of remote security analysis of information systems and methods of improving it's performance. *SPIIRAS Proceedings*, 2015, vol. 38, no. 1, pp. 75-93 (in Russian).

31. Gorbatov V. S., Meshcheryakov A. A. Comparative analysis of computer network security scanners. *IT Security*, 2013, vol. 20, no. 1, pp. 43-48 (in Russian).

32. Herzog P. *OSSTMM – The Open Source Security Testing Methodology Manual*. New York, 2006. 129 p. Available at: https://www.isecom.org/OSSTMM.3.pdf (accessed 20 September 2020).

33. *ISSAF - Information System Security Assesment Framework*. 2006. 1264 p. Available at: http://www.oissg.org/issaf02/issaf0.1-5.pdf (accessed 20 September 2020).

34. *OSWAP Testing Guide. Version 4*. 2014. Available at: https://www.owasp.org/index.php/OWASP_Testing_Project (accessed 20 September 2020).

35. *PTES – The Penetration Testing Execution Standard*. 30 April 2012. Available at: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines (accessed 20 September 2020).

36. *NIST Special Publications 800-115. Technical Guide to Information Security Testing and Assessment*. USA, Gaithersburg, 2008. 80 p. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (accessed 20 September 2020).

37. *BSI – Study A Penetration Tesing Model*. Germany, Bonn, 2008 111 p. Available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf (accessed 20 September 2020).

38. Klíma T. PETA: Methodology of information systems security penetration testing. *Acta Informatica Pragensia*, 2016, vol. 5, no. 2, pp. 98-117.

39. Orrey K. Penetration Test Framework. Vulnerability Assessment, 2014. Available at: http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html (accessed 20 September 2020).

40. Testy na proniknovenie [Penetration tests]. *Positive Technologies*, 2018. Available at: https://www.ptsecurity.com/ru-ru/services/pentest/ (accessed 20 September 2020).

41. Avetisyan A. I., Belevantsev A. A., Chucklyaev I. I. The technologies of static and dynamic analyses detecting vulnerabilities of software. *Voprosy kiber-bezopasnosti*, 2014, vol. 4, no. 3, pp. 20-28 (in Russian).

Статья поступила 02 октября 2020 г.

Информация об авторах

Макаренко Сергей Иванович – доктор технических наук, доцент. Ведущий научный сотрудник. Санкт-Петербургский Федеральный исследовательский центр РАН. Профессор кафедры информационной безопасности. Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина). Область научных интересов: сети и системы

связи; радиоэлектронная борьба; информационное противоборство. E-mail: mak-serg@yandex.ru

Адрес: 199178, Россия, Санкт-Петербург, 14 линия, д. 39.

Смирнов Глеб Евгеньевич – соискатель ученой степени кандидата наук. Преподаватель кафедры информационной безопасности. Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина). Область научных интересов: информационная безопасность. E-mail: science.cybersec@yandex.ru

Адрес: 197376, Россия, Санкт-Петербург, ул. Профессора Попова, д. 5.

Analysis of penetration testing standards and methodologies

S. I. Makarenko, G. E. Smirnov

Relevance. *At present, the issues of security of information systems of critical infrastructure objects are becoming important. At the same time, the current tasks of the audit of information security (IS) of critical infrastructure objects, as a rule, are limited to checking them for compliance with IS requirements. However, with this approach to auditing, it often remains unclear the resistance of these objects to real attacks by malefactors. To check such stability, objects are subjected to a testing procedure, namely, penetration testing. Analysis of domestic publications in this area shows that there is no systematic approach to penetration testing in domestic practice. In this regard, it is relevant to analyze and systematize the best foreign approaches and practices for penetration testing.* ***The purpose of this paper*** *is a comparative analysis of existing foreign and domestic penetration testing techniques and standards.* ***Results***. *The article presents the results of the analysis of the following foreign standards and methods: OSSTMM, ISSAF, OWASP, PTES, NIST SP 800-115, BSI, PETA, PTF, as well as the domestic method Positive Technology. The elements of novelty of the paper are the identified features, advantages, disadvantages and the scope of applicability of existing standards and penetration testing methods.* ***Practical significance***. *The material of the article can be used to form the initial data, the sequence of stages and their content, in a practical audit of the security of information systems of critical information infrastructure objects by penetration testing.*

Key words: *penetration testing, standard, methodology, audit, information security, critical information infrastructure, information technology impact, information and psychological impact, OSSTMM, ISSAF, OWASP, PTES, NIST SP 800-115, BSI, PETA, PTF, Positive Technology.*

Information about Authors

Sergey Ivanovich Makarenko – Dr. habil. of Engineering Sciences, Docent. Leading Researcher. St. Petersburg Federal Research Center of the Russian Academy of Sciences. Professor of Information Security Department. Saint Petersburg Electrotechnical University 'LETI'. Field of scientific research: stability of network against the purposeful destabilizing factors; electronic warfare; information struggle. E-mail: mak-serg@yandex.ru

Address: Russia, 197376, Saint Petersburg, 14th Linia, 39.

Gleb Evgenevich Smirnov – doctoral candidate. Lecturer at the Department of Information Security. Saint Petersburg Electrotechnical University "LETI". Field of scientific research: information security. E-mail: science.cybersec@yandex.ru

Address: Russia, 197376, Saint Petersburg, Professor Popov street 5.