ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ НА ОСНОВЕ СТАНДАРТА NIST SP 800-115

Макаренко С.И.[1]

Актуальность. *В настоящее время вопросы безопасности информационных систем объектов критической инфраструктуры приобретают важное значение. Вместе с тем текущие задачи аудита информационной безопасности (ИБ) объектов критической инфраструктуры, как правило, ограничиваются проверкой их на соответствие требованиям по ИБ со стороны руководящих документов. Однако при таком подходе к аудиту, зачастую, остается неясным защищенность этих объектов от реальных атак злоумышленников. Для объективной проверки такой защищенности объекты подвергают процедуре тестирования, а именно – тестированию на проникновение. Указания по проведению такого тестирования, например, содержаться в рекомендациях Банка России, по проверке ИБ банковских систем. Однако, сдерживающим фактором в проведении тестирование на проникновение отечественных объектов критической инфраструктуры является отсутствие единого отечественного стандарта проведения такого тестирования.*

Целью работы *является анализ американского стандарта тестирования NIST SP 800-115 в интересах оценки целесообразности его использования для разработки отечественного проекта стандарта тестирования на проникновение.*

Методы исследования. *Для достижения цели работы в работе использованы методы анализа и декомпозиции из теории системного анализа.*

Результаты. *В статье поведен глубокий анализ стандарта NIST SP 800-115, в частности рассмотрены: типы мероприятий оценки ИБ; этапы оценки ИБ; способы анализа и тестирования, используемые при оценке ИБ; типы и последовательность проведения тестирования на проникновение; проверяемые уязвимости; рекомендуемый инструментарий проведения анализа и тестирования, представленные в NIST SP 800-11. Сделаны выводы о сильных и слабых сторонах стандарта NIST SP 800-115. Представлены рекомендации по его использованию при разработки отечественного проекта стандарта тестирования на проникновение.*

Ключевые слова: *тестирование на проникновение, компьютерная атака, NIST SP 800-115, тестирование, тестирование безопасности, социальная инженерия, тестирование программ, уязвимость, сканирование сети.*

DOI: 10.21681/2311-3456-2022-3-44-57

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) информационных систем (ИС) объектов КИИ и обеспечения ее защищённости.

В подавляющем числе случаев аудит ИБ ИС проводиться на основе сравнительного анализа с нормативно-правовой документацией, регламентирующей обеспечение ИБ, или на основе анализа рисков. Вместе с тем, в предыдущих работах автора [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 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 для такого подхода используется термин «тестирование на проникновение» (в англоязычной литературе – «penetration testing»), а также другие термины «активный аудит», «инструментальный аудит», «тесто-

1 Макаренко Сергей Иванович, доктор технических наук, доцент, ведущий научный сотрудник Санкт-Петербургского Федерального исследовательского центра РАН, Санкт-Петербург, Россия. E mail: mak-serg@yandex.ru, ORCID: 0000-0001-9385-2074

вые информационно-технические воздействия», «тестовые кибератаки» 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 является реализация в отношении ИС объектов КИИ тестов на проникновение – воздействий на ИС тестовых компьютерных атак, аналогичных реальным атакам, которые, с высокой степенью вероятности, могут использоваться злоумышленниками. Целесообразность проведения такого тестирования подтверждается рекомендациями Банка России РС БР ИББС-2.6-2014 о необходимости тестирования на проникновение банковских ИС на стадии приема и ввода в эксплуатацию, на стадии эксплуатации и на стадии модернизации.

Несмотря на то, что такое тестирование представляет собой достаточно адекватный и максимально приближенный к реальности подход к оценке защищенности, он не получил широкого распространения. Основной причиной этого, на взгляд автора, является отсутствие единой отечественной методики проведения тестирования на проникновение, которая бы была утверждена и рекомендована регулирующими органами в сфере ИБ к использованию при аудите ИБ объектов КИИ. Вместе с тем, в ведущих зарубежных странах разработаны и введены в действие многочисленные стандарты и методики тестирования на проникновение, в частности, такие как OSSTMM, ISSAF, OWASP, PTES, NIST SP 800-115, BSI, PETA, PTF [3]. Целесообразно взяв за основу эти зарубежные стандарты и методики, провести их анализ, и на его основе сформировать научно-обоснованный отечественный проект стандарта на проникновение, который бы вбирал в себя наилучшие зарубежные практики в области тестирования.

Вопросы проведения тестирования на проникновения и исследования защищенности ИС путем целенаправленного использования компьютерных атак довольно широко рассматриваются в научных работах отечественных специалистов: А.С. Маркова [4-6, 8], В.Л. Цирлова, А.В. Барабанова [4-6], Ю.В. Раткина [5, 8], А.В. Дорофеева [7, 8], С.М. Климова [9, 10], А.А. Бойко [11-14], А.Н. Бегаева, С.Н. Бегаева, В.А. Федотова [15]. Практические аспекты проведения тестирования на проникновение рассматриваются в работах Н. Скабцова [16] и А.А. Бирюкова [17]. Вместе с тем, в этих работах не ставится и не рассматривается возможность разработки отечественного проекта стандарта на проникновение.

Целью статьи является анализ стандарта тестирования на проникновение NIST SP 800-115 [18] в интересах оценки целесообразности его использования для разработки отечественного проекта стандарта тестирования на проникновение.

Данная статья продолжает и развивает предыдущие работы автора [1-3, 19, 20], направленные на развитие теоретического базиса тестирования на проникновение.

Введем базовую терминологию, которую будем использовать в дальнейшем.

Объект – информационная система, информационно-телекоммуникационная или компьютерная сеть, автоматизированная система управления, в отношение которого проводится аудит/тестирование ИБ.

Тестирование – проверка выполнения требований к объекту при помощи наблюдения за ее работой в конечном наборе специально выбранных ситуаций.

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

Аудитор – специалист, который проводит аудит, экспертизу и тестирование объекта.

Компьютерная атака – целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

Тестирование на проникновение – экспериментальная проверка с целью оценивания состояния ИБ и выявления уязвимостей объекта тестирования (тестируемой системы) путем интегрального и целенаправленного применения против него компьютерных атак, социальной инженерии, а также других способов анализа и проверки уязвимостей.

Социальная инженерия – совокупность способов изменения установок людей, управления поведением и действиями человека без использования технических средств, основанная на использовании слабостей человека и особенностей его психики.

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.

Уязвимость – недостаток объекта, эксплуатация которого делает возможным реализацию инцидента, на-

несение объекта повреждений любой природы, либо снижение эффективности его функционирования.

Оценка ИБ в соответствии со стандартом NIST SP 800-115

Стандарт NIST SP 800-115 – Technical Guide to Information Security Testing and Assessment [18] 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.

1. Типы мероприятий оценки ИБ

Оценка ИБ в соответствии с NIST SP 800-115 – это процесс определения того, насколько оцениваемый объект соответствует критериям обеспечения ИБ. Для этого рекомендуется использовать три типа мероприятий, направленных на оценку ИБ:

1) анализ – это процесс экспертизы, проверки, изучения и наблюдения объекта оценки для понимания его функциональности и степени защищенности (соответствует использованию способов анализа, рассмотренных в подразделе 3.2 данной работы);

2) тестирование – это процесс использования объекта оценки в определенных условиях для сравнения фактического и ожидаемого поведения этого объекта (соответствует использованию способов тестирования, рассмотренных в подразделе 3.3 данной работы);

3) интервью – это процесс проведения опроса отдельных лиц или групп лиц внутри организации для облегчения понимания функциональности оцениваемого объекта, а также для получения дополнительной информации о системе (не является основным типом мероприятий оценки ИБ, а используется дополнительно к двум вышеуказанным, преимущественно совместно с мероприятиями анализа).

В стандарте NIST SP 800-115 рассматриваются способы анализа и способы технического тестирования ИБ, которые можно использовать для выявления, проверки и оценки технических уязвимостей, а также для помощи организациям в понимании и улучшении состояния ИБ их объектов.

Оценка ИБ, в соответствии со стандартом NIST SP 800-115, предназначено для решения следующих задач:

1) обеспечить адекватность оценки ИБ целевых объектов в интересах снижения риска проведения атак злоумышленниками;

2) минимизировать риски нарушения нормального функционирования объектов поверяемой системы при проведении тестирования на проникновение;

3) сформировать мероприятия по выявлению, анализу и ликвидации выявленных уязвимостей целевых объектов.

2. Этапы оценки ИБ

В стандарте NIST SP 800-115 процесс оценки ИБ декомпозирован на три основных этапа.

1) Планирование. Этот этап является критически важным для успешного оценки ИБ тестируемого объекта. На этом этапе проводится сбор информации, необходимой для выполнения тестирования, такой как: тестируемые объекты, угрозы и уязвимости объектов, проверяемые меры обеспечения ИБ, используемые способы анализа и оценки уязвимостей. Этот этап завершается разработкой плана тестирования, в котором отражаются цели и задачи тестирования, области и объекты тестирования, ограничения, выделенные ресурсы, используемые способы, роли и обязанности аудиторов, ожидаемые результаты и сроки.

2) Анализ и проверка уязвимостей. Основные цель этого этапа – выявить уязвимости тестируемых объектов и проверить возможность их эксплуатации в интересах нанесения ущерба. На этом этапе реализуются способы анализа и способы проверки уязвимостей, предусмотренные планом тестирования. Результатом этого этапа является перечень актуальных уязвимости объектов и организационных процессов.

3) Анализ результатов оценки ИБ и пост-тестовые мероприятия. Данный этап предусматривает анализ выявленных уязвимостей, определение основных причин их появления, выработку рекомендаций по устранения уязвимостей. Все эти аспекты включаются в итоговый отчет по результатам тестирования.

3. Способы оценки ИБ

3.1. Общие сведения о способах оценки ИБ и их классификация

Существует множество способов проведения оценки ИБ и проверки безопасности, которые можно использовать для оценки состояния целевых объектов, систем и компьютерных сетей. В NIST SP 800-115 все способы оценивания ИБ сгруппированы в следующие две основные категории:

1) Способы анализа – это способы экспертизы, проверки, изучения и наблюдения, используемые для оценки объектов, систем, приложений, сетей, политик

и процедур для обнаружения уязвимостей, которые, как правило, выполняются аудитором вручную. Данные способы включают в себя:

1.1) анализ документации;

1.2) анализ журналируемых событий;

1.3) анализ наборов правил;

1.4) анализ конфигураций системы;

1.5) сканирование сети;

1.6) проверку целостности файлов.

2) Способы проверки уязвимостей – эти способы практически подтверждают наличие уязвимостей у проверяемых объектов и могут выполняться как вручную, так и с использованием специализированных технических средств и программного обеспечения (ПО). Способы проверки уязвимостей у объектов включают в себя:

2.1) тестирование паролей;

2.2) тестирование на проникновение;

2.3) тестирование безопасности приложений;

2.4) социальную инженерию.

Для обеспечения высокой степени полноты тестирования рекомендуется комбинировать различные способы в рамках отведенных на тестирование время, финансовые ресурсы и компетенции персонала.

В стандарте NIST SP 800-115 подробно объясняется суть и содержание различных вышеуказанных способов, но не уточняется, какие способы следует использовать при каких обстоятельствах. Что, с одной стороны, является недостатком этого стандарта, с другой стороны, дает организациям гибкость в выборе и использовании конкретных способов.

3.2. Способы анализа

Способы анализа используются для пассивного изучения объектов, систем, приложений, сетей, политик и процедур в целях обнаружения уязвимостей ИБ и, в своем большинстве, ориентированы на проверку и оценку документов. С помощью анализа можно собрать информацию о системе в интересах формирования перечня тестируемых объектов и используемых способов проверки уязвимостей. Поскольку способы анализа пассивны, их использование несет минимальный риск для функционирования систем и сетей.

Далее более подробно рассмотрим основные способы анализа.

3.2.1. Анализ документации

Анализ документации позволяет определить являются ли технические аспекты политик и процедур ИБ актуальными и действительно обеспечивающими надлежащий уровень ИБ. Как правило, внутренние документы служат основой для обеспечения безопасности организации. Необходимо проверить на техническую точность и полноту процедур следующие документы организации:

1) политики безопасности;

2) архитектуру и требования по безопасности;

3) типовые рабочие процедуры обеспечения ИБ на рабочих местах;

4) планы безопасности системы и соглашения об авторизации;

5) планы и алгоритмы реагирования на инциденты.

Анализ документации может выявить «пробелы» и слабые места, которые могут привести к отсутствию или неправильной реализации мер безопасности. Аудиторы обычно проверяют, соответствует ли документация организации стандартам и правилам и ищут политики, которые являются несовершенными или устаревшими. Анализ документации не гарантирует, что меры безопасности реализованы должным образом, они показывают только то, что существуют указания и инструкции для обеспечения определенного уровня безопасности. Соблюдение персоналом этих указаний и инструкций – это отдельный вопрос, который выходит за рамки анализа документации.

3.2.2. Анализ журналируемых событий

Анализ журналов фиксируемых событий позволяет определить регистрируют ли системы управления безопасностью правильную информацию и соблюдает ли организация свои политики управления журналами. Аудит журналируемых событий позволяет выявить такие проблемы, как неправильно настроенные службы и средства управления ИБ, факты НСД и попытки вторжения.

Далее представлены примеры журналов и журналируемых событий различных объектов ИС, которые могут быть полезны при проведении оценки ИБ:

1) сервер аутентификации или системные журналы могут регистрировать успешные и неудачные попытки аутентификации;

2) системные журналы могут содержать информацию о запуске и завершении работы операционной системы (ОС), служб, об установке неавторизованного ПО, доступе к файлам, изменениях политики безопасности, изменениях учетных записей (например, создании и удалении учетной записи, назначении привилегий учетной записи) и использовании привилегий;

3) журналы систем обнаружения вторжений IDS (Intrusion Detection System) и систем предотвращения вторжений IPS (Intrusion Prevention System), мо-

гут регистрировать факты злонамеренных действий и ненадлежащее использование привилегий;

4) журналы брандмауэров и маршрутизаторов могут содержать данные о исходящих соединениях, указывающих на взломанные внутренние устройства. Кроме того, они могут регистрировать попытки несанкционированного подключения и ненадлежащее использование сетевого оборудования;

5) журналы различных приложений могут отображать попытки несанкционированного подключения, изменения учетных записей, использование привилегий и информацию об использовании приложения или базы данных.

6) журналы антивируса могут содержать данные о событиях неудавшиеся попытки обновления и другие признаки устаревших сигнатур и ПО.

7) журналы безопасности IDS/IPS могут содержать информацию об известных уязвимых в используемых ОС, службах и приложениях.

3.2.3. Анализ наборов правил

Набор правил – это совокупность правил или сигнатур, с которыми сравнивается сетевой трафик или активность системы для определения, какое действие следует предпринять системе. Анализ наборов правил выполняется для проверки их полноты и выявления «слабых мест» в технических и программных средствах обеспечения ИБ в интересах выявления таких нарушений ИБ как: уязвимости компьютерных сетей, нарушения политик безопасности, использование небезопасных или уязвимых каналов связи. Этот анализ также может выявить недостатки, которые негативно влияют на качество выполнения набора правил.

При проведении анализа целесообразно проверить наборы правил сетевого и хост-брандмауэра, наборы правил IDS/IPS, а также списки управления доступом маршрутизатора.

3.2.4. Анализ конфигураций системы

Анализ конфигураций системы – это процесс выявления слабых мест в настойках и элементах управления конфигурацией безопасности системы. Он ориентирован на выявление систем, которые не настроены в соответствии с политиками безопасности или настроены так, что создают угрозу нарушения безопасности.

Данный тип проверки по отношению к ОС может обнаружить не использующиеся службы и приложения, неправильные настройки учетных записей и паролей пользователей, а также неправильные настройки ведения журналов событий и резервного копирования. Примерами файлов конфигурации безопасности, которые можно просмотреть, являются параметры политики безопасности ОС Windows и файлы конфигурации безопасности ОС Unix, например, в папке etc.

Так как анализ конфигураций системы вручную требуют много времени, рекомендуется использовать протокол автоматизации управления данными безопасности SCAP (Security Content Automation Protocol).

3.2.5. Сканирование сети

Сканирование сети – это пассивный способ исследования, который отслеживает сетевую связь объектов, идентифицирует используемые сетевые протоколы и проверяет заголовки пакетов и пользовательских данных, чтобы выявить интересующую информацию.

Цели использования сетевого сканирования:

1) захват и воспроизведение сетевого трафика;

2) выполнение пассивного анализа сети (например, определение активных устройств в сети);

3) определение ОС, приложений, служб и протоколов, включая незащищенные и несанкционированные протоколы;

4) выявление несанкционированных и несоответствующих действий, таких как незашифрованная передача конфиденциальной информации;

5) сбор полезной информации, такой как незашифрованные имена пользователей и пароли.

Сканирование сети, в соответствии со стандартом NIST SP 800-115, может включать в себя проведение следующих мероприятиями:

1) доступ и сканирование проводной сетевой инфраструктуры;

2) доступ и сканирование беспроводных сетей;

3) сканирование возможности доступа к отдельным компьютерным системам пользователей с использованием таких радиоинтерфейсов как Wi-Fi (IEEE 802.11) или BlueTooth (IEEE 802.15.1).

Мероприятия и сценарии доступа и проведения сканирования этих сетей подробно рассмотрены в разделе 4 стандарта NIST SP 800-115.

Для проведения сканирования сети используется специальное ПО – сниффер (от англ. sniffer – вынюхиватель). В некоторых случаях необходимо дополнительное оборудование: сетевой концентратор, ответвитель или коммутатор с поддержкой технологии зеркалирования трафика SPAN (Switch Port Analyzer), при которой трафик, передаваемый на все другие порты коммутатор, копируется в порт, где установлен сканер.

Организации могут развернуть сетевые сканеры в нескольких местах:

1) по периметру системы для оценки трафика, входящего и выходящего из сети;

2) за брандмауэрами, чтобы убедиться, что наборы правил точно фильтруют трафик;

3) за системами IDS/IPS, чтобы определить, запускаются ли сигнатуры и на них реагируют должным образом;

4) перед критически важной системой или приложением для оценки его сетевой активности;

5) в определенном сегменте сети для проверки зашифрованных протоколов.

3.2.6. Проверка целостности файлов

Средства проверки целостности файлов позволяют определить, были ли изменены системные файлы объектов, вычисляя и сохраняя контрольную сумму для каждого защищенного файла, а также создавая базу данных (БД) контрольных сумм файлов. Сохраненные контрольные суммы позже пересчитываются для сравнения их текущего значения с ранее сохраненным значением, что позволяет определить факт нарушения целостности файла идентифицирует изменения файла.

Несмотря на то, что проверка целостности фалов не требует высокой степени взаимодействия с человеком, его следует использовать осторожно, чтобы гарантировать его эффективность. Проверка целостности файлов наиболее эффективна, когда системные файлы ОС сравниваются с эталонной БД, созданной с использованием заведомо безопасной системы – это позволяет гарантировать, что эталонная БД не была построена с использованием скомпрометированных файлов. Эталонная БД должна храниться в автономном режиме, чтобы злоумышленники не взломали эту БД и не смогли изменить контрольные суммы файлов. Кроме того, поскольку исправления и другие обновления изменяют файлы, БД контрольных сумм следует поддерживать в актуальном состоянии.

3.3. Способы проверки уязвимостей

3.3.1. Тестирование паролей

Когда пользователь вводит пароль, создается хэш введенного пароля, который в дальнейшем сравнивается с сохраненным хэшем фактического пароля пользователя. Если хэши совпадают, то считается что аутентификация пользователя в системе произошла и пользователь получает определенный набор привилегий, который предусмотрен политикой безопасности.

Тестирование паролей – это процесс восстановления паролей из хэшей паролей, хранящихся в системе. Обычно этот процесс выполняется во время аудита системы для выявления учетных записей со слабыми паролями.

Взлом паролей выполняется для хэшей, которые либо перехватываются сетевым анализатором трафика при передаче по сети, либо извлекаются из компьютерной системы, что обычно требует доступа на уровне администратора или физического доступа к целевой системе. Как только эти хэши получены, специализированное ПО типа «взломщик паролей» генерирует дополнительные хэши, пока не будет найдено совпадение или пока аудитор не остановит попытку взлома.

Данный способ тестирования может быть использован для проверки требований к уровню сложности пароля, исключения использования типовых фраз или паролей по умолчанию. Если в организации действует политика истечения срока действия пароля, этот способ проверки может использоваться с интервалами, совпадающими с предполагаемым сроком действия пароля. Использование данного способа контроля паролей, выполняемый в автономном режиме, практически не влияет на быстродействие системы или сети, а преимущества этой операции включают проверку как политики паролей организации, так и проверку ее соответствия требованиям ИБ.

3.3.2. Тестирование на проникновение

Тестирование на проникновение – это тестирование, при котором аудиторы воспроизводят реальные компьютерные атаки потенциальных злоумышленников, чтобы оценить уровень защищенности тестируемого объекта.

Ввиду важности, многоаспектности и комплексности этого способа проверки уязвимостей, рассмотрение тестирования на проникновение вынесено в отдельный подраздел – подраздел 4 данной работы.

3.3.3. Тестирование безопасности приложений

Тестирование и проверка безопасности приложений помогают организации определить, содержит ли ее специализированное и прикладное ПО уязвимости, которые можно использовать, правильно ли работает ПО, безопасно ли оно взаимодействует с пользователями и другими приложениями, является ли безопасной среда их исполнения.

Безопасность приложений можно оценить несколькими способами, от анализа исходного кода до тести-

рования готового приложения. Многие тесты безопасности подвергают приложение известным сценариям атак, типичным для этого типа приложений. Эти сценарии могут быть ориентированы непосредственно на само приложение или могут пытаться атаковать его косвенно, ориентируясь на среду выполнения (например, на ОС) или на инфраструктуру безопасности. Примерами таких сценариев атак разведка и раскрытие конфиденциальной информации, использование эксплойтов аутентификации, эксплойтов управления сеансом, использование спуфинга, инъекции команд, атаки типа «отказ в обслуживании».

Оценка безопасности приложения должна быть интегрирована в жизненный цикл разработки ПО этого приложения, чтобы гарантировать, что она выполняется на протяжении всего жизненного цикла.

Например, контроль безопасности кода может выполняться во время его формирования. Не следует ждать, пока все приложение будет готово и для его тестирования. Тестирование безопасности также следует проводить периодически после того, как приложение запущено в «тиражирование»; при внесении значительных исправлений, обновлений или других модификаций; при значительных изменениях в среде, в которой функционирует приложение.

3.3.4. Социальная инженерия

На начальных этапах сбора информации о целевых объектах, а также на отдельных этапах проникновения в систему среди злоумышленников широко распространены приемы социальной инженерии. Это позволяет сделать вывод о том, что при проведении оценки ИБ помимо технических составляющих обеспечения безопасности в обязательном порядке необходимо учитывать психологические особенности персонала и лиц, принимающих решения. Для этого аудиторы могут использовать способы социальной инженерии с целью оценки вероятности нарушения ИБ с учетом «человеческого фактора».

Социальная инженерия – совокупность способов изменения установок людей, управления поведением и действиями человека без использования технических средств, основанная на использовании слабостей человека и особенностей его психики.

Способы социальной инженерии ориентированы на обман или введение в заблуждение отдельных лиц из числа персонала организации с целью принудить его раскрыть важную информацию, которая может быть использована для атаки на тестируемые объекты, или совершить действия, направленные на нарушение политики безопасности.

Результаты проверки на уязвимость на основе способов социальной инженерии должны использоваться для повышения безопасности организации, а не для наказания отдельных лиц, в отношении которых применение этих способов оказалось успешным.

По итогам использования способов социальной инженерии аудиторы должны подготовить подробный окончательный отчет, в котором будут описаны как успешные, так и неудачные попытки реализации этих способов (возможно в обезличенном виде), а также причины и недостатки политики безопасности, влияющие на успех попыток. Это поможет организации адаптировать свои программы обучения для сотрудников по вопросам безопасности к использованию способов социальной инженерии со стороны реальных злоумышленников.

4. Тестирование на проникновение

4.1. Общие сведения

Тестирование на проникновение – экспериментальная проверка с целью оценивания состояния ИБ и выявления уязвимостей объекта тестирования (тестируемой системы) путем интегрального и целенаправленного применения против него компьютерных атак.

В процессе тестирования аудиторы воспроизводят реальные компьютерные атаки потенциальных злоумышленников, чтобы оценить уровень защищенности тестируемого объекта.

Компьютерная атака – целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

Целями проведения тестирования на проникновение является определение:

1) уровня фактической защищенности тестируемых объектов в условиях реальных компьютерных атак;

2) вероятный уровень компетенций злоумышленника, достаточный для успешного взлома системы, а также уровень трудоемкости успешной атаки;

3) формирование и проверка дополнительных меры защиты, которые могут снизить угрозы системе;

4) способность сотрудников службы безопасности и ИТ-персонала вовремя обнаруживать компьютерные атаки и надлежащим образом на них реагировать.

Тестирование на проникновение является многоаспектным интегральным способом проверки защищённости тестируемых объектов и позволяет получить более адекватную оценку защищенности чем, например, способы анализа, но оно более трудоемкое и требует большого опыта аудитора, чтобы минимизировать риск для целевых систем. Важные объекты системы могут быть повреждены или иным образом выведены из строя в ходе тестирования на проникновение, даже если организация извлекает выгоду из понимания того, как система может быть выведена из строя злоумышленником. Хотя опытные аудиторы могут снизить этот риск, полностью исключить его невозможно. Тестирование на проникновение следует проводить только после тщательного обсуждения и планирования.

4.2. Типы тестирования

4.2.1. Внутреннее и внешнее тестирование

По расположению аудитора, имитирующего злоумышленника, относительно периметра безопасности тестируемого объекта тестирование можно декомпозировать на:

1) внешнее тестирование – аудитор находится за пределами периметра безопасности тестируемого объекта и имитирует действия внешнего злоумышленника;

2) внутреннее тестирование – аудитор находится в пределах периметра безопасности тестируемого объекта и имитирует действия внутреннего злоумышленника.

Проведение внешнего тестирования дает возможность исследовать как выглядит состояние среды безопасности из вне с целью выявления уязвимостей, которые могут быть использованы внешним злоумышленником.

При внутреннем тестировании аудиторы работают внутри системы и имитируют действия доверенного инсайдера или внутреннего злоумышленника, уже проникшего через защиту периметра. Такое тестирование позволяет выявить уязвимости, которые могут быть использованы злоумышленником, и демонстрирует потенциальный ущерб, который может быть нанесен системе изнутри. Внутреннее тестирование безопасности также акцентируется на безопасности и конфигурации на уровне системы, включая настройку приложений и служб, аутентификацию, контроль доступа и улучшении защиты системы.

Если необходимо провести как внутреннее, так и внешнее тестирование, то сначала проводится внешнее тестирование, а потом внутреннее.

4.2.2. Открытое и скрытое тестирование

По степени осведомленности должностных лиц, отвечающих за безопасность, и ИТ-персонала организации о проводимом тестировании, тестирование можно декомпозировать на:

1) открытое тестирование – аудитор действует при полной осведомленности должностных лиц, отвечающих за безопасность и ИТ-персонала организации, о проводимом тестировании;

2) скрытое тестирование – аудитор действует в условиях, когда должностные лица, отвечающие за безопасность и ИТ-персонал организации не осведомлены о проводимом тестировании.

Поскольку служба безопасности и ИТ-персонал полностью осведомлен о тестировании и участвует в нем, он может дать рекомендации по работе с системой. В процессе тестирования персонал также может наблюдать за действиями аудитора в обучающих целях.

Целью скрытого тестирования является изучение степени ущерба или воздействия, которое может нанести злоумышленник. Этот тип тестирования не проверяет все меры безопасности, не выявляет каждую уязвимость и не оценивает все объекты в организации. Скрытое тестирование обычно имеет определенные ограничения, такие как прекращение тестирования при достижении определенного уровня доступа или при достижении возможности нанесения определенного типа ущерба на следующем шаге тестирования.

4.2.3. Тестирование на основе принципов «белого», «серого» и «черного ящика»

Условно все варианты проведения тестирования можно соотнести с тремя основными принципами:

1) принцип «белого ящика» – предусматривает предоставление аудитору наиболее полной информации о принципах функционирования тестируемых объектов, их конфигурации, структуре связей, используемых протоколах, исходных кодах приложений и т.д.;

2) принцип «черного ящика» – аудитору не предоставляется никакой информации о тестируемых объектах, всю необходимую информацию он должен собрать и использовать самостоятельно;

3) принцип «серого ящика» – аудитору предоставляется часть общей информации о тестируемых объектах, исходные данные, которые могли бы быть получены аудитором самостоятельно (в интересах снижения длительности этапа сбора данных), отдельные сведения о принципах функционирования тести-

руемых объектов, их конфигурации, структуре сети, используемых протоколах, исходных кодах отдельных модулей приложений и т.д.

4.3. Этапы тестирования на проникновение

Тестирование проводится в несколько этапов, которые позволяют структурированно и комплексно произвести оценку безопасности тестируемых объектов. В стандарте NIST SP 800-115 сформулировано четыре этапа тестирования на проникновение:

1) планирование;
2) сбор информации;
3) проведение компьютерных атак;
4) составление отчета о тестировании.

4.3.1. Этап планирования

На этапе планирования определяются правила тестирования, утверждается и документируется руководство по тестированию и определяются цели тестирования.

На этапе планирования с руководством организации согласовываются цели тестирования, начальные условия, объекты тестирования, проверяемые уязвимости, содержание тестов на проникновение. Также определяются области исследования и подход к проведению тестирования на основе исходных сведений о системе (по принципу «белый ящик», «черный ящик» или «серый ящик»), уровень осведомленности персонала организации о проводимых испытаниях (открытое или скрытое тестирование) и нахождения специалиста, проводящего тесты, относительно сети системы (внешнее или внутреннее тестирование). Определяется перечень специального ПО которое будет использовано для автоматизации процессов тестирования.

4.3.2. Этап сбора информации

Этап сбора информации состоит из двух частей. Первая часть состоит из сбора информации о системе, сети и приложениях. На этом этапе производится сбор следующей информации:

1) идентификация используемых сетевых протоколов, портов и служб, осуществляется путем сканирования сети;

2) сбор информации об именах хостов и IP-адресах с использованием различных способов, в том числе, с помощью запросов DNS, запросов InterNIC (WHOIS), а также анализ сети во время проведения внутренних тестов;

3) сбор информации о сотрудниках организации – их имена и контактные данные, осуществляется с помощью поиска на web-серверах или серверах каталогов организации;

4) сбор системной информации, такой как имена компьютеров и общие ресурсы, осуществляется во время внутренних тестов с помощью перечисления NetBIOS, и с помощью сетевой информационной системы NIS (Network Information System);

5) сбор информации о приложениях, пользовательском ПО и прикладных сервисах, функционирующих в системе.

Вторая часть этапа сбора информации – это анализ стандартных и потенциальных уязвимостей, которые могут присутствовать в найденных в первой части этого этапа сетевых протоколах, ОС и пользовательском ПО. Для этого аудиторы могут использовать как свои собственные БД уязвимостей, так и общедоступные БД для выявления уязвимостей вручную. Ручной анализ может выявить новые или скрытые уязвимости, которые могут пропустить автоматические сканеры, но они намного медленнее, чем автоматические процедуры.

4.3.4. Этап проведения компьютерных атак

Проведение компьютерных атак является основным этапом теста на проникновение. В то время как сканеры уязвимостей проверяют только возможное наличие уязвимости, на этапе проведения компьютерных атак подтверждается факт существования уязвимости. Оценивается опасность уязвимости с точки зрения достижения цели тестирования и потенциального ущерба который может быть нанесен при ее эксплуатации. Если проводимая атака успешна, то выявленная уязвимость проверяется и предпринимаются меры предосторожности, чтобы уменьшить негативное воздействие данного типа атаки на безопасность системы.

В большинстве случаев на этом этапе выполняются небольшие программы – эксплойты, ориентированные на использование стандартных или потенциальных уязвимостей в сетевых протоколах, ОС и пользовательском ПО, выявленном на предыдущем этапе тестирования.

Эксплойты не предоставляют аудитору максимального уровня привилегий в системе. Однако, их использование, приводит к тому, что аудиторы получают больше об исследуемой системе, сети и их потенциальных уязвимостях, или же может вызвать требуемое изменение состояния безопасности целевых объектов. Некоторые эксплойты позволяют аудиторам повышать свои привилегии в системе или в сети, чтобы

получить доступ к дополнительным ресурсам. В этом случае требуются дополнительный анализ и тестирование для определения истинного уровня ущерба, который потенциально может быть нанесен аудитором с имеющимся уровнем привилегий, например, определение тех данных, которые можно собрать, изменить или удалить из системы.

Если атака на конкретную уязвимость оказывается невозможной, аудитор переходит к следующей уязвимости. Рекомендуется вести перебор уязвимостей от наиболее распространённых или ведущих к максимальному уровню ущерба, к менее распространенным и менее разрушительным.

Если в результате атаки аудитор выявил активную уязвимость, которую можно эксплуатировать, он может реализовать дополнительные способы компьютерных атак, эффективных именно с этой уязвимостью, а также установить дополнительные инструменты в целевой системе или сети, чтобы облегчить процесс эксплуатации уязвимости. Эти дополнительные инструменты используются для получения доступа к другим объектам системы или ресурсам в сети, а также расширяют возможности получения доступа к информации о сети или организации.

Во время тестирования на проникновение следует проводить атаку и анализ всех доступных объектов в системе. После выявления конкретных активных уязвимостей следует эксплуатировать либо наиболее опасные уязвимости, позволяющие получить максимальный уровень привилегий в системе, либо те, которые позволят осуществить доступ к наиболее важным объектам.

4.3.5. Этап составления отчета

Отчет, как правило, формируется параллельно с тремя другими этапами теста на проникновение.

На этапе планирования разрабатывается план оценки и показатель рентабельности тестирования [19]. На этапах сбора информации и проведения компьютерных атак обычно ведутся журналы успешных атак, проверенных и выявленных уязвимостей, периодически отправляются отчеты системным администраторам и/или руководству. По завершении тестирования формируется отчет о тестировании, в котором приводится описание проведенных тестов, выявленных уязвимостей, оценивается потенциальный ущерб, вследствие их эксплуатации реальным злоумышленником.

Результаты тестирования безопасности должны быть задокументированы и предоставлены соответствующим должностным лицам, в число которых могут входить ИТ-директор, глава отдела безопасности, глава отдела информационной безопасности, сотрудники отдела безопасности и ИТ-отдела, а также соответствующие менеджеры продукта или владельцы системы.

4.4. Типовые уязвимости, выявляемые при тестировании на проникновение

В соответствии с NIST SP 800-115 уязвимости, выявляемые при тестировании на проникновение, подразделяются на следующие основные категории:

1) Неверные конфигурации.

2) Уязвимости ядра ОС.

3) Переполнение буфера.

4) Недостаточная проверка корректности ввода данных.

5) Использование ложных символических ссылок.

6) Некорректные файловые дескрипторы.

7) Использование состояний «гонки» (конкуренции) между программами или процессами ОС.

8) Неправильные права доступа для файлов или каталогов.

Для формирования конкретных, более полных, перечней уязвимостей, проверяемых в процессе тестирования, в стандарте NIST SP 800-115 рекомендуется использовать следующие web-ресурсы:

1) Common Configuration Enumeration (CCE): https://nvd.nist.gov/config/cce/index;

2) Common Vulnerabilities and Exposures (CVE): http://cve.mitre.org;

3) Common Weakness Enumeration (CWE): http://cwe.mitre.org;

4) Default Password List: http://www.phenoelit-us.org/dpl/dpl.html;

5) National Vulnerability Database (NVD): http://nvd.nist.gov;

6) Open Source Vulnerability Database: http://www.osvdb.org;

7) Open Web Application Security Project (OWASP) Vulnerabilities: http://www.owasp.org/index.php/Category:Vulnerability;

8) Security Focus Vulnerabilities: http://www.securityfocus.com/vulnerabilities;

9) SecurityTracker: http://www.securitytracker.com;

10) The Hacker's Choice (THC): http://freeworld.thc.org;

11) United States Computer Emergency Readiness Team (US-CERT) Vulnerability Notes Database: http://www.kb.cert.org/vuls;

12) Wireless Vulnerabilities and Exploits (WVE): http://www.wirelessve.org.

5. Инструментарий оценки ИБ

Стандарт NIST SP 800-115 для проведения тестирования на проникновение рекомендует использование следующих программных комплексов:

1) BackTrack: https://www.backtrack-linux.org;

2) Knoppix Security Tools Distribution (STD): https://s-t-d.org/download.html;

3) F.I.R.E.: https://www.dmzs.com/tools;

4) INSERT Rescue Security Toolkit: http://www.inside-security.de/insert_en.html;

5) PHLAK: http://sourceforge.net/projects/phlakproject;

6) Top 100 Network Security Tools: http://sectools.org.

При этом в NIST SP 800-115 отдельно выделяются программные средства, которые могут быть использованы для реализации способов тестирования из комплекса BackTrack и Knoppix STD (таблица 1 и 2). При этом комплекс BackTrack рекомендуется как наиболее полный и содержащий разнообразные средства тестирования.

Заключение

Анализ стандарта NIST SP 800-115 показал, что по своей ширине и глубине охвата вопросов проведения тестирования его целесообразно использовать при разработке отечественного стандарта тестирования на проникновения.

Преимуществами стандарта NIST SP 800-115 является то, что стандарт включает в сферу оценки ИБ не только вопросы проведения тестирования, но и вопросы анализа документации организации, политик обеспечения безопасности, а также вопросы использования способов социальной инженерии и их влияние на итоговый уровень безопасности организации. Именно эти преимущества целесообразно заимствовать из NIST SP 800-115 при разработке отечественного проекта стандарта тестирования на проникновение.

Слабыми сторонами стандарта NIST SP 800-115 являются следующие. Во-первых, NIST SP 800-115 не содержит исчерпывающего перечня уязвимостей, рекомендуемых к проверке. В этой части NIST SP 800-115, ссылается на другие базы уязвимостей, которые целесообразно использовать в отечественном стандарте, а также дополнить отечественный стандарт уязвимостями из ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем». Во-вторых, в NIST SP 800-115 не приводятся конкретные реализации и сценарии компьютерных атак, предназначенных для проверки конкретных уязвимостей. В этой части NIST SP 800-115 существенно проигрывает таким методикам как PTES и OWASP, содержащих конкретный перечень широко распространенных уязвимостей и рекомендации по способам их проверки.

Таблица 1

Пример программных средств из состава комплекса BackTrack, которые могут использоваться для тестирования

Анализ сети	Autonomous System Scanner, Ettercap, Firewalk, Netdiscover, Netenum, Netmask, Nmap, P0f, Tctrace, Umit
«Снифферы» и программы захвата трафика	Dsniff, Ettercap, Kismet, Mailsnarf, Msgsnarf, Ntop, Phoss, SinFP, SMB Sniffer, Wireshark
Идентификация портов и сетевых сервисов	Amap, AutoScan, Netdiscover, Nmap, P0f, Umit, UnicornScan
Сканирование уязвимостей	Firewalk, GFI LANguard, Hydra, Metasploit, Nmap, Paros Proxy, Snort, SuperScan
Сканирование беспроводных сетей	Airsnarf, Airsnort, BdAddr, Bluesnarfer, Btscanner, FakeAP, GFI LANguard, Kismet, WifiTAP
Проверка целостности файлов	Autopsy, Foremost, RootkitHunter, Sleuthkit
Взлом паролей	Hydra, John the Ripper, RainbowCrack, Rcrack, SIPcrack, SIPdump, TFTP-Brute, THC PPTP, VNCrack, WebCrack
Тестирование удаленного доступа	IKEProbe, IKE-Scan, PSK-Crack, VNC_bypauth
Тестирование на проникновение	Driftnet, Dsniff, Ettercap, Kismet, Metasploit, Nmap, Ntop, SinFP, SMB Sniffer, Wireshark
Тестирование безопасности приложений	CIRT Fuzzer, Fuzzer 1.2, NetSed, Paros Proxy, Peach

Таблица 2

Пример программных средств из состава комплекса Knoppix STD Toolkit, которые могут использоваться для тестирования

Анализ сети	Cryptcat, Ettercap, Firewalk, Netcat, Nmap, P0f
«Снифферы» и программы захвата трафика	Dsniff, Ettercap, Ethereal, Filesnarf, Kismet, Mailsnarf, Msgsnarf, Ngrep, Ntop, TCPdump, Webspy
Идентификация портов и сетевых сервисов	Amap, Netcat, Nmap, P0f
Сканирование уязвимостей	Exodus, Firewalk, Nmap, Snort
Сканирование беспроводных сетей	Airsnarf, Airsnort, GPSdrive, Kismet, MACchanger
Проверка целостности файлов	Autopsy, Biew, Bsed, Coreography, Foremost, Hashdig, Rifiuti, Sleuthkit
Взлом паролей	Allwords2, chntpw, Cisilia, Djohn, Hydra, John the Ripper, Rcrack
Тестирование удаленного доступа	Apache Server, IKE-Scan, Net-SNMP, SSHD, TFTPD, VNC Server
Тестирование на проникновение	Driftnet, Dsniff, Ethereal, Ettercap, Kismet, Nessus, Netcat, Ngrep, Nmap, Ntop, TCPdump
Тестирование безопасности приложений	NetSed

В-третьих, в NIST SP 800-115 не рассматриваются вопросы физического доступа к информационной инфраструктуре организации и способы проверки ее безопасности. В-четвертых, NIST SP 800-115 содержит довольно устаревший набор инструментария тестирования, который, на взгляд автора, проигрывает в полноте и эффективности программным средствам в составе последних дистрибутивов Kali Linux. Эти недостатки показывают, что при разработке соответствующих вопросов отечественного стандарта на проникновение целесообразно использовать другие методики и стандарты, отличные от NIST SP 800-115.

В дальнейших работах автор планирует продолжить работу по анализу известных зарубежных стандартов и методик тестирования в интересах в интересах оценки целесообразности их использования для разработки аналогичного отечественного проекта стандарта тестирования на проникновение.

Отдельные, частные результаты этой работы получены в рамках исследований по бюджетной теме FFZF-2022-0004.

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. 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
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. Барабанов А. В., Марков А. С., Цирлов В. Л., Раутkин Ю.В. Исследование уязвимостей программного обеспечения. – М.: Научный центр правовой информации при Министерстве юстиции Российской Федерации, 2018. – 76 с.
6. Барабанов А. В., Марков А. С., Цирлов В. Л. Тестирование межсетевых экранов по требованиям безопасности информации. – М.: МГТУ им. Н.Э. Баумана, 2021. – 53 с.
7. Дорофеев А. Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? // Защита информации. Инсайд. 2010. № 6 (36). С. 72-73.

8. Dorofeev A. V., Markov A. S., Rautkin Y. V. Ethical hacking training // ISTMC 2019 - Selected Papers of the 4th All-Russian Scientific and Practical Conference with International Participation «Information Systems and Technologies in Modeling and Control». – CEUR Workshop Proceedings, 2019. – С. 47-56.
9. Климов С. М. Имитационные модели испытаний критически важных информационных объектов в условиях компьютерных атак // Известия ЮФУ. Технические науки. 2016. № 8 (181). С. 27-36.
10. 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.
11. 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.
12. 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.
13. Бойко А. А. Боевая эффективность кибератак: аналитическое моделирование современного боя // Системы управления, связи и безопасности. 2020. № 4. С. 101-133. DOI: 10.24411/2410-9916-2020-10404
14. Бойко А. А. Боевая эффективность кибератак: практические аспекты // Системы управления, связи и безопасности. 2020. № 4. С. 134-162. DOI: 10.24411/2410-9916-2020-10405
15. Бегаев А. Н., Бегаев С. Н., Федотов В. А. Тестирование на проникновение. – СПб: Университет ИТМО, 2018. – 45 с.
16. Скабцов Н. Аудит безопасности информационных систем. – СПб.: Питер, 2018. – 272 с.
17. Бирюков А. А. Собираем устройства для тестов на проникновение. – М.: ДМК Пресс, 2018. – 378 с.
18. NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment (NIST SP 800-115). – Computer Security Resource Center, 2008. – 80 p.– URL: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf (дата доступа 20.05.2022).
19. Макаренко С. И. Критерии и показатели оценки качества тестирования на проникновение // Вопросы кибербезопасности. 2021. № 3 (43). С. 43-57. DOI: 10.21681/2311-3456-2021-3-43-57
20. Макаренко С. И., Смирнов Г. Е. Методика обоснования тестовых информационно-технических воздействий, обеспечивающих рациональную полноту аудита защищенности объекта критической информационной инфраструктуры // Вопросы кибербезопасности. 2021. № 6 (46). С. 12-25. DOI: 10.21681/2311-3456-2021-6-12-25

PENETRATION TESTING IN ACCORDANCE WITH NIST SP 800-115 STANDARD

Makarenko S.I. [2]

Relevance. *Security issues of information systems in critical infrastructure objects become important now. However, current tasks of information security audit of critical infrastructure objects are mainly limited to checking them for compliance with requirements of standards and documents. With this approach to the audit, security of these objects from real attacks by hackers remains unclear. Therefore, objects are subjected to a testing procedure, namely, penetration testing, in order to objectively verify their security. For example, there are instructions of the Bank of Russia to carry out such testing when the information security of banking systems are checked. However, there is no formal national standard for conducting penetration testing in Russia. This is the deterrent factor to testing critical infrastructure objects.*

The goal of the paper *is to analysis of the American testing standard – NIST SP 800-115 to estimate the possibility of its used for development of the Russian national penetration testing standard.*

Research methods. *Methods of analysis and decomposition from the theory of system analysis are used in the paper to achieve the research goal.*

Results. *In-depth analysis of the NIST SP 800-115 standard is provided in the paper. The following are considered: types of information security assessment measures; stages of information security assessment; methods of analysis and testing which used in the assessment of information security; types and sequence of penetration*

2 Sergey I. Makarenko, Dr.Sc. (in Tech.), Associate Professor, Leading Researcher of the St. Petersburg Federal Research Center of the Russian Academy of Sciences, St. Petersburg, Russia. E-mail: mak-serg@yandex.ru. ORCID: 0000-0001-9385-2074

testing; tested vulnerabilities; recommended tools for analysis and testing, are presented in NIST SP 800-11. Conclusions about the strengths and weaknesses of the NIST SP 800-115 standard are made. Recommendations about as NIST SP 800-115 is used in the development of the national Russian standard of penetration testing are presented.

Keywords: *penetration testing, computer attack, NIST SP 800-115, testing, security testing, social engineering, software testing, vulnerability, network scanning.*

References

1. Makarenko S. I. Audit informacionnoj bezopasnosti: osnovnye jetapy, konceptual'nye osnovy, klassifikacija meroprijatij // Sistemy upravlenija, svjazi i bezopasnosti. 2018. № 1. S. 1-29. DOI: 10.24411/2410-9916-2018-10101
2. Makarenko S. I. Audit bezopasnosti kriticheskoj infrastruktury special'nymi informacionnymi vozdejstvijami. Monografija. – SPb.: Naukoemkie tehnologii, 2018. – 122 s.
3. Makarenko S. I., Smirnov G. E. Analiz standartov i metodik testirovanija na proniknovenie // Sistemy upravlenija, svjazi i bezopasnosti. 2020. № 4. S. 44-72. DOI: 10.24411/2410-9916-2020-10402
4. Markov A. S., Cirlov V. L., Barabanov A. V. Metody ocenki nesootvetstvija sredstv zashhity informacii / pod red. A.S. Markova. – M.: Radio i svjaz', 2012. – 192 s.
5. Barabanov A. V., Markov A. S., Cirlov V. L., Rautkin Ju.V. Issledovanie ujazvimostej programmnogo obespechenija. – M.: Nauchnyj centr pravovoj informacii pri Ministerstve justicii Rossijskoj Federacii, 2018. – 76 s.
6. Barabanov A. V., Markov A. S., Cirlov V. L. Testirovanie mezhsetevyh jekranov po trebovanijam bezopasnosti informacii. – M.: MGTU im. N.Je. Baumana, 2021. – 53 s.
7. Dorofeev A. Testirovanie na proniknovenie: demonstracija odnoj ujazvimosti ili ob#ektivnaja ocenka zashhishhennosti? // Zashhita informacii. Insajd. 2010. № 6 (36). S. 72-73.
8. Dorofeev A. V., Markov A. S., Rautkin Y. V. Ethical hacking training // ISTMC 2019 - Selected Papers of the 4th All-Russian Scientific and Practical Conference with International Participation "Information Systems and Technologies in Modeling and Control". – CEUR Workshop Proceedings, 2019. – S. 47-56.
9. Klimov S. M. Imitacionnye modeli ispytanij kriticheski vazhnyh informacionnyh ob#ektov v uslovijah komp'juternyh atak // Izvestija JuFU. Tehnicheskie nauki. 2016. № 8 (181). S. 27-36.
10. Klimov S. M., Sychjov M. P. Stendovyj poligon uchebno-trenirovochnyh i ispytatel'nyh sredstv v oblasti obespechenija informacionnoj bezopasnosti // Informacionnoe protivodejstvie ugrozam terrorizma. 2015. № 24. S. 206-213.
11. Bojko A. A., D'jakova A. V. Sposob razrabotki testovyh udalennyh informacionno-tehnicheskih vozdejstvij na prostranstvenno raspredelennye sistemy informacionno-tehnicheskih sredstv // Informacionno-upravljajushhie sistemy. 2014. № 3 (70). S. 84-92.
12. Bojko A. A., Obushhenko E. Ju., Shheglov A. V. Osobennosti sinteza polnogo mnozhestva testovyh sposobov udalennogo informacionno-tehnicheskogo vozdejstvija na prostranstvenno raspredelennye sistemy informacionno-tehnicheskih sredstv // Vestnik Voronezhskogo gosudarstvennogo universiteta. Serija: Sistemnyj analiz i informacionnye tehnologii. 2017. № 2. S. 33-45.
13. Bojko A. A. Boevaja jeffektivnost' kiberatak: analiticheskoe modelirovanie sovremennogo boja // Sistemy upravlenija, svjazi i bezopasnosti. 2020. № 4. S. 101-133. DOI: 10.24411/2410-9916-2020-10404
14. Bojko A. A. Boevaja jeffektivnost' kiberatak: prakticheskie aspekty // Sistemy upravlenija, svjazi i bezopasnosti. 2020. № 4. S. 134-162. DOI: 10.24411/2410-9916-2020-10405
15. Begaev A. N., Begaev S. N., Fedotov V. A. Testirovanie na proniknovenie. – SPb: Universitet ITMO, 2018. – 45 s.
16. Skabcov N. Audit bezopasnosti informacionnyh sistem. – SPb.: Piter, 2018. – 272 s.
17. Birjukov A. A. Sobiraem ustrojstva dlja testov na proniknovenie. – M.: DMK Press, 2018. – 378 s.
18. NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment (NIST SP 800-115). – Computer Security Resource Center, 2008. – 80 p.– URL: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf (data dostupa 20.05.2022).
19. Makarenko S. I. Kriterii i pokazateli ocenki kachestva testirovanija na proniknovenie // Voprosy kiberbezopasnosti. 2021. № 3 (43). S. 43-57. DOI: 10.21681/2311-3456-2021-3-43-57
20. Makarenko S. I., Smirnov G. E. Metodika obosnovanija testovyh informacionno-tehnicheskih vozdejstvij, obespechivajushhih racional'nuju polnotu audita zashhishhennosti ob#ekta kriticheskoj informacionnoj infrastruktury // Voprosy kiberbezopasnosti. 2021. № 6 (46). S. 12-25. DOI: 10.21681/2311-3456-2021-6-12-25