КРИТЕРИИ И ПОКАЗАТЕЛИ ОЦЕНКИ КАЧЕСТВА ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

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. Анализ отечественных и зарубежных публикаций в этой области показывает, что в настоящее время отсутствует какой-либо формальный подход к выбору тестов, а также показателей и критериев оценки эффективности тестирования на проникновение.*

Целями работы *является формирование частных показателей полноты, оперативности, достоверности и стоимости тестирования, а также, в обобщенном виде, группы критериев «эффективности/стоимость», позволяющих провести оценку качества тестовых наборов, а также сравнивать различные сценарии тестирования на проникновение между собой.*

Методы исследования. *Для достижения цели исследования в работе использованы методы теории вероятностей и математической статистики, методы обработки экспериментальных данных, а также результаты других исследований в области тестирования безопасности программного обеспечения.*

Результаты. *В статье представлены: общий вид критериев «эффективности/стоимость» для оценки качества тестирования на проникновение, а также формальные частные показатели для оценки отдельных параметров в предложенных критериях – параметры полноты, оперативности, достоверности и стоимости. Полученные результаты могут быть использованы аудиторами ИБ и тестировщиками для объективного обоснования тестовых наборов и сравнения различных сценариев тестирования на проникновение между собой. Материал статьи может быть полезен специалистам, чей областью исследований является такой вид практического аудита безопасности информационных систем, как тестирование на проникновение.*

Ключевые слова: *тестирование на проникновение, информационно-техническое воздействие, критерий качества тестирования, качество тестирования, полнота тестирования, оперативность тестирования, достоверность тестирования, стоимость тестирования.*

DOI:10.21681/2311-3456-2021-3-43-57

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) 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 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 [3-8], 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 является реализации в отношении объектов КИИ тестов на проникновение – воздействие на объект тестовых информационно-технических воздействий (ИТВ), ана-

1 Макаренко Сергей Иванович, доктор технических наук, доцент, ведущий научный сотрудник Санкт-Петербургского Федерального исследовательского центра РАН. Область научных интересов: сети и системы связи; радиоэлектронная борьба; информационная безопасность; информационное противоборство. Санкт-Петербург, Россия. E-mail: mak-serg@yandex.ru. ORCID: 0000-0001-9385-2074

логичных реальным ИТВ, 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, для такого тестирования, а также критериев оценки его результатов.

Целями статьи является: формирование показателей полноты, оперативности, достоверности и затратности тестирования, а также, в обобщенном виде, группы критериев «эффективности/стоимость», позволяющих провести оценку качества наборов ИТВ для тестирования на проникновение, а также сравнивать различные такие тестовые наборы между собой; формирование группы дополнительных показателей, которые характеризуют отдельные аспекты качества процесса тестирования.

Статья продолжает исследования автора [1, 2, 9], направленные на развитие теоритического базиса тестирования на проникновение. Положения, представленные в данной статье, на взгляд автора, не являются окончательными, а носят, в большей степени, дискуссионный характер. Автор не претендует на окончательную верность своих суждений, однако надеется, что его работа станет своеобразной «отправной точкой» для специалистов в области ИБ при формировании научно-обоснованных подходов для такого перспективного способа практического аудита ИБ, как тестирование на проникновение.

1. Обоснование тестирования на проникновение как перспективного практического подхода к проведению аудита информационной безопасности

В настоящее время в теории аудита ИБ сложилась ситуация, при которой большинство работ в этой области ориентировано на исследование экспертного аудита и оценки соответствия преимущественно на основе моделей анализа рисков, либо на основе анализа стандартов ИБ. Вместе с тем, требования стандартов ИБ, как правило, формулируется по итогам анализа инцидентов, что приводит к тому, что они регулярно отстают от современных возможностей и практики действий злоумышленников. При этом, тестирование и, в особенности, тестирование на проникновение, является недостаточно изученной областью исследований.

Вместе с тем прослеживается тенденция к наращиванию доли тестов, которые проводятся в форме экспериментальных исследований реального объекта или его прототипа. Особенно это характерно при тестировании программного обеспечения [3]. Как правило, для этого используются виртуальные машины, на которых осуществляется контролируемое выполнение тестируемого программного обеспечения [3]. Дальнейшее развитие данного подхода к тестированию привело к разработке так называемых киберполигонов, которые виртуализируют как аппаратное, так и программное обеспечение распределенной информационной системы и позволяют отработать защиту от различных известных ИТВ. Сейчас это направление активно развивается, и ему посвящены работы [10-12].

В настоящее время к наиболее распространенному комплексному тесту защищенности реальной информационной системы относится «тест на проникновение». Исследованию тестирования на проникновение посвящены работы [4-8, 13, 14, 15-25]. Однако в подавляющем числе данных работ не содержатся какие-либо научно-обоснованные методики проведения тестирования (подобные тем, которые задаются для испытаний при оценке соответствия [3]). Более того, исследователи этого типа тестирования отмечают, что выбор конкретных способов и средств тестирования остается за экспертом-тестировщиком, и в первую очередь должен быть направлен на выявление тех уязвимостей, на которые обращает внимание заказчик и исправление которых в максимальной степени выгодны эксперту (особенно, если по итогам тестирования ожидается принятие решения о заказе определенной системы защиты). Таким образом, этому виду тестирования характерна еще и субъективность как в отношении ожидаемых результатов со стороны заказчика, так и в отношении заинтересованности эксперта в демонстрации наиболее «зрелищных» инцидентов с целью склонения заказчика к организации определенной конфигурации защиты.

Как показано в работах [1, 2], тестирование на проникновение является более гибким инструментом аудита чем, например, мероприятия оценки соответствия, так как его проведение не ограниченно рамками действующих стандартов и регламентов. Это позволяет выбирать более широкий диапазон средств и способов ИТВ, а также быть более избирательным в направлении достижения цели аудита. Например, проводить исследование объектов КИИ к угрозам и выявлять уязвимости, еще не описанные в базах угроз и уязвимостей. При этом, при проведении тестирования на проникновение целесообразно придерживаться системного подхода как к выбору тестовых ИТВ, так и к проведению тестирования.

Введем базовую терминологию, которую будем использовать в дальнейшем.

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

Тестирование – проверка выполнения требований к объекту при помощи наблюдения за ее работой в конечном наборе специально выбранных ситуаций [26].

Тест – отдельное мероприятие по исследованию объекта или способ изучения процессов его функционирования [26].

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 формирования, передачи, обработки, хранения и воспроизведения информации, с целью выявить уязвимости объекта на которое производится воздействие [26].

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 информационно-психологических воздействий (ИПВ) [2].

Тестовый набор – конечное множество специально выбранных ситуаций (тестов), на основе которого выполняется проверка выполнения требований к системе.

Стоимость тестирования – совокупные затраты всех видов ресурсов на проведение тестирования.

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.

Общая классификация мероприятий, способов и средств ИТВ, которые могут быть использованы при тестировании на проникновение, представлена на рис. 1.

В рамках тестирования на проникновение должны реализовываться сценарии поэтапного интегрального применения средств и способов ИТВ, для всеобъемлющего анализа уязвимостей тестируемых объектов в технической сфере, а также для формирования предложений по модернизации средств защиты. При этом, различные типы ИТВ целесообразно объединить в единый комплекс тестирования защищенности объектов. Целью такого комплекса будет являться непрерывное наращивание возможностей тестирования с целью повышения адекватности и качества тестирования объектов, за счет применения обеспечивающих и атакующих средств ИТВ имитирующих передовые возможности как непрофессиональных злоумышленников, так и профессиональных нарушителей (сил информационных операций).

2. Анализ актуальных работ в области тестирования на проникновение

Практическим вопросам оценки состояния ИБ объектов путем их тестирования посвящены работы Маркова А. С., Цирлова В. Л., Барабанова А. В. [3], Климова С. М. [10, 11], Петренко А. А., Петренко С. А. [12], Бойко А. А. [27-29], Храмова В. Ю. [28-30], Щеглова А. В. [29, 30], Дьяковой А. В. [27, 28], Макаренко С.И. [2], Скабцова Н. [4], Moeller R. R. [31], Kennedy D., O'Gorman J., Kearns D., Aharoni M. [6], Makan K. [7], Cardwell K. [8].

В работах McDermott J. P. [32], Klevinsky T. J., Laliberte S., Gupta A. [33], Pfleeger C.P., Pfleeger S.L., Theofanos M.F. [34], Alisherov F., Sattarova F. [35], Ami P., Hasan A. [36], Holik F., Horalek J., Marik O., Neradova S., Zitta S. [37], Herzog P. [38], Engebretson P. [39], Барановой Е.К. [13, 40], Бегаева А.Н., Бегаева С.Н., Федотова В.А. [41], Богораза А. Г., Песковой О. Ю. [42], Дорофеева А. [14], Умницына М. Ю. [15], Бородина М. К., Бородиной П. Ю. [16], Baloch R. [18], Полтавцевой М. А., Печенкина А. И. [19], Кадана А. М., Доронина А. К. [20], Еременко Н. Н., Кокоулина А. Н. [21], Туманова С. А. [22], Кравчука А. В. [23], Горбатова В. С., Мещерякова А. А. [24], Косенко М. Ю. [25], 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 в области тестирования на проникновение показал следующее.

В настоящее время имеется значительное количество работ, посвященных аудиту ИБ. Однако в подавляющем большинстве этих работ аудит рассматривается как процесс проверки информационных систем на соответствие заранее определенным требованиям ИБ. Вместе с тем требования по ИБ, как правило, формулируется по итогам анализа инцидентов, что приводит к тому, что они регулярно отстают от современных возможностей и практики действий нарушителей. Более того, существующая практика проведения аудита зачастую не предусматривает использование для проверки защищенности информационных систем известных способов, средств и сценариев действий реальных нарушителей. В связи с этим, существующий уровень развития теории и практики аудита защищённости объектов не предполагает проведение полномасштабных экспериментальных исследований анализируемой системы путем применения тестовых информационных воздействий, аналогичных тем, которые применяют реальные нарушители!

Незначительное количество работ, посвященных 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 каким-либо системным или хотя бы общетеоретическим подходом. В некоторых отечественных работах по тестированию на проникновение акцент делается на необходимости выявления наиболее «зрелищных» уязвимостей или тех уязвимостей устранение которых принесет максимальные экономические выгоды компании, выполняющий аудит. Имеющиеся зарубежные и отечественные методики тестирования на проникновение не содержат исчерпывающего научного обоснования параметров и критериев выбора ИТВ для проведения тестирования.

DOI: 10.21681/2311-3456-2021-3-43-57

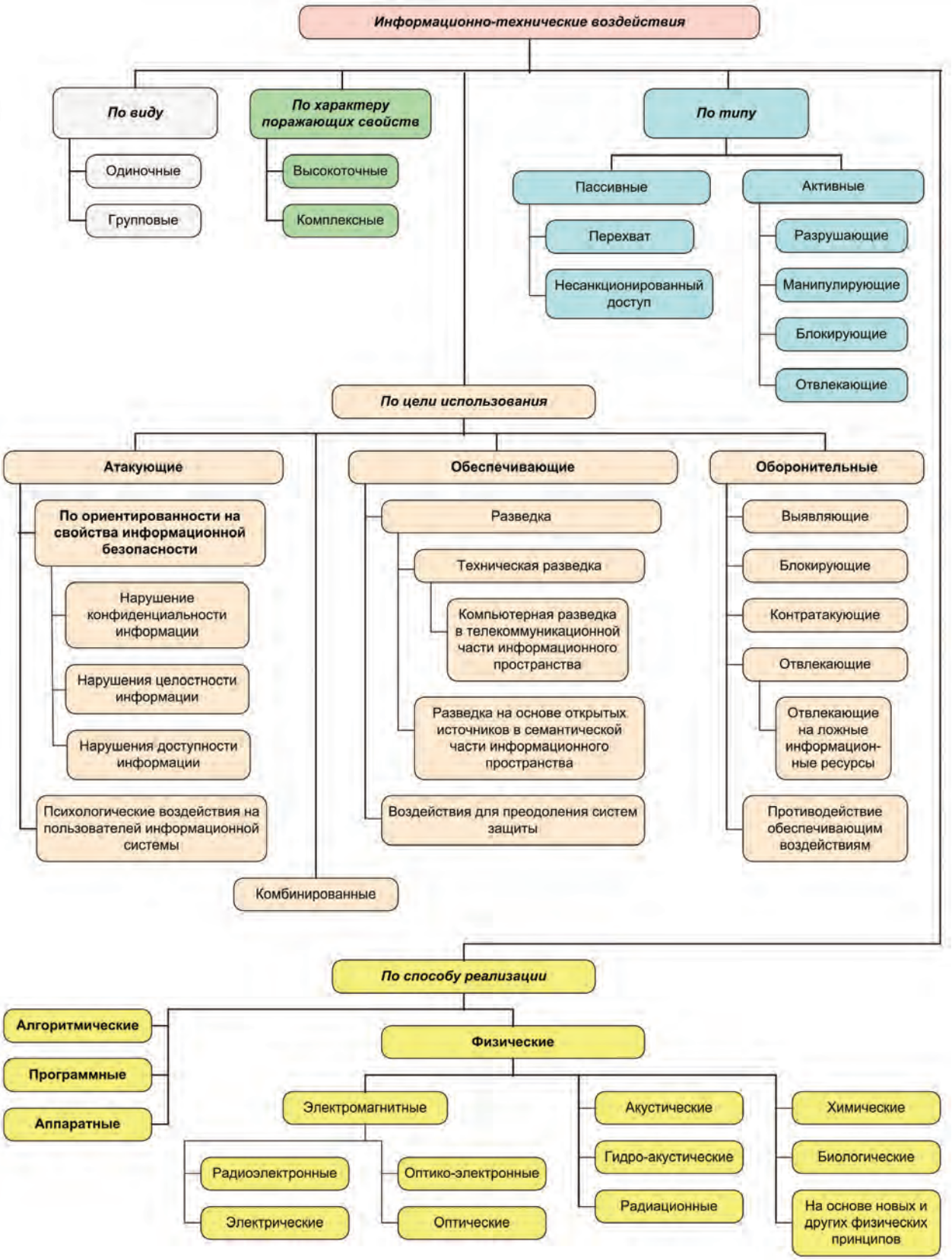

Рис. 1. Классификация ИТВ, которые могут быть использованы при тестировании на проникновение [2]

Обобщая, можно сделать вывод, что в настоящее время научно-обоснованные теоритические основы применения тестирования на проникновения для оценки уровня ИБ тестируемых объектов проработаны чрезвычайно слабо. В частности, не проработанными являются:

- научные основы применения тестирования на проникновение с использованием ИТВ, как одного из основных способов практического аудита состояния защищенности объектов;
- методов и методик формирования тестовых наборов ИТВ, обладающих целесообразной полнотой и адекватностью проверки уровня защищенности тестируемых объектов, а также достоверно воспроизводящим прогнозируемые целевые атаки на них;
- методов и методик проведения тестирования в режимах «белого», «серого» и «черного ящиков», а также в режимах имитации внутреннего и внешнего нарушителя;
- методов и методик согласующих критерии и показатели аудита, проводимого на основе известных методов теоритического подхода (процессный подход, оценка на основе модели зрелости или модели оценки) и практического подхода (анализ рисков, анализ стандартов, комбинированный анализ), а также критерии и показатели тестирования на проникновения;
- методов и методик комплексирующих способы тестирования в технической сфере, путем использования тестовых ИТВ, и в психологической сфере, путем использования ИПВ и социоинженерных атак.

При этом к работам в которых сделана попытка подвести научную основу под тестирование на проникновение относятся работы: Pfleeger C.P., Pfleeger S.L., Theofanos M.F. [34], McDermott J.P. [32], Макаренко С.И. [2], Pfleeger C.P., Pfleeger S.L., Alisherov F., Sattarova F. [35], Ami P., Hasan A. [36], Holik F., Horalek J., Marik O., Neradova S., Zitta S. [37], Herzog P. [38]. Так, в статье McDermott J. P. [32] представлена модель тестирования в формализме теории сетей Петри. В работе Макаренко С.И. [2] сделана попытка систематизировать и подвести научную базу под возможности использования тестовых ИТВ для оценки защищенности объектов КИИ. В статьях Pfleeger C.P., Pfleeger S.L., Theofanos M.F. [34], Alisherov F., Sattarova F. [35], Ami P., Hasan A. [36], Holik F., Horalek J., Marik O., Neradova S., Zitta S. [37], Herzog P. [38] представлены различные варианты методик тестирования. Однако во всех этих работах вопросы обоснования тестовых ИТВ при оценки защищенности тестируемого объекта на основе обобщённого критерия «эффективность / стоимость» – не рассматривались.

3. Группа обобщённых критериев «эффективность / стоимость» для оценки качества тестирования на проникновение

Технология построения тестов на проникновение, прежде всего, должна обеспечивать решение следующих задач:

- тесты на основе ИТВ должны позволять оценить реальное состояние ИБ тестируемого объекта;
- различные ИТВ, используемые в тестах, должны соответствовать типовым ИТВ, применяемым злоумышленниками, т.е. обеспечивать определенную репрезентативность по отношению как ко всем возможным используемым ИТВ, так и к вариантам реакции объекта на них;
- различные ИТВ, используемые в тестах, должны обеспечивать проверку типовых уязвимостей объектов, т.е. обеспечивать определенную репрезентативность по отношению к всем возможным уязвимостям тестируемых объектов по общепринятым свойствам ИБ: конфиденциальности, доступности, целостности.

В связи с вышеуказанным, правила формирования наборов ИТВ для проведения тестирования на проникновения должны быть научно-обоснованными и выбираться исходя из:

- обеспечения высокого уровня эффективности проведения тестирования;
- стоимости ресурсов, необходимых для проведения тестирования временных, финансовых, людских, технические и других видов ресурсов.

В самом общем случае критерий «эффективность / стоимость» для выбора ИТВ при проведении тестирования на проникновение можно выразить следующим правилом:

$$K \geq K_{\text{треб}}, K = \frac{E}{Z}, \quad (1)$$

где: K – показатель качества теста; $K_{\text{треб}}$ – требуемое критериальное значение показателя качества, при котором тест целесообразно применять для анализа объекта; E – показатель эффективности теста; Z – показатель всех видов затрат на разработку теста, проведение тестирования и анализ результатов.

Наиболее важными параметрами в выражении (1) являются параметры E и Z. При этом их размерность и физический смысл, в зависимости о ситуации может быть различен. Рассмотрим эти параметры и их возможную физическую сущность более подробно.

3.1. Понятие эффективности тестирования

В теории систем понятию «эффективность» дается следующее определение.

Эффективность – это комплексное операционное свойство целенаправленного процесса, характеризующее его приспособленность к достижению цели операции или к выполнению задачи системы [26].

При этом, как правило, цель тестирования – практическая оценка состояния ИБ тестируемого объекта, а вот задача(-чи) тестирования, для достижения этой цели, могут быть разными и определяются заказчиком. К наиболее распространенным задачам тестирования можно отнести:

- проверка возможности формирования заранее заданного типа инцидента;
- выявление инцидентов, которые могут быть реализованы при текущей конфигурации средств защиты;
- выявление уязвимостей, ведущих к инциденту определённого типа;
- выявление уязвимостей, ведущих к инциденту, связанному с нарушением определенного свойства ИБ

DOI: 10.21681/2311-3456-2021-3-43-57

(конфиденциальность, целостность, доступность);
- оценка трудоемкости и вероятности преодоления средств защиты объекта при реализации определённого типа ИТВ;
- оценка ущерба, который может причинён объекту, при воздействии ИТВ определенного типа.

Традиционно, в теории тестирования, в качестве показателя эффективности *E* может рассматриваться один или совокупность нескольких основных показателей.

Полнота – достаточность тестового набора для достижения задачи тестирования.

Оперативность – время за которое будет достигнута задача тестирования.

Достоверность – статистически обоснованный уровень точности и репрезентативности результатов тестирования.

Таким образом, комбинации различных частных показателей эффективности образует множество различных критериев, которые могут быть использованы при оценке эффективности проведения тестирования на проникновение:
- критерий «полнота тестирования / стоимость тестирования» при заданном ровне оперативности тестирования и достоверности результатов;
- критерий «оперативность тестирования / стоимость тестирования» при заданном уровне полноты тестирования и достоверности результатов;
- интегральный критерий «полнота и оперативность тестирования / стоимость тестирования» при заданном уровне достоверности результатов.

Рассмотрим более подробно, параметры полноты, оперативности и достоверности которые могут использоваться в этих критериях эффективности.

3.1.1. Показатели полноты тестирования

В качестве параметра полноты тестирования могут быть использованы различные показатели. К основным из них относятся показатели, приведенные ниже. При этом данный список не является исчерпывающим, и другие исследователи в зависимости от контекста и задач тестирования могут обосновывать и применять свои показатели.

1) Полнота тестирования требований по ИБ к объекту:

$$\pi = \frac{N_{\text{тр тест}}}{N_{\text{тр}}}, \qquad (2)$$

где: $N_{\text{тр}}$ – количество требований по ИБ, предъявляемых к объекту; $N_{\text{тр тест}}$ – количество требований по ИБ, проверяемых в процессе тестирования, при этом отдельное требование по ИБ считается протестированным, если оно проверяется хотя бы одним ИТВ в процессе проведения тестирования.

2) Полнота тестирования требований к объекту по свойствам ИБ:

$$\pi = \frac{\sum_{i=1}^{3} N_{\text{тр тест } i}}{\sum_{i=1}^{3} N_{\text{тр } i}}, \quad \pi_i = \frac{N_{\text{тр тест } i}}{N_{\text{тр } i}}, \qquad (3)$$

где: i – номер свойства ИБ (i=1 – конфиденциальность, i=2 – доступность, i=3 – целостность); π_i – полнота тестирования требований к объекту по i-му свойству ИБ; $N_{\text{тр } i}$ – количество требований по i-му свойству ИБ, предъявляемых к объекту; $N_{\text{тр тест } i}$ – количество требований по i-му свойству ИБ, проверяемых в процессе тестирования, при этом отдельное требование по ИБ считается протестированным, если оно проверяется хотя бы одним ИТВ в процессе проведения тестирования.

3) Полнота тестирования элементов (подсистем) объекта:

$$\pi = \frac{N_{\text{эл тест}}}{N_{\text{эл}}}, \qquad (4)$$

где: $N_{\text{эл}}$ – количество элементов (подсистем) объекта; $N_{\text{эл тест}}$ – количество элементов, проверяемых в процессе тестирования, при этом отдельный элемент (подсистема) считается протестированным, если он проверяется хотя бы одним ИТВ в процессе проведения тестирования.

4) Полнота тестирования элементов (подсистем) объекта по свойствам ИБ:

$$\pi = \frac{\sum_{i=1}^{3} N_{\text{эл тест } i}}{\sum_{i=1}^{3} N_{\text{эл } i}}, \quad \pi_i = \frac{N_{\text{эл тест } i}}{N_{\text{эл } i}}, \qquad (5)$$

где: i – номер свойства ИБ (i=1 – конфиденциальность, i=2 – доступность, i=3 – целостность); π_i – полнота тестирования элементов объекта по i-му свойству ИБ; Nэл i – количество элементов объекта, к котором предъявляются требования по i-му свойству ИБ; $N_{\text{эл тест } i}$ – количество элементов, проверяемых на соответствие по i-му свойству ИБ, при этом отдельный элемент считается протестированным, если он проверяется хотя бы одним ИТВ в процессе проведения тестирования.

5) Полнота тестирования уязвимостей объекта по свойствам ИБ:

$$\pi = \frac{\sum_{i=1}^{3} N_{\text{уяз тест } i}}{\sum_{i=1}^{3} N_{\text{уяз } i}}, \quad \pi_i = \frac{N_{\text{уяз тест } i}}{N_{\text{уяз } i}}, \qquad (6)$$

где: i – номер свойства ИБ (i=1 – конфиденциальность, i=2 – доступность, i=3 – целостность); π_i – полнота тестирования уязвимостей объекта по i-му свойству ИБ; $N_{\text{уяз } i}$ – количество потенциальных уязвимостей объекта по i-му свойству ИБ; $N_{\text{уяз тест } i}$ – количество уязвимостей по i-му свойству ИБ, проверяемых в процессе тестирования, при этом отдельная уязвимость считается протестированной, если она проверялась хотя бы одним ИТВ в процессе проведения тестирования.

6) Полнота тестирования уязвимостей элементов объекта по свойствам ИБ:

$$\pi = \frac{\sum_{i=1}^{3}\sum_{j=1}^{n_{эл}} N_{уяз\ тест\ i,j}}{\sum_{i=1}^{3}\sum_{j=1}^{n_{эл}} N_{уяз\ i,j}}, \quad \pi_{i,j} = \frac{N_{уяз\ тест\ i,j}}{N_{уяз\ i,j}}, \qquad (7)$$

где: i – номер свойства ИБ (i=1 – конфиденциальность, i=2 – доступность, i=3 – целостность); j – номер элемента в составе объекта; $n_{эл}$ – число элементов в составе объекта; $\pi_{i,j}$ – полнота тестирования уязвимостей j-го элемента по i-му свойству ИБ; $N_{уяз\ i,j}$ – количество потенциальных уязвимостей j-го элемента по i-му свойству ИБ; $N_{уяз\ тест\ i,j}$ – количество уязвимостей j-го элемента по i-му свойству ИБ, проверяемых в процессе тестирования, при этом отдельная уязвимость считается протестированной, если она проверялась хотя бы одним ИТВ в процессе проведения тестирования.

7) Полнота тестирования по выявленному и потенциально предотвращенному ущербу в отношении объекта или его владельца с учетом элементов объекта, его уязвимостей и свойств ИБ:

$$\pi = \frac{\sum_{i=1}^{3}\sum_{j=1}^{n_{эл}}\sum_{k=1}^{n_{уяз}} U_{тест\ i,j,k}}{\sum_{i=1}^{3}\sum_{j=1}^{n_{эл}}\sum_{k=1}^{n_{уяз}} U_{i,j,k}}, \qquad (8)$$

где: i – номер свойства ИБ (i=1 – конфиденциальность, i=2 – доступность, i=3 – целостность); j – номер элемента в составе объекта; k – номер потенциальной объекта; $n_{эл}$ – число элементов в составе объекта; $n_{уяз}$ – число уязвимостей объекта; $U_{i,j,k}$ – ущерб от инцидента, реализованного за счет использования k-ой уязвимостей объекта по i-му свойству ИБ для j-го элемента; $U_{тест\ i,j,k}$ – ущерб от инцидента, реализованного за счет использования k-ой уязвимостей объекта по i-му свойству ИБ для j-го элемента, выявленный и потенциально предотвращенный в процессе тестирования, при этом ущерб считается потенциально предотвращенным, если он выявляется хотя бы одним ИТВ в процессе проведения тестирования.

8) Достаточность тестового набора для достижения задачи тестирования:

$$\pi = \frac{N_{тест\ усп}}{N_{тест}}, \qquad (9)$$

где: $N_{тест}$ – количество тестовых ИТВ в тестовом наборе; $N_{тест\ усп}$ – количество тестовых ИТВ, которые успешно реализуют задачу тестирования (о задачах тестирования см. выше), при этом ИТВ считается успешным, если оно достигает хотя бы одной задачи тестирования.

9) Вероятность успешного достижения задачи тестирования:

$$P_{усп} = 1 - \prod_{i=1}^{N_{тест}} \left(1 - P_{тест\ усп\ i}\right), \qquad (10)$$

где: $N_{тест}$ – количество тестовых ИТВ в тестовом наборе; i – номер тестового ИТВ; $P_{тест\ усп\ i}$ – вероятность того что i-ое ИТВ, успешно достигает задачи тестирования.

В качестве показателей полноты могут быть использованы и другие показатели (в некоторых работах они называются «метриками»). Некоторые из таких показателей представлены в работах [3, 26].

3.1.2. Показатели оперативности

В качестве параметра оперативности тестирования могут быть использованы различные параметры, количественно определяющие вероятностно-временные аспекты тестирования. К основным из них относятся показатели, приведенные ниже. При этом данный список не является исчерпывающим, и другие исследователи, в зависимости от контекста и задач тестирования, могут обосновывать и применять свои показатели.

1) Время, за которое будет с заданной вероятностью будет достигнута цель тестирования:

$$T_{тест} = \arg\left(F(T)\right)\Big|F(T) = P_{треб}, \qquad (11)$$

где: $T_{тест}$ – время тестирования (показатель оперативности тестирования), $F(T)$ – функция вероятности, распределения времени тестирования T; arg($F(\circ)$) –аргумент функции $F(\circ)$; $P_{треб}$ – требуемое значение вероятности, которое соответствует уровню достоверности оценки времени тестирования.

2) Время за которое будет достигнута цель тестирования, с учетом детерминированной длительности этапов тестирования. Большинство методик тестирования разделяет этот процесс на этапы, основными из которых являются: анализ системы; поиск уязвимостей; реализации тестовых ИТВ; анализ результатов воздействия и достижения цели тестирования; подготовка итогового отчета. В свою очередь каждый из этих основных этапов состоит из конечного числа подэтапов и операций и т.д. В этом случае время, за которое будет достигнута цель тестирования, с учетом длительности этапов (подэтапов, операций и т.д.) тестирования будет равно:

$$T_{тест} = \sum_{i=1}^{N} T_i, \qquad (12)$$

где: $T_{тест}$ – время тестирования (показатель оперативности тестирования), T_i – длительность n-го этапа тестирования; N – количество этапов тестирования.

3) Время за которое будет с заданной вероятностью будет достигнута цель тестирования, с учетом случайной длительности этапов тестирования. В случае, когда длительность каждого n-го этапа тестирования характеризуется длительностью T_n, которая является случайной величиной, распределенной по нормальному закону, получим следующее. Итоговая длительность тестирования $T_{тест}$ также будет случайной величиной, распределенной по нормальному закону, математическое ожидание (МОЖ) которой $M(T_{тест})$ равно сумме математических ожиданий длительности отдельных этапов $M(T_n)$, а дисперсия $\sigma^2(T_{тест})$ – сумме дисперсий длительности отдельных этапов $\sigma^2(T_n)$. В этом случае время, за которое будет с заданной вероятностью будет достигнута цель тестирования, с учетом длительности этапов тестирования будет равно:

DOI: 10.21681/2311-3456-2021-3-43-57

$$T_{\text{тест}} = \arg\left(\Phi\left(\frac{T - \sum_{n=1}^{N} M(T_n)}{\sqrt{\sum_{n=1}^{N} \sigma^2(T_n)}} \right) \right) \Bigg| \Phi(T) = P_{\text{треб}}, \quad (13)$$

где: $T_{\text{тест}}$ – время тестирования (показатель оперативности тестирования); Ф(T) – функция вероятности нормального распределения; T – время тестирования; T_n – длительность n-го этапа тестирования; arg(Ф (○)) – аргумент функции Ф (○); $M(T_n)$ – МОЖ n-го этапа тестирования; σ^2 (T_n) – дисперсия n-го этапа тестирования; $P_{\text{треб}}$ – требуемое значение вероятности, которое соответствует уровню достоверности оценки времени тестирования.

4) Время, за которое будет с заданной вероятностью будет проведено тестирование с требуемой полнотой. Пусть на достижение определенного значения параметра полноты тестирования π с вероятностью $P(\pi, T_\pi)$ требуется время T_π. Тогда время, за которое с заданной вероятностью будет достигнута требуемая полнота тестирования $\pi_{\text{треб}}$ будет равно:

$$T_{\text{тест}} = \arg\left(F(\pi, T_\pi)\right) \Big| \begin{matrix} \pi = \pi_{\text{треб}}, \\ F(\pi, T_\pi) = P_{\text{треб}}, \end{matrix} \quad (14)$$

где: $T_{\text{тест}}$ – время тестирования (показатель оперативности тестирования); $F(\pi, T_\pi)$ – двухмерная функция вероятности, распределения времени тестирования T_π и полноты π; arg(F(○)) –аргумент функции F(○); $P_{\text{треб}}$ – требуемое значение вероятности, которое соответствует уровню достоверности оценки времени тестирования; π – показатель полноты тестирования; $\pi_{\text{треб}}$ – требуемое значение полноты тестирования.

5) Средняя скорость нахождения уязвимостей:

$$v_{\text{уяз}} = \frac{N_{\text{уяз}}}{T_{\text{тест}}},$$

где: $T_{\text{тест}}$ – время тестирования; $N_{\text{уязв}}$ – количество уязвимостей, найденных за время тестирования $T_{\text{тест}}$.

6) Средняя скорость выявления и потенциального предотвращения ущерба:

$$v_{\text{ущ}} = \frac{U_{\text{тест}}}{T_{\text{тест}}}, \quad (15)$$

$U_{\text{тест}}$ – суммарное значение показателя ущерба, которой бы произойти от инцидента, реализованного за счет использования уязвимостей, выявленных и потенциально предотвращенных в процессе тестирования; $T_{\text{тест}}$ – время тестирования.

8) Эффективность использования времени тестирования:

$$E = \frac{T_{\text{тест усп}}}{T_{\text{тест}}}, \quad (16)$$

где: $T_{\text{тест}}$ – время, затраченное на реализацию всех тестовых ИТВ в тестовом наборе; $T_{\text{тест усп}}$ – время, затраченное на реализацию тестовых ИТВ, которые успешно реализуют задачу тестирования (о задачах тестирования см. выше), при этом ИТВ считается успешным, если оно достигает хотя бы одной задачи тестирования.

3.1.3. Показатели достоверности

Процессы выявления уязвимостей, достижения инцидента, преодоления средств защиты в процессе тестирования – это случайные процессы, успешность которых, в отношении достижения задач тестирования, может зависеть от большого числа разнообразных факторов. К таким факторам относятся: конфигурация средств защиты, выполнение пользователями требований политики безопасности, наличие в системе «типовых» уязвимостей и т.д. Все это ведет к тому, что реакция объекта на тестовые ИТВ носит случайный характер. В результате решение о достижении той или иной задачи тестирования, оценки результативности тестирования, можно принимать только с учетом степени достоверности, которая является статистической мерой точности.

Общие методики оценки достоверности тестирования представлены в работах по обработке экспериментальных данных [43, 44]. Здесь же остановимся на отдельных параметрах оценки достоверности тестирования из этих методик.

1) Точность оценки величины / вероятности события. Пусть результативность тестирования определяется измерением какой-либо ключевой величины или достижения какого-либо события в результате некоторого числа испытаний. Здесь под ключевой величиной можно понимать значение некоторого важного параметра, оцениваемого в процессе тестирования:

- количество инцидентов, инициированных в процессе тестирования;
- количество выявленного и потенциально предотвращенного ущерба;
- вероятностная оценка выполнения свойств конфиденциальности, целостности, доступности и т.д.

Под событием можно понимать достижение какой-либо из задач тестирования:

- успешное преодоление системы защиты объекта;
- формирование инцидента требуемого типа;
- успешное нарушение какого-либо определённого свойства ИБ в отношении объекта и т.д.

При формировании погрешностей точечного оценивания некоторой величины x, физический смысл которой может соответствовать величинам или вероятностям событий, указанных выше, применяются такие статистические оценки как «арифметическое среднее», «выборочное среднее квадратичное отклонение (СКО)» и «выборочный коэффициент вариации» [43].

Пусть в результате проведения N испытаний (реализаций тестовых ИТВ) по оцениванию определённой величины или события была получена выборка значений $x_1, \ldots, x_N$ (для статистической оценки события можно считать, что по итогу испытания x_i принимает значение «1» если событие произошло и «0» – если не произошло).

В этом случае в качестве значения $\tilde{x}$ величины x принимается среднее арифметическое [43]:

$$\tilde{x} = \frac{1}{N} \sum_{i=1}^{N} x_i. \quad (17)$$

Мерой точности оценки величины x может служить «выборочное СКО» [43]:

$$S_x = \sqrt{\frac{1}{N-1}\left(\sum_{i=1}^{N}(x_i - \tilde{x})^2\right)}. \quad (18)$$

Зная среднее арифметическое $\tilde{x}$ и выборочное СКО S_x можно определить меру относительной изменчивости величины x – выборочный коэффициент вариации v_x, значение которого равно [43]:

$$v_x = \frac{S_x}{\tilde{x}}, \quad (19)$$

или в процентах:

$$v_x = \frac{S_x}{\tilde{x}} \cdot 100\%. \quad (20)$$

Довольно часто при оценке точности величин используются понятия «доверительный интервал», «доверительная вероятность», «уровень значимости».

Доверительный интервал – интервал, который с заданной вероятностью накроет действительное значение величины, оцениваемой по выборочным значениям [43].

Доверительная вероятность – вероятность того, что доверительный интервал накроет действительное значение величины, оцениваемой по выборочным значениям [43].

Интервал $[x_{min}, x_{max}]$ называется доверительным, а соответствующую ему вероятность $P_x(x_{min} \le x \le x_{max})$ – доверительной, если с вероятностью $P_x=1-a$ выборочное значение величины x попадет в интервал $[x_{min}, x_{max}]$. Где a – уровень значимости, вероятность того, что доверительный не накроет действительное значение величины. При фиксированном значении a чем меньше доверительный интервал $[x_{min}, x_{max}]$, тем точнее оценивается величина x [43].

Согласно ГОСТ 8.201-76 в технических измерениях следует принимать доверительную вероятность P_x=0,95, а в научных исследованиях P_x=0,68 [44].

Часто доверительный интервал, находится как интервал, симметричный относительной оценки величины. Так для симметричного доверительного интервала его ширина 2δ определяется условием [43]:

$$P_x\left(|x - \tilde{x}| \le \delta\right) = 1 - a, \quad (21)$$

при этом значение доверительного полуинтервала δ фактически соответствует абсолютной погрешности определения величины x: $x=\tilde{x}\pm\delta$ [44].

Достаточно часто, при оценки точности используют меру относительной погрешности, выраженной в процентах:

$$\varepsilon = \frac{\delta}{\tilde{x}} \cdot 100\%.$$

Вышеуказанные оценки точности справедливы для количества испытаний $N \to \infty$ (на практике $N \ge 20$). В этом случае можно принять допущение, что ошибки оценки величины x в отдельных испытаниях распределены по нормальному закону. Однако если количество испытаний $N<20$, то данное допущение неверно и вышеуказанные оценки теряют свою устойчивость, и как результат, пользоваться этими мерами точности нельзя [44].

При небольшом количестве испытаний $N<20$ используют коэффициент Сьюдента t_a [44]:

$$t_a = \frac{\delta}{S_x / \sqrt{n}}. \quad (22)$$

В этом случае, в начале задают доверительную вероятность P_x, затем по числу опытов N и числу искомых величин K (в рассматриваемом случае мы определяем одну величину – x т.е. K=1) определяют число степеней свободы $m=N-K$. По табулированным функциям (заданным в виде таблиц) [44] для P_x и m определяют значение коэффициента t_a, с помощью которого, предварительно вычислив значение S_x можно определить величину доверительного полуинтервала [44]:

$$\delta = \frac{t_a S_x}{\sqrt{n}}. \quad (23)$$

Таким образом, для числа опытов $N<20$ значение величины x с доверительной вероятностью P_x будет лежать в диапазоне $[\tilde{x}-\delta, \tilde{x}+\delta]$.

2) Трудоемкость тестирования для достижения требуемой точности. Результаты отдельных тестов над информационной системой, могут быть различны. Это обусловлено тем что, во-первых, информационная система, сама по себе является сложной организационно-технической системой защищенность и реакция которой зависит от большого числа факторов, во-вторых, условия проведения тестов не всегда являются идентичными: меняется конфигурация средств защиты, нагрузка сети, поведение пользователей и администраторов. В этой связи возникает задача определения числа повторений одних и тех же тестов (числа испытаний), для того чтобы достичь требуемой статистической точности получаемого результата. С учетом того, что на проведение каждого теста (испытания) расходуются человеко-машинные ресурсы уместно говорить о трудоемкости тестирования для достижения требуемой точности.

Здесь под *испытанием* будем понимать однократное проведение определенного одиночного теста. Под *количеством испытаний* будем понимать число проведений над тестируемой системой одного и того же теста. Увеличение количества испытаний позволит повысить доверительную вероятность P_x или сузить доверительный интервал 2δ при неизменной точности оценки результата. Необходимое число испытаний k при известном выборочном СКО S_x и допущении о нормальном распределении результатов испытаний можно определить как [43]:

$$k \ge \frac{t_{a,m}^2 S_x^2}{\delta^2}, \quad (24)$$

где $t_{a,m}$ – значение коэффициента Сьюдента t_a из выражения (22) при числе степеней свободы m.

3) Достоверность проверяемых гипотез. В начале тестирования может быть сформулирована одна или несколько проверяемых гипотез, которые должны быть подтверждены или отвергнуты в процессе тестирования. К таким гипотезам можно отнести следующие: невозможность формирования в системе определённого заранее заданного типа инцидента; защищённость си-

стемы по отношению к определённому типу ИТВ; отсутствие в системе определённых уязвимостей или наоборот их наличие и т.д.

Как правило при проверке гипотез рассматривают нулевую гипотезу H_0 – основную гипотезу подлежащую проверке и одну или несколько альтернативных гипотез, выбор между которыми производится после того как основная гипотеза H_0 будет отклонена.

В процессе тестирования по результатам проведения отдельных тестов набирается статистика, которая позволяет оценить правдоподобность основной гипотезы. Ситуации, возникающие при проверке гипотезы H_0 представлены в таблице 1.

Подробности расчета ошибок первого и второго рода для проверяемых гипотез зависят от функции плотности распределения оцениваемого параметра, на основе которого проверяется гипотеза. Подробности методики проверки гипотезы тестирования более подробно изложены в работе [43].

3.2. Показатели затрат на проведение тестирования

Высокие значения полноты и оперативности тестирования, требуют соответствующих затрат на разработку тестов и проведение тестирования.

В общем случае, понятию «затраты» соответствует следующее определение.

Затраты – ресурсы, необходимые для решения определённой задачи, или достижения требуемого эффекта.

В зависимости от физической сути ресурсов, показатель затрат может быть различен.

Материальные ресурсы – количественная мера оценки всех материальных средств, расходуемых и используемых в процессе разработки теста, проведения тестирования и анализа результатов. Как правило, определяется: стоимостью разработки, покупки или аренды аппаратных и программных средств; стоимостью физического или информационного доступа к объекту тестирования; спутывающие расходы на оплату электроэнергии, аренду помещений и т.д.

Людские ресурсы – количество персонала и длительность его привлечения для разработки теста, проведения тестирования и анализа результатов. Как правило, рассчитывается в человеко-часах и зависит от трудоемкости тестирования.

Временные ресурсы – количество времени, необходимое для разработки теста, проведения тестирования и анализа результатов. Как правило, рассчитывается в часах и зависит от трудоемкости тестирования.

Финансовые ресурсы – денежный эквивалент затрат, требуемых на оплату материальных ресурсов, привлечение людских ресурсов и прочие расходы, необходимые для разработки теста, проведения тестирования и анализа результатов.

Численным показателем последнего ресурса, который в достаточной степени универсален и позволяет интегрально оценить практически все виды затрат вышеперечисленных ресурсов является «стоимость».

Стоимость – выраженная в деньгах величина затрат, по оплате материальных ресурсов, труда людей и прочие расходы, необходимые для разработки теста, проведения тестирования и анализа результатов [26].

Примем в качестве показателя затрат Z в показателе эффективности (1) стоимость создания и эксплуатации программно-аппаратного комплекса (ПАК) тестирования C. Проведем примерную оценку стоимости создания и эксплуатации ПАК тестирования C взяв для этого методику, представленную в работе [45].

Эта стоимость определяется суммированием стоимости обоснования $C_{об}$ задач тестирования и используемого тестового набора на основе предварительного анализа объекта, стоимости создания ПАК тестирования $C_{созд}$ и стоимости годовой эксплуатации этого комплекса $C_{эг}$ в течении срока его службы $T_{сл}$:

$$C = C_{об} + C_{созд} + C_{эг}\, T_{сл}. \qquad (25)$$

Стоимость обоснования $C_{об}$ задач тестирования и используемого тестового набора на основе предварительного анализа объекта рассчитывается на основе стоимости работы группы аудиторов и тестировщиков, которые проводят первоначальное обследование объекта тестирования, формируют рекомендации по проверяемым уязвимостям, составляют план проведения тестирования:

$$C_{об} = N_{ауд} \cdot C_{ауд} \cdot T_{об},$$

где: $N_{ауд}$ – количество аудиторов и тестировщиков, привлекаемых к первоначальному обследованию объекта и составлению плана тестирования; $C_{ауд}$ – средняя стоимость оплаты труда аудитора в год; $T_{об}$ – длительность первоначального обследования объекта и составления плана тестирования (в годах).

Таблица 1

Ситуации, возникающие при проверке гипотезы H_0

Фактическая ситуация	Гипотеза H_0 принимается	Гипотеза H_0 отклоняется
Гипотеза H_0 верна	Правильное решение	Ошибка 1-го рода (*a*) – ошибочное отклонение гипотезы H_0, в то время как в действительности она верна
Гипотеза H_0 не верна	Ошибка 2-го рода (β) – ошибочное принятие гипотезы H0, в то время как в действительности она не верна	Правильное отклонение

При этом стоимость создания ПАК $C_{созд}$ рассчитывается исходя из стоимости покупных изделий для ПАК $C_{ПИ}$, затрат на разработку нового программного обеспечения (ПО) для ПАК $C_{ПО}$, затрат на разработку специализированных аппаратных средств для ПАК $C_{САС}$, а также доли других капиталовложений K на производство одного ПАК:

$$C_{созд} = C_{ПИ} + C_{ПО} + C_{САС} + K. \quad (26)$$

Если ПАК является сложной системой, то капиталовложения K необходимо рассчитывать по составляющим.

Подавляющая часть работ по созданию новых ПАК тестирования основана покупке готовых аппаратных и программных средств, при этом новое ПО и специализированные аппаратные средства разрабатываются только в случае необходимости проведения каких-либо узко направленных или специализированных тестовых ИТВ, которые не могут быть реализованы существующими средствами. Для таких ПАК доля других капиталовложений либо равна нулю, либо не превышает 10 %. Таким образом, ведя допущение о $K \approx 0$ выражение (26) примет вид:

$$C_{созд} = C_{ПИ} + C_{ПО} + C_{САС}. \quad (27)$$

Стоимость покупных изделий ($C_{ПИ}$), к которым будем относить все аппаратные, сетевые и программные средства, которые не разрабатываются, а могут быть закуплены в готовом виде у поставщиков, из (26) рассчитывается как:

$$C_{ПИ} = C_{СПН} + \sum_{i=1}^{J} \left(N_{изд\,i} C_{ПИ\,i} + C_{тр\,i} \right), \quad (28)$$

где: $N_{изд\ i}$ – количество изделий i-го типа для ПАК; $C_{ПИ\,i}$ – цена одного покупного изделия i-го типа для ПАК; $C_{тр\,i}$ – транспортные расходы на доставку изделия i-го типа для ПАК; J – количество типов покупных изделий для ПАК; $C_{СПН}$ – расходы на сборку всех изделий в единый ПАК и на пуско-наладочные работы.

Стоимость разработки нового ПО $C_{ПО}$ и специализированных аппаратных средств $C_{САС}$, которые реализует специализированные тестовые ИТВ, которые не могут быть реализованы существующими средствами, в выражении (27) оценивается примерно по одинаковой схеме:

$$C_{ПО} = C_{КПН} + \sum_{i=1}^{Z_{ПС}} \left(C_{ПИ\,i} + C_{разр\,i} \right), \quad (29)$$

$$C_{САС} = C_{СПН\,САС} + \sum_{i=1}^{Z_{САС}} \left(C_{ПИ\,i} + C_{тр\,i} + C_{разр\,i} \right), \quad (30)$$

где: $Z_{ПС}$ – количество вновь разрабатываемых программных средств; $Z_{САС}$ – количество вновь разрабатываемых специальных аппаратных средств; $C_{КПН}$ – расходы на комплексирование вновь разработанных программных средств между собой и интеграцию их в ПО ПАК, а также на пуско-наладочные работы; $C_{СПН\ САС}$ – расходы на сборку всех средств в единый ПАК и на пуско-наладочные работы; $C_{ПИ\,i}$ – цена покупных изделий для разработки i-го средства; $C_{разр\,i}$ – стоимость разработки i-го средства; $C_{тр\,i}$ – транспортные расходы на доставку покупных изделий для i-го средства.

При этом стоимость разработки каждого i-го средства $C_{разр\,i}$ в выражениях (29) и (30) может быть оценена по затратам на привлечение специалистов, осуществляющих разработку:

$$C_{разр\,i} = N_{спц\,i} \cdot C_{спц\,i} \cdot T_{разр\,i},$$

где: $N_{спц\,i}$ – количество специалистов, привлекаемых к разработке i-го средства; $C_{спц\,i}$ – средняя стоимость оплаты труда специалиста, привлекаемого к разработке i-го средства (в год); $T_{разр\,i}$ – длительность разработки i-го средства (в годах).

Годовая стоимость эксплуатации ТС $C_{эг}$ из выражения (25) рассчитывается как:

$$C_{эг} = C_{мг} + C_{обсл\,г} + C_{эн\,г} + C_{рг} + C_{аг} + C_{пр\,г}, \quad (31)$$

где: $C_{мг}$ – стоимость материалов, расходуемых в процессе эксплуатации ПАК за год; $C_{обсл\,г}$ – расходы на рабочий и обслуживающий персонал ПАК за год; $C_{эн\,г}$ – расходы на энергию всех видов для ПАК за год; $C_{рг}$ – стоимость ремонтов ПАК за год; $C_{аг}$ – амортизационные отчисления за год; $C_{пр\,г}$ – прочие годовые расходы.

Заключение

В представленной статье автором предпринята попытка подвести научную основу под такой практический тип аудита ИБ, как тестирование на проникновение, а именно – на качественном и количественном уровне сформировать критерии оценки эффективности проведения тестирования и выбора ИТВ в тестовый набор.

Положения, представленные в данной статье, на взгляд автора, не являются окончательными, а носят, в большей степени, дискуссионный характер. Автор не претендует на окончательную верность своих суждений, однако надеется, что его работа станет своеобразной «отправной точкой» для специалистов в области ИБ при формировании научно-обоснованных подходов для такого перспективного способа аудита ИБ, как тестирование на проникновение.

В дальнейших работах автор планируют продолжить работу по развитию и конкретизации формальных выражений для критериев «эффективность / стоимость», показателей эффективности и стоимости, а также методик их вычисления и моделей анализа.

Исследование выполнено 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. 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.
4. Скабцов Н. Аудит безопасности информационных систем. СПб.: Питер, 2018. 272 с.
5. Penetration Testing. Procedures & Methodologies. – EC-Council Press, 2011. 237 p.
6. Kennedy D., O'Gorman J., Kearns D., Aharoni M. Metasploit. The Penetration Tester's Guide. San Francisco: No Starch Press, 2011. 299 p.
7. Makan K. Penetration Testing with the Bash shell. – Birmingham: Pact Publishing, 2014. 133 p.
8. Cardwell K. Building Virtual Pentesting Labs for Advanced Penetration Testing. Birmingham: Pact Publishing, 2016. 518 p.
9. 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.
10. Климов С. М. Имитационные модели испытаний критически важных информационных объектов в условиях компьютерных атак // Известия ЮФУ. Технические науки. 2016. № 8 (181). С. 27–36.
11. 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.
12. Петренко А. А., Петренко С. А. Киберучения: методические рекомендации ENISA // Вопросы кибербезопасности. 2015. № 3 (11). С. 2–14.
13. 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.
14. Дорофеев А. Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? // Защита информации. Инсайд. 2010. № 6 (36). С. 72–73.
15. Умницын М. Ю. Подход к полунатурному анализу защищенности информационной системы // Известия Волгоградского государственного технического университета. 2018. № 8 (218). С. 112–116.
16. Бородин М. К., Бородина П. Ю. Тестирование на проникновение средства защиты информации VGATE R2 // Региональная информатика и информационная безопасность. СПб., 2017. С. 264–268.
17. Трещев И. А., Воробьев А. А. О подходе к проведению тестирования на наличие уязвимостей информационных систем // Производственные технологии будущего: от создания к внедрению. Материалы международной научно-практической конференции. Комсомольск-на-Амуре, 2017. С. 175–182.
18. Baloch R. Ethical hacking and penetration testing guide. London: CRC Press, 2017. 492 c.
19. 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.
20. Кадан А. М., Доронин А. К. Инфраструктурные облачные решения для задач тестирования на проникновение // Ученые записки ИСГЗ. 2016. Т. 14. № 1. С. 296–302.
21. Еременко Н. Н., Кокоулин А. Н. Исследование методов тестирования на проникновение в информационных системах // Master's Journal. 2016. № 2. С. 181–186.
22. Туманов С. А. Средства тестирования информационной системы на проникновение // Доклады Томского государственного университета систем управления и радиоэлектроники. 2015. № 2 (36). С. 73–79.
23. Кравчук А. В. Модель процесса удаленного анализа защищенности информационных систем и методы повышения его результативности // Труды СПИИРАН. 2015. № 1 (38). С. 75–93.
24. Горбатов В. С., Мещеряков А. А. Сравнительный анализ средств контроля защищенности вычислительной сети // Безопасность информационных технологий. 2013. Т. 20. № 1. С. 43–48.
25. Косенко М. Ю. Сбор информации при проведении тестирования на проникновение // Вестник УрФО. Безопасность в информационной сфере. 2013. № 3 (9). С. 11–15.
26. Макаренко С. И. Справочник научных терминов и обозначений. СПб.: Наукоемкие технологии, 2019. 254 с.
27. 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.
28. 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.
29. 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.
30. 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.

31. Moeller R. R. IT Audit, Control, and Security. Hoboken: John Wile & Sons, Inc., 2010. 667 p.
32. McDermott J. P. Attack net penetration testing // NSPW. 2000. С. 15-21.
33. Klevinsky T. J., Laliberte S., Gupta A. Hack IT: security through penetration testing. Addison-Wesley Professional, 2002. 512 с.
34. Pfleeger C. P., Pfleeger S. L., Theofanos M. F. A methodology for penetration testing // Computers & Security. 1989. Т. 8. № 7. С. 613–620.
35. Alisherov F., Sattarova F. Methodology for penetration testing // International Journal of Grid and Distributed Computing. 2009. С. 43–50.
36. Ami P., Hasan A. Seven phrase penetration testing model // International Journal of Computer Applications. 2012. Т. 59. № 5. С. 16–20.
37. Holik F., Horalek J., Marik O., Neradova S., Zitta S. Effective penetration testing with Metasploit framework and methodologies // 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI). IEEE, 2014. С. 237–242.
38. Herzog P. Open-source security testing methodology manual // Institute for Security and Open Methodologies (ISECOM). 2003.
39. Engebretson P. The Basics of Hacking and Penetration Testing. Ethical Hacking and Penetration Testing Made Easy. Amsterdam: Syngress, Elsevier, 2011. 159 с.
40. 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.
41. Бегаев А. Н., Бегаев С. Н., Федотов В. А. Тестирование на проникновение. СПб: Университет ИТМО, 2018. 45 с.
42. Богораз А. Г., Пескова О. Ю. Методика тестирования и оценки межсетевых экранов // Известия ЮФУ. Технические науки. 2013. № 12 (149). С. 148–156.
43. Спирин Н. А., Лавров В. В. Методы планирования и обработки результатов эксперимента / под ред. Н.А. Спирина. – Екатеринбург: ГОУ ВПО УГТУ-УПИ, 2004. 257 с.
44. Хорольский В. Я., Таранов М. А., Шемякин В. Н., Аникуев С. В. Экспериментальные исследования в электроэнергетике и агроинженерии. Ставрополь: АГРУС, 2013. 106 с.
45. Макаренко С. И. Технико-экономический анализ целесообразности внедрения новых технологических решений // Системы управления, связи и безопасности. 2016. № 1. С. 278–287. DOI: 10.24411/2410-9916-2016-10112.

CRITERIA AND PARAMETERS FOR ESTIMATING QUALITY OF PENETRATION TESTING

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. An analysis of publications in this area shows that there is not mathematical approaches to selection of tests, as well as parameters and criteria for evaluating the effectiveness of penetration testing.*

The goals of the paper *is to form specific parameters of completeness, efficiency, reliability and cost of testing, as well as, in a generalized form, a group of criteria "efficiency/cost", allowing to estimate the quality of test sets, as well as to compare different penetration testing scenarios with each other.*

Research methods. *Methods of probability theory and mathematical statistics, methods of processing experimental data, as well as the results of other studies in the field of software security testing are used in the paper to achieve the research goals.*

Results. *The general form of the "efficiency/cost" criteria for estimating the quality of penetration testing, as well as formal particular parameters for evaluating separate parameters in the proposed criteria – the parameters of completeness, efficiency, reliability and cost are presented in the paper. The results of the paper can be used by auditors and testers to objectively justify test sets and compare different penetration testing scenarios with each other. The material of the paper can be useful for specialists who make research is such an area as penetration testing.*

Keywords: *penetration testing, information technology impact, testing quality criterion, testing quality, testing completeness, testing efficiency, testing reliability, testing cost.*

2 Sergey Makarenko, Dr.Sc., Associate Professor, Lead researcher St. Petersburg Federal Research Center of the Russian Academy of Sciences. The field of scientific interests: networks and communication systems; Electronic warfare; Information security Information confrontation. St. Petersburg, Russia. E-mail: mak-serg@yandex.ru. ORCID: 0000-0001-9385-2074

References

1. Makarenko S. I. Audit informatcionnoi` bezopasnosti: osnovny`e e`tapy`, kontceptual`ny`e osnovy`, classifikatciia meropriiatii` // Sistemy` upravleniia, sviazi i bezopasnosti. 2018. № 1. S. 1–29. DOI: 10.24411/2410-9916-2018-10101.
2. Makarenko S. I. Audit bezopasnosti kriticheskoi` infrastruktury` spetcial`ny`mi informatcionny`mi vozdei`stviiami. Monografiia. SPb.: Naukoemkie tekhnologii, 2018. 122 s.
3. Markov A. S., Tcirlov V. L., Barabanov A. V. Metody` ocenki nesootvetstviia sredstv zashchity` informatcii / pod red. A.S. Markova. – M.: Radio i sviaz`, 2012. 192 s.
4. Skabtcov N. Audit bezopasnosti informatcionny`kh sistem. SPb.: Peter, 2018. 272 s.
5. Penetration Testing. Procedures & Methodologies. – EC-Council Press, 2011. 237 p.
6. Kennedy D., O'Gorman J., Kearns D., Aharoni M. Metasploit. The Penetration Tester's Guide. San Francisco: No Starch Press, 2011. 299 p.
7. Makan K. Penetration Testing with the Bash shell. – Birmingham: Pact Publishing, 2014. 133 p.
8. Cardwell K. Building Virtual Pentesting Labs for Advanced Penetration Testing. Birmingham: Pact Publishing, 2016. 518 p.
9. Makarenko S. I., Smirnov G. E. Analiz standartov i metodik testirovaniia na proniknovenie // Sistemy` upravleniia, sviazi i bezopasnosti. 2020. № 4. S. 44–72. DOI: 10.24411/2410-9916-2020-10402.
10. Climov S. M. Imitatcionny`e modeli ispy`tanii` kriticheski vazhny`kh informatcionny`kh ob``ektov v usloviiakh komp`iuterny`kh atak // Izvestiia IUFU. Tekhnicheskie nauki. 2016. № 8 (181). S. 27–36.
11. Climov S. M., Sy`chyov M. P. Stendovy`i` poligon uchebno-trenirovochny`kh i ispy`tatel`ny`kh sredstv v oblasti obespecheniia informatcionnoi` bezopasnosti // Informatcionnoe protivodei`stvie ugrozam terrorizma. 2015. № 24. S. 206–213.
12. Petrenko A. A., Petrenko S. A. Kiberucheniia: metodicheskie rekomendatcii ENISA // Voprosy` kiberbezopasnosti. 2015. № 3 (11). S. 2–14.
13. Baranova E. K., Hudy`shkin A. A. Osobennosti analiza bezopasnosti informatcionny`kh sistem metodom testirovaniia na proniknovenie // Modelirovanie i analiz bezopasnosti i riska v slozhny`kh sistemakh. Trudy` mezhdunarodnoi` nauchnoi` shkoly` MABR - 2015. S. 200–205.
14. Dorofeev A. Testirovanie na proniknovenie: demonstratciia odnoi` uiazvimosti ili ob``ektivnaia ocenka zashchishchennosti? // Zashchita informatcii. Insai`d. 2010. № 6 (36). S. 72–73.
15. Umnitcy`n M. Iu. Podhod k polunaturnomu analizu zashchishchennosti informatcionnoi` sistemy` // Izvestiia Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta. 2018. № 8 (218). S. 112–116.
16. Borodin M. K., Borodina P. Iu. Testirovanie na proniknovenie sredstva zashchity` informatcii VGATE R2 // Regional`naia informatika i informatcionnaia bezopasnost`. SPb., 2017. S. 264–268.
17. Treshchev I. A., Vorob`ev A. A. O podhode k provedeniiu testirovaniia na nalichie uiazvimostei` informatcionny`kh sistem // Proizvodstvenny`e tekhnologii budushchego: ot sozdaniia k vnedreniiu. Materialy` mezhdunarodnoi` nauchno-prakticheskoi` konferentcii. Komsomol`sk-na-Amure, 2017. S. 175–182.
18. Baloch R. Ethical hacking and penetration testing guide. London: CRC Press, 2017. 492 c.
19. Poltavtceva M. A., Pechenkin A. I. Intellektual`ny`i` analiz danny`kh v sistemakh podderzhki priniatiia reshenii` pri testirovanii na proniknovenie // Problemy` informatcionnoi` bezopasnosti. Komp`iuterny`e sistemy`. 2017. № 3. S. 62–69.
20. Kadan A. M., Doronin A. K. Infrastrukturny`e oblachny`e resheniia dlia zadach testirovaniia na proniknovenie // Ucheny`e zapiski ISGZ. 2016. T. 14. № 1. S. 296–302.
21. Eremenko N. N., Kokoulin A. N. Issledovanie metodov testirovaniia na proniknovenie v informatcionny`kh sistemakh // Master's Journal. 2016. № 2. S. 181–186.
22. Tumanov S. A. Sredstva testirovaniia informatcionnoi` sistemy` na proniknovenie // Doclady` Tomskogo gosudarstvennogo universiteta sistem upravleniia i radioe`lektroniki. 2015. № 2 (36). S. 73–79.
23. Kravchuk A. V. Model` protcessa udalennogo analiza zashchishchennosti informatcionny`kh sistem i metody` povy`sheniia ego rezul`tativnosti // Trudy` SPIIRAN. 2015. № 1 (38). S. 75–93.
24. Gorbatov V. S., Meshcheriakov A. A. Sravnitel`ny`i` analiz sredstv kontrolia zashchishchennosti vy`chislitel`noi` seti // Bezopasnost` informatcionny`kh tekhnologii`. 2013. T. 20. № 1. S. 43–48.
25. Kosenko M. Iu. Sbor informatcii pri provedenii testirovaniia na proniknovenie // Vestneyk UrFO. Bezopasnost` v informatcionnoi` sfere. 2013. № 3 (9). S. 11–15.
26. Makarenko S. I. Spravochnik nauchny`kh terminov i oboznachenii`. SPb.: Naukoemkie tekhnologii, 2019. 254 s.
27. Boi`ko A. A., D`iakova A. V. Sposob razrabotki testovy`kh udalenny`kh informatcionno-tekhnicheskikh vozdei`stvii` na prostranstvenno raspredelenny`e sistemy` informatcionno-tekhnicheskikh sredstv // Informatcionno-upravliaiushchie sistemy`. 2014. № 3 (70). S. 84–92.
28. Boi`ko A. A., D`iakova A. V., KHramov V. Iu. Metodicheskii` podhod k razrabotke testovy`kh sposobov udalennogo informatcionno-tekhnicheskogo vozdei`stviia na prostranstvenno raspredelenny`e sistemy` informatcionno-tekhnicheskikh sredstv // Kibernetika i vy`sokie tekhnologii XXI veka XV Mezhdunarodnaia nauchno-tekhnicheskaia konferentciia. Voronezh: NPF «SAKVOEE», 2014. S. 386–395.
29. Boi`ko A. A., Obushchenko E. Iu., Shcheglov A. V. Osobennosti sinteza polnogo mnozhestva testovy`kh sposobov udalennogo informatcionno-tekhnicheskogo vozdei`stviia na prostranstvenno raspredelenny`e sistemy` informatcionno-tekhnicheskikh sredstv // Vestneyk Voronezhskogo gosudarstvennogo universiteta. Seriia: Sistemny`i` analiz i informatcionny`e tekhnologii. 2017. № 2. S. 33–45.
30. Shcheglov A. V., KHramov V. Iu. Sposob razrabotki testovy`kh udalenny`kh informatcionno-tekhnicheskikh vozdei`stvii` na prostranstvenno-raspredelenny`e sistemy` informatcionno-tekhnicheskikh sredstv // Sbornik studencheskikh nauchny`kh rabot fakul`teta komp`iuterny`kh nauk VGU FGBOU VO «Voronezhskii` gosudarstvenny`i` universitet». Voronezh, 2016. S. 203–210.

31. Moeller R. R. IT Audit, Control, and Security. Hoboken: John Wile & Sons, Inc., 2010. 667 p.
32. McDermott J. P. Attack net penetration testing // NSPW. 2000. S. 15-21.
33. Klevinsky T. J., Laliberte S., Gupta A. Hack IT: security through penetration testing. Addison-Wesley Professional, 2002. 512 c.
34. Pfleeger C. P., Pfleeger S. L., Theofanos M. F. A methodology for penetration testing // Computers & Security. 1989. T. 8. № 7. S. 613–620.
35. Alisherov F., Sattarova F. Methodology for penetration testing // International Journal of Grid and Distributed Computing. 2009. S. 43–50.
36. Ami P., Hasan A. Seven phrase penetration testing model // International Journal of Computer Applications. 2012. T. 59. № 5. S. 16–20.
37. Holik F., Horalek J., Marik O., Neradova S., Zitta S. Effective penetration testing with Metasploit framework and methodologies // 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI). IEEE, 2014. S. 237–242.
38. Herzog P. Open-source security testing methodology manual // Institute for Security and Open Methodologies (ISECOM). 2003.
39. Engebretson P. The Basics of Hacking and Penetration Testing. Ethical Hacking and Penetration Testing Made Easy. Amsterdam: Syngress, Elsevier, 2011. 159 c.
40. Baranova E. K., Chernova M. V. Sravnitel`ny`i` analiz programmnogo instrumentariia dlia analiza i ocenki riskov informatcionnoi` bezopasnosti // Problemy` informatcionnoi` bezopasnosti. Komp`iuterny`e sistemy`. 2014. № 4. S. 160–168.
41. Begaev A. N., Begaev S. N., Fedotov V. A. Testirovanie na proniknovenie. SPb: Universitet ITMO, 2018. 45 s.
42. Bogoraz A. G., Peskova O. Iu. Metodika testirovaniia i ocenki mezhsetevy`kh e`kranov // Izvestiia IUFU. Tekhnicheskie nauki. 2013. № 12 (149). S. 148–156.
43. Spirin N. A., Lavrov V. V. Metody` planirovaniia i obrabotki rezul`tatov e`ksperimenta / pod red. N.A. Spirina. – Ekaterinburg: GOU VPO UGTU-UPI, 2004. 257 s.
44. Horol`skii` V. Ia., Taranov M. A., Shemiakin V. N., Anikuev S. V. E`ksperimental`ny`e issledovaniia v e`lektroe`nergetike i agroinzhenerii. Stavropol`: AGRUS, 2013. 106 s.
45. Makarenko S. I. Tekhniko-e`konomicheskii` analiz tcelesoobraznosti vnedreniia novy`kh tekhnologicheskikh reshenii` // Sistemy` upravleniia, sviazi i bezopasnosti. 2016. № 1. S. 278–287. DOI: 10.24411/2410-9916-2016-10112.