УДК 004.056

# АНАЛИЗ МЕТОДОВ ТЕСТИРОВАНИЯ ДЛЯ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Мухамеджанова К.А., Мекенбаева А.М., Абдулаев А.А.**
Кыргызский государственный университет строительства, транспорта и архитектуры им. Н. Исанова

В статье проводится анализ методов тестирования с целью проведения аудита информационной безопасности информационной системы.

***Ключевые слова:*** тесты, тести при аудите, аудит информационной безопасности, пентесты.

# МААЛЫМАТТЫК КООПСУЗДУКТУН АУДИТИН ЖҮРГҮЗҮҮ ҮЧҮН ТЕСТИРЛӨӨ ЫКМАЛАРЫН ТАЛДОО

**Мухамеджанова К.А., Мекенбаева А.М.**
Н.Исанов атындагы Кыргыз мамлекеттик курулуш, транспорт жана архитектура университети

Макалада маалыматтык системанын маалыматтык коопсуздугунун аудитин жүргүзүү максатында тестирлөө ыкмаларын талдоо жүргүзүлөт.

***Баштапкы сөздөр****:* тест, аудиттеги тест, маалыматтык коопсуздуктун аудити, пентесттер.

# ANALYSIS OF TESTING METHODS FOR CONDUCTING AN INFORMATION SECURITY AUDIT

**Mukhamedzhanova K.A., Mekenbayeva A.M.**
Kyrgyz state university of construction, transport and architecture named after N. Isanov

The article analyzes the methods of testing in order to audit the information security of an information system.

***Keywords:*** tests, fathers-in-law at audit, internal audit of information security, pentests.

При построении систем информационной безопасности (ИБ) важное значение имеют процессы контроля адекватности мер и средств защиты, а также выявление уязвимостей в существующей информационной системе. Аудит ИБ позволяет провести такой контроль и выявить новые уязвимости. Однако в известных работах недостаточно внимания уделяется системной классификации мероприятий аудита, а также внутреннему аудиту как одному из основных типов аудита ИБ. Эксперименты по тестированию реальных систем при проведении рассматриваются в ограниченном виде исключительно как «тестирование на проникновение» или как «инструментальный аудит», при этом проведение такого типа аудита не регламентируется каким-либо системным подходом [1].

В настоящее время имеется значительное количество работ, посвященных аудиту ИБ. Однако, материалы представлены в подавляющем большинстве этих работ не соответствуют системному подходу, терминология и классификация мероприятий аудита используемые в известных работах отличаются противоречивостью и неоднозначностью.

Кроме того, общими недостатками известных работ является то, что основной упор в них делается на: этапы проведения аудита и мероприятия на каждом из этапов; проведение аудита только на основе анализа рисков или анализа стандартов ИБ; формирование и формализацию модели аудита, модели нарушителя/противника, модели угроз. В известных работах недостаточно внимания уделяется системной классификации мероприятий аудита, а также тестированию как одному из типов аудита ИБ. Эксперименты по тестированию реальной ИС рассматриваются в ограниченном виде исключительно как «тестирование на проникновение» или как «инструментальный аудит», при этом проведение такого типа аудита не регламентируется каким-либо системным или даже теоретическим подходом [2, 3].

Аудит представляет собой независимую экспертизу отдельных областей функционирования организации. Различают внешний и внутренний

аудит. Внешний аудит — это, как правило, разовое мероприятие, проводимое по инициативе руководства организации или акционеров. Рекомендуется проводить внешний аудит регулярно, а, например, для многих финансовых организаций и акционерных обществ это является обязательным требованием со стороны их учредителей и акционеров. Внутренний аудит представляет собой непрерывную деятельность, которая осуществляется на основании «Положения о внутреннем аудите» и в соответствии с планом, подготовка которого осуществляется подразделениями службы безопасности и утверждается руководством организации.

Целями проведения аудита безопасности являются [4]:

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов;
- оценка текущего уровня защищенности ИС;
- локализация узких мест в системе защиты ИС;
- оценка соответствия ИС существующим стандартам в области информационной безопасности;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС.

Аудит безопасности предприятия (фирмы, организации) должен рассматриваться как конфиденциальный инструмент управления, исключающий в целях конспирации возможность предоставления информации о результатах его деятельности сторонним лицам и организациям.

Тестирование при аудите ИБ информационных систем — это определение одной или нескольких параметров системы характеризующих определенную категорию ИБ (например, целостности, доступности, конфиденциальности).

Более общим определением тестирования является следующее.

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

Отдельное мероприятие по исследованию системы или способ изучения процессов ее функционирования называется тестом.

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

1) тесты должны проверять требования к проверяемой системе;

2) ситуации, используемые в тестах, должны обеспечивать определенную представительность по отношению ко всем возможным вариантам поведения проверяемой системы, иначе выводы о качестве системы, сделанные на основе проведенного тестирования, будут недостоверны.

Второе требование к тестовому набору принято называть полнотой тестирования и характеризовать с помощью выбираемых критериев полноты, задающих разбиения пространства всех возможных ситуаций на классы эквивалентности точки зрения возможных ошибок. Так, если в одной из ситуаций данного класса возникает ошибка, то она с большой вероятностью проявляется и в других ситуациях этого класса.

Общая классификация мероприятий, способов и средств тестирования используемых при аудите ИБ представлена на рис. 3.4.

Основаниями, по которым могут быть классифицированы мероприятия, способы и средства тестирования:

1) по цели;

2) по степени воздействия на объект аудита;

3) по степени легальности;

Цели тестирования можно классифицировать следующим образом:

- превентивные - направленные на превентивное выявление угроз, уязвимостей и предотвращение инцидентов ИБ;

- детектирующие - направленные на обнаружение новых или уточнение особенностей уже имеющихся угроз и уязвимостей системы защиты вовремя или после инцидентов ИБ;
- корректирующие - направленные на формирование комплекса мер повышения эффективности существующей системы защиты после инцидентов ИБ с учетом вновь выявленных угроз и уязвимостей.

По степени воздействия на объект исследования могут быть выделены следящие виды тестирования:

- пассивное;
- активное.

Пассивное тестирование не вносит изменений в реальный объект исследования или его модель-прототип, а также не переводит их в измененное состояние. К пассивному тестированию относятся подача на вход тестируемой системы различных вариантов входных (в том числе и некорректных) данных, изучение поведения системы в новых условиях, тестирование на основе моделей когда параметр нарушителя/противника является постоянно действующим случайным фактором в модели и т. д. Так же к пассивному тестированию также можно отнести мероприятия связанные с экспериментальным применением средств и способов ИТВ или ИПВ пассивно-разведывательного характера, ориентированных на наблюдение и сбор сведений об объекте тестирования или его средств защиты.

Активное тестирование, предусматривает целенаправленное воздействие на объект, с целью провести анализ его реакций или перевести его в требуемое состояние, как правило, с более низким уровнем защищенности. К активному тестированию можно отнести проведение тестирования объекта целенаправленными ИТВ и ИПВ, внесение изменений в код тестируемой программы или в аппаратную часть технических средств, а также тесты на проникновение.

По степени легальности тестирование может быть классифицировано на:

- легальное;
- нелегальное.

Легальное тестирование, проводятся на основании договора с заказчиком, имеющим прямое отношение к обеспечению ИБ объекта аудита, с целью выработки мер, направленных на повышение уровня его защиты.

Нелегальное тестирование связанно с получением информации об уязвимостях объекта тестирования с использованием способов, которые содержат признаки противоправных деяний.

По местонахождению относительно объекта, тестирование может быть классифицировано на:

- внешнее;
- внутреннее.

Внешнее тестирование - проводится с использованием средств и способов, находящихся вне тестируемого объекта. К таким способам тестирования можно отнести: использование специальных ИТВ и ИПВ ориентированных на проверку устойчивости защищаемого периметра объекта, тесты на проникновение, создание неблагоприятной среды функционирования и т. д.

Внутреннее тестирование - проводится с использованием средств и способов, находящихся внутри защищаемого периметра тестируемого объекта. К таким способам тестирования можно отнести: использование новых программных или аппаратных модулей, внедряемых в технические средства, использование способов ИПВ внутри коллектива организации, использование специальных ИТВ и ИПВ ориентированных на проверку устойчивости защищаемого периметра объекта, тесты на проникновение, создание неблагоприятной среды функционирования и т. д.

## ЛИТЕРАТУРА

1. Аверичников В. И., Рытов М. Ю., Кувылкин А. В., Рудановский М. В. Аудит информационной безопасности органов исполнительной власти: учебное пособие. - М.: Флинта, 2011. - 100 с.

2. Кульба В. В., Шелков А. Б., Гладков Ю. М., Павельев С. В. Мониторинг и аудит информационной безопасности автоматизированных систем. - М.: ИПУ им. В.А. Трапезникова РАН, 2009. - 94 с.
3. Астахов А. Введение в аудит информационной безопасности [Доклад] // GlobalTrust Solutions [Электронный ресурс]. 2018. - URL: http://globaltrust.ru (дата обращения: 29.01.2018).
4. Скабцов Н. Аудит безопасности информационных систем. - СПб.: Питер, 2018. - 272 с.