УДК 004.056

Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий

Макаренко С. И.

Актуальность. *При построении систем информационной безопасности (ИБ) важное значение имеют процессы контроля адекватность 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 тестированию как одному из основных типов аудита ИБ. Эксперименты по тестированию реальных систем 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.* ***Целью работы является*** *систематизация основных сведений об этапах, теоретических и практических подходах к аудиту ИБ, классификации мероприятий аудита. Особое внимание в работе уделено вопросам тестирования и экспериментального исследования информационных систем.* ***Результаты и их новизна.*** *В работе представлен авторский подход к систематизации и классификации мероприятий аудита и тестирования. Рассмотрен теоретический подход к аудиту на основе известной концепции «тестирование на основе моделей». Предложен новый практический подход к аудиту – экспериментальное исследование систем с использованием специальных способов и средств на основе информационно-технических и информационно-психологических воздействий.* ***Используемые методы.*** *При проведении систематизации и классификации мероприятий аудита использовались методы системного анализа, логической индукции и дедукции.* ***Практическая значимость.*** *Представленная в работе систематизация и классификация мероприятий аудита и тестирования, а также предложения по проведению аудита в виде экспериментальных исследований может быть использована для обоснования разработки новых средств и способов информационно-технических и информационно-психологических воздействий, целью применения которых является аудит ИБ широкого спектра прикладных систем.*

Ключевые слова: *информационная безопасность, аудит, аудит информационной безопасности, тестирование, тестирование на основе моделей, тестирование на основе специальных средств и способов, информационное противоборство, информационно-техническое воздействие, информационно-психологическое воздействие.*

Актуальность

При построении системы обеспечения информационной безопасности (ИБ) наряду с процессами реализации защитных мер, обучения персонала, внедрения политики безопасности и т. д., важное значение имеют процессы контроля и проверки состояния ИБ. Такой контроль позволяет проверить адекватность выбранных мер и средств защиты, а также выявить уязвимости в су-

Библиографическая ссылка на статью:
Макаренко С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. С. 1–29. URL: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf

Reference for citation:
Makarenko S. I. Audit of Information Security – the Main Stages, Conceptual Framework, Classification of Types. *Systems of Control, Communication and Security*, 2018, no. 1, pp. 1–29. Available at: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf (in Russian).

ществующей информационной системе (ИС). Среди процессов контроля и проверки ИБ особое положение занимает аудит ИБ, основным назначением которого является формирование независимой оценки ИБ.

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.

Цель статьи – систематизировать основные сведения об этапах, теоретических и практических подходах к аудиту ИБ, классификации мероприятий аудита. Особое внимание в работе уделено вопросам тестирования ИС, как одного из основных типов аудита. В работе представлен авторский подход к систематизации и классификации мероприятий тестирования, с учетом возможности использования специальных способов и средств на основе информационно-технических (ИТВ) и информационно-психологических воздействий (ИПВ), что отличает данную работу от других работ по тематике аудита ИБ.

Ввиду объемности материала, статья была декомпозирована на следующие подразделы.

1. Определение аудита информационной безопасности.
2. Цели и задачи аудита.
3. Этапы проведения аудита.
4. Концептуальные основы аудита.
5. Классификация мероприятий аудита.
6. Тестирование как один из основных типов аудита.
   6.1. Тестирование на основе моделей.
   6.2. Тестирование специальными средствами и способами.

1. Определение аудита информационной безопасности

В настоящее время нет сложившегося определения аудита применяемого для анализа уровня ИБ. В различных источниках можно встретить различные определения. Приведем некоторые из них.

Аудит – форма независимого, нейтрального контроля какого-либо направления деятельности организации [1].

Аудит – совокупность специальных приемов (методов), используемых для обработки исходной информации для достижения поставленных целей.

Многообразные приемы аудита проверок обычно объединяют в четыре группы: определение реального состояния объектов, анализ, оценка, формирование технических предложений [2].

Аудит – систематический, независимый и документированный процесс получения записей, фиксирования фактов или другой соответствующей информации и их объективного оценивания с целью установления степени выполнения заданных требований [3].

Аудит информационных систем – проверка используемых компанией информационных систем, систем безопасности, систем связи с внешней средой, корпоративной сети на предмет их соответствия бизнес-процессам, протекающим в компании, а также соответствия международным стандартам, с последующей оценкой рисков сбоев в их функционировании [4].

Аудит информационной безопасности – мероприятия по оценке состояния информационной безопасности информационной автоматизированной системы и разработки рекомендаций по применению комплекса организационных мер и программно-технических средств, направленных на обеспечение защиты информационных ресурсов информационной системы от угроз ИБ [1].

Аудит информационной безопасности – системный процесс получения объективных качественных и количественных оценок о текущем состоянии ИБ компании в соответствии с определенными критериями и показателями безопасности [4].

Аудит информационной безопасности – комплекс организационно-технических мероприятий, проводимых независимыми экспертами, имеющих целью оценку состояния ИБ объекта аудита и степени его соответствия критериям аудита [5].

На взгляд автора, является наиболее общим и в максимальной степени отражающим процесс проведения аудита, а также гармонизирующем ISO 19011 – 2011, является следующее.

Аудит информационной безопасности – систематический, независимый и документируемый процесс получения оценок состояния ИБ объекта аудита и объективного их оценивания с целью установления степени соответствия критериям аудита.

2. Цели и задачи аудита

Анализируя вышеуказанные определения можно сделать вывод, об общей и частных задачах аудита.

Общей задачей аудита является проверка и оценивание ИС на соответствие критериям, которые определяют требования к уровню ИБ.

Частными задачами аудита является [1, 5]:

- анализ рисков, связанных с возможностью реализации угроз безопасности;
- оценка текущего уровня защищенности;
- выявление уязвимостей в подсистеме защиты и «узких мест» системы;
- оценка соответствия системы и ее защиты существующим стандартам в области ИБ, а также политике безопасности;

- формирование рекомендаций по комплексу мер, направленных на повышение эффективности существующей системы защиты.

Цели аудита можно подразделить на [5]:

- *превентивные* – направленные на превентивное выявление угроз и уязвимостей и предотвращение инцидентов ИБ;
- *детектирующие* – направленные на обнаружение новых или уточнение особенностей уже имеющихся угроз и уязвимостей системы защиты во время 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.

В настоящее время аудит ИБ проводят по отношению к следующим объектам [3]:

- организации;
- бизнес-процессы;
- системы управления (менеджмента);
- информационные системы;
- технические системы.

По форме аудит может быть [3]:

- организационно-нормативным – когда анализируется организационные мероприятия обеспечения ИБ и нормативные акты в данной сфере;
- техническим – когда анализируется технические средства и способы обеспечения ИБ.

Аудит является наиболее общей формой оценки состояния ИБ объекта аудита. Аудит проводиться на соответствие любым требованиям, сформулированным как заинтересованными лицами, так и нормативными документами. Аудит может включать в себя проведение различных способов тестирования подсистем и процессов объекта аудита, анализ документации и других информационных источников, интервьюирование специалистов и т. д.

3. Этапы проведения аудита

При проведении аудита ИБ обычно проводится следующая последовательность мероприятий [1, 2]:

1 этап – подготовительный:

- выбор объекта аудита;
- выбор критериев и методов аудита;
- выбор средств и способов аудита;
- формирование команды аудиторов;
- определение объема и масштаба аудита, установление его сроков.

2 этап – основной:

- анализ состояния ИБ объекта аудита;
- регистрация, сбор и проверка статистических данных и результатов инструментальных измерений уязвимостей и угроз;
- оценка результатов проверки;

- формирование отчета о результатах проверки по отдельным элементам объекта аудита и различным аспектам ИБ.

3 этап – заключительный:

- составление итогового отчета;
- формирование рекомендаций по комплексу мер, направленных на повышение эффективности существующей системы защиты;
- разработка плана мероприятий по устранению уязвимостей и недостатков в обеспечении ИБ.

Последовательность проведения аудита, особенно при использовании подхода, основанного на анализе стандартов ИБ и оценке соответствия, достаточно подробно описана в известной литературе [1, 3, 6], поэтому в данной статье подробно не рассматривается.

4. Концептуальные основы аудита

Проведение аудита предусматривает следование определенной формальной процедуре проверки объекта аудита. Данная процедура проводится в соответствии с предварительно сформированными формальными описаниями объекта и процесса аудита, а также актуальных угроз [1, 5]:

- моделью аудита;
- моделью нарушителя/противника;
- моделью угроз;
- общим практическим подходом к проведению аудита;
- общим теоретическим подходом к проведению аудита.

При проведении такой формализации обязательно прописываются следующие аспекты исследования [2]:

- источники угроз;
- защищаемые подсистемы, ресурсы, процессы или другие элементы системы;
- связи между источниками угроз и защищаемыми элементы системы;
- структура и процессы функционирования подсистемы защиты.

Общая схема взаимодействия вышеуказанных объектов при проведении аудита представлена на рис. 1.

Модель аудита включает в себя формализованное описание [1]:

- объекта аудита;
- цели аудита;
- предъявляемых требований;
- используемых практических и теоретических подходов;
- масштаба и глубины;
- исполнителей;
- порядка проведения аудита.

Модель нарушителя/противника включает в себя формализованное описание [5]:

- формализованное понятие нарушителя/противника;
- критерии нарушения ИБ;
- категорирование нарушителей/противников;

- предположения о квалификации, возможностях, располагаемых средствах и способах информационного воздействия для каждой категории нарушителей/противников;
- предположения о сценариях действий каждой категории нарушителей/противников;
- уровень полномочий и способы получения доступа к системе для каждой категории нарушителей/противников.

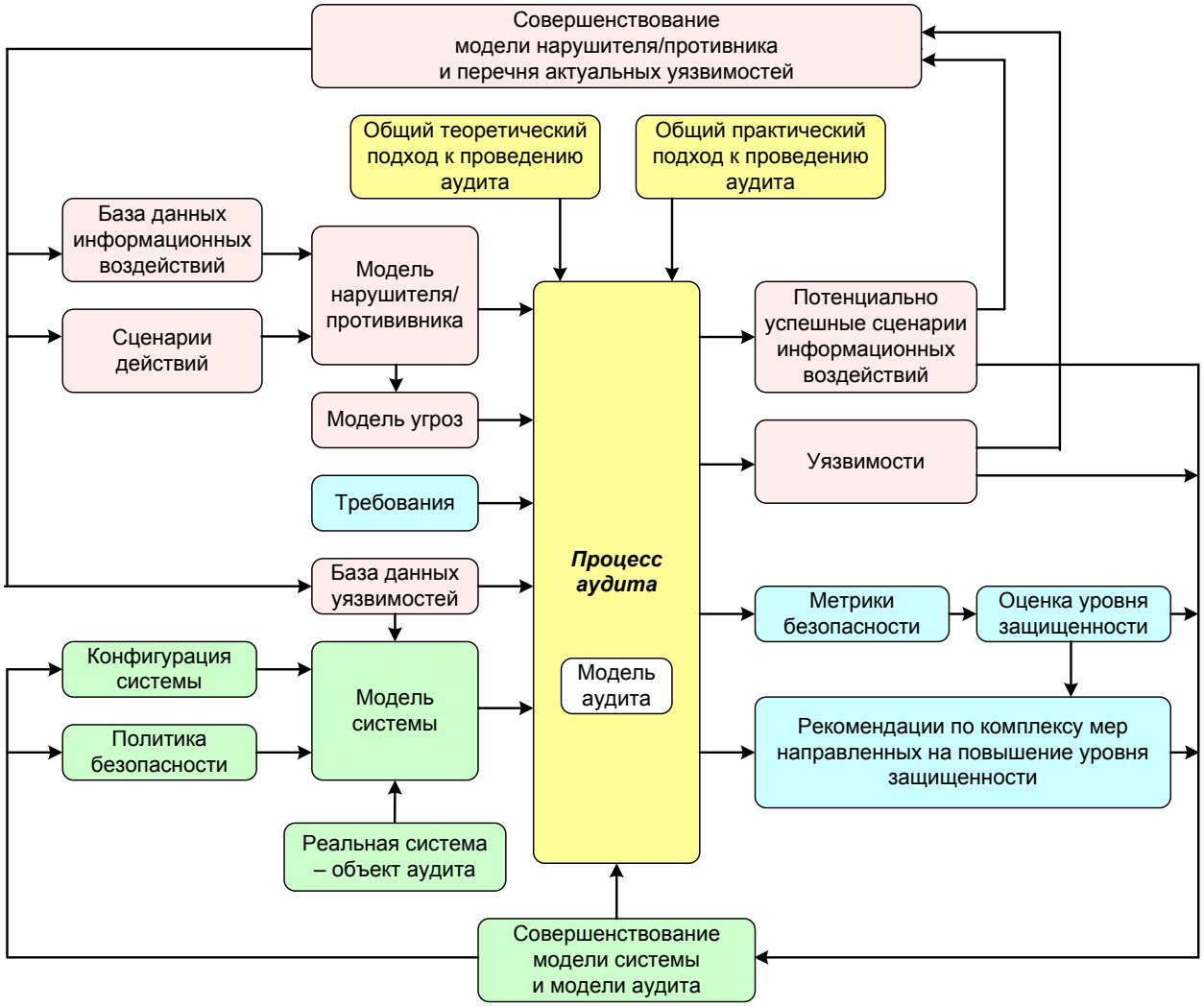

Рис. 1. Схема процесса аудита [7]

Модель угроз включает в себя формализованное описание [5]:

- категорий угроз:
  - угрозы доступности;
  - угрозы целостности;
  - угрозы конфиденциальности;
- групп угроз:
  - угрозы, реализуемые путем использования технических каналов утечки информации;
  - угрозы, реализуемые с использованием средств и способов информационно-технических воздействий (ИТВ) [9];

- угрозы, реализуемые с использованием средств и способов информационно-психологических воздействий (ИПВ) или социальной инженерии [9].

Общими практическими подходами к проведению аудита являются следующие [5]:

- аудит на основе анализа рисков;
- аудит на основе анализа стандартов ИБ;
- аудит на основе комбинирования анализа рисков и анализа стандартов ИБ;
- аудит на основе экспериментальных исследований системы или ее прототипа.

Аудит на основе анализа рисков проводится с использованием формальных методов анализа рисков, когда аудитор определяет для обследуемой системы индивидуальный набор требований ИБ, в наибольшей степени учитывающий особенности данной системы, среды ее функционирования и существующие в данной среде угрозы безопасности. Данный подход является наиболее трудоемким и требует высокой теоретической квалификации аудитора. На качество результатов аудита, в этом случае, сильно влияет используемая методология анализа и управления рисками, а также ее применимость к конкретному типу исследуемой системы.

Анализ риска – систематическое использование информации для идентификации источников угроз и оценки величины риска. Методы анализа риска могут быть качественными, полуколичественными и количественными. Необходимо отметить, что полный количественный анализ систем не всегда возможен вследствие сложности систем ИБ, затрудненности получения адекватной статистики инцидентов и др. Анализ риска включает этапы инвентаризации и категорирования ресурсов, идентификации значимых угроз и уязвимостей, а также оценку вероятностей реализации угроз и уязвимостей [3].

В настоящее время сложилась нормативная база анализа риска в области ИБ в виде ГОСТ Р ИСО/МЭК 27005 – 2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности», который определяет процессный подход к управлению рисками, включающий в том числе оценку и обработку риска. Более подробная информация об аудите на основе анализа рисков представлена в работах [2, 3, 11].

Аудит на основе анализа стандартов информационной безопасности является самым практичным. Стандарты ИБ определяют базовый набор требований безопасности для широкого класса систем, который формируется в результате обобщения мировой практики. Стандарты ИБ могут определять разные наборы требований безопасности, в зависимости от уровня защищенности исследуемой системы, который требуется обеспечить, ее принадлежности (коммерческая организация, либо государственное учреждение), а также назначения (финансы, промышленности, связь и т. п.). От аудитора в данном случае требуется правильно определить набор требований стандарта, соответствие которым требуется обеспечить для конкретной исследуемой системы. Более подробная

информация об аудите на основе анализа стандартов ИБ представлена в работах [1, 3, 6].

Комбинирование, как анализа рисков, так и стандартов информационной безопасности является наиболее эффективным подходом к проведению аудита. Базовый набор требований безопасности, предъявляемых к исследуемым системам, определяется стандартами. Дополнительные требования, в максимальной степени учитывающие особенности функционирования конкретной системы, формируются на основе анализа рисков. Этот подход проще аудита на основе анализа рисков, т. к. большая часть требований ИБ уже определена стандартами, и, в то же время, он лишен недостатка второго подхода, заключающего в том, что требования стандарта могут не учитывать специфики конкретных систем.

В большинстве фундаментальных работ по аудиту [1-3, 6-7], представлены только эти три подхода. Вместе с тем отдельно выделяют, так называемый, «тест на проникновение» [8]. От вышеуказанных подходов, его отличает то, что это разновидность именно экспериментального исследования объекта, проводимое с целью выявления слабых мест в защите или новых уязвимостей, как правило, по итогам внедрения новых мер защиты. На взгляд автора «тест на проникновение» является не более чем, частной разновидностью еще одного общего подхода к аудиту – аудит на основе экспериментальных исследований системы или ее прототипа.

Аудит на основе экспериментальных исследований системы или ее прототипа, проводится с применением против системы средств или способов ИТВ или ИПВ с целью практической проверки эффективности технических или организационных мер защиты, а также выявления новых уязвимостей системы. Данный подход по степени направленности на техническую или организационно-психологическую сферу можно подразделить на:

- *аудит технических подсистем* – проводится с целью практически оценить устойчивость технических средств и способов защиты (как аппаратных, так и программных), при применении против них целенаправленных ИТВ, а также уровень ИБ, обеспечиваемый в таких условиях;
- *аудит организационных подсистем* – проводится с целью практически оценить устойчивость организационных мер, регламентов обеспечения ИБ организации и поведения ее персонала, при применении против организации или ее персонала целенаправленных ИПВ, а также уровень ИБ, обеспечиваемый в таких условиях;
- *комплексный аудит* – проводится с целью практического оценивания уровня ИБ, обеспечиваемый в условиях целенаправленного применения как ИТВ, так и ИПВ. Именно к этому виду аудита, по мнению автора, относится «тестирование на проникновение»

В некоторых работах, например, таких как [3, 4, 8], для данного подхода используют термины «активный аудит» или «инструментальный аудит». Однако, на взгляд автора, эти понятия являются некорректными. Инструментальный аудит терминологически соответствует исследованию системы с помощью лю-

бых «инструментальных» средств, под которыми в известной литературе понимаются преимущественно технические средства (аппаратные или программные), но не способы целенаправленного ИТВ или ИПВ. Термин «активный аудит» в большей степени соответствует высокой степени воздействия на объект исследования, с целью вызвать в нем требуемые изменения. При этом под данный термин не попадают ИТВ и ИПВ, проводимые с разведывательными целями [9, 10].

Рассмотрим основные теоретические подходы, которые лежат в основе методологии аудита.

В зависимости от используемой формы формализации процесса анализа выделяют следующие теоретические подходы к аудиту [11, 12]:

- процессный подход:
  - на основе методологии IDEF0;
  - на основе методологии IDEF1;
  - на основе методологии IDEF2;
  - на основе методологии IDEF3;
  - на основе методологии IDEF4;
- основанные на модели оценки;
- основанные на модели зрелости:
  - на основе стандарта ISO/IEC 15504 «Информационная технология. Оценка процесса»;
  - на основе стандарта ISO/IEC 21827 «Инжиниринг безопасности систем — модель зрелости возможностей»;
  - на основе стандарта COBIT (Control Objectives for Information and related Technology);
  - на основе стандарта URSIT (Uniform Interagency Rating System for Information Technology).

Рассмотрим эти теоретические подходы к аудиту более подробно.

Процессный подход рассматривает деятельность по обеспечению ИБ, как вспомогательный процесс в функционировании организации и ее бизнес-процессов [11]. Это обусловлено тем, что система обеспечения ИБ, включая соответствующие процессы, напрямую не участвуют в целевых процессах организации (например, в выпуске конкретной продукции), а наоборот, даже повышают стоимость продукции, по своей сути являясь затратными для организации. Вместе с тем, затраты на обеспечение ИБ способствуют снижению потенциальных потерь, участвуя таким образом в основных бизнес-процессах организации. На основе процессного подхода деятельность организации представляется в виде совокупности и иерархии целевых и вспомогательных процессов трех групп [11]:

- процессы управления (процессы менеджмента организации);
- основные процессы (процессы целевой деятельности организации);
- вспомогательные процессы (процессы, связанные с ресурсами организации).

Данные процессы формализуется на основе методологии IDEF (Integrated DEFinition) – представление любой изучаемой системы в виде набора взаимо-

действующих и взаимосвязанных блоков, отображающих процессы, операции, действия, происходящие в изучаемой системе. При этом в методологии IDEF различают три уровня подробности представления процессов [11, 12]:

- IDEF0 – формализует процессы с учетом их функций, иерархии и логических отношений между ними;
- IDEF1 – формализует информационные процессы с учетом их структуры и взаимосвязи;
- IDEF2 – формализует процессы так же как IDEF0, при этом дополнительно учитывает динамику протекания процессов во времени;
- IDEF3 – формализует процессы так же как IDEF0, при этом каждый процесс дополнительно может быть декомпозирован на отдельные функциональные блоки, что требуется для более подробного описания технологических операций;
- IDEF4 – формализует процессы на основе объектно-ориентированного подхода, в дальнейшем данный теоретический подход был положен в основу прикладной концепции SOA (Service-Oriented Architectures).

Теоретический *подход, основанный на модели оценки* задает перечень и эталонную модель оцениваемых процессов объекта аудита, определяет критерии аудита и ключевые показатели, а также способ оценивания процессов с помощью этих показателей и способ отображения результатов оценивания. Основу модели оценки составляют перечень и модель оцениваемых процессов и совокупность показателей, которые используются для сбора данных и определения степени достижения установленных критериев обеспечения ИБ [11]. К этому теоретическому подходу относится подавляющее большинство прикладных подходов к аудиту, которые ориентированы на оценку показателей ИБ и проверку их на соответствие заранее определенным критериям.

Теоретический *подход, основанный на модели зрелости* (Capability Maturity Model – CMM) был разработан в программной индустрии для оценки зрелости процессов разработки программных продуктов и определения ключевых действий, необходимых для дальнейшего их развития. Исходная модель CMM стала стандартом де-факто для оценки и совершенствования процессов создания программного обеспечения. Базовая методология CMM определяет критерии и выделяет 5 уровней зрелости процессов от первого — «начального», характеризующегося тем, что некая целенаправленная деятельность осуществляется, но не контролируется, не формализуется и т. д., до пятого — «непрерывно совершенствующегося», характеризующегося тем, что деятельность в рамках процессов не только основывается на лучших стандартах, но и непрерывно улучшается и оптимизируется.

Позже теоретический подход, основанный на модели зрелости с определенными изменениями был положен в основу международных стандартов информационных технологий и ИБ, таких, как ISO/IEC 15504 «Информационная технология. Оценка процесса», ISO/IEC 21827 «Инжиниринг безопасности систем – модель зрелости возможностей», так и иных отраслевых или профильных стандартов, таких, как COBIT (Control Objectives for Information and related

Technology) и URSIT (Uniform Interagency Rating System for Information Technology) [11].

В зависимости от степени доступности информации об объекте аудита выделяют следующие теоретические подходы [15]:

- подход на основе «белого ящика»;
- подход на основе «серого ящика»;
- подход на основе «черного ящика».

При аудите на основе «белого ящика» аудитор имеет доступ к полной информации о структуре и функционировании исследуемой системы. Например, для организационной системы это может быть информация о полномочиях, о формальных и неформальных социальных связях; о формальных регламентах и принятых (неформальных) нормах поведения. Для технических систем, это может быть полный доступ к структурным, функциональным и принципиальным схемам аппаратных средств, а также доступ к исходному коду и сопроводительной документации программного обеспечения.

При аудите на основе «серого ящика» о параметрах исследуемой системы частично известно, но информация обо всех принципах ее функционирования и структуры являются скрытыми от аудитора. Может быть известно: о входных и выходных данных, о самых общих принципах функционирования системы и ее предполагаемая структура. Например, для организационной системы это может быть информация только о нормах руководящих документов, о формальных полномочиях и обязанностях должностных лиц, без указания психологических особенностей конкретных персоналий и принятых норм поведения в коллективе. Для технических систем, это может быть доступ к входным и выходным данным объекта аудита, а также некоторые предположения об основных принципах функционирования и структуры его аппаратных средств и программного обеспечения.

При аудите на основе «черного ящика» информация о параметрах, структуре и принципах функционирования исследуемой системы является изначально недоступной для аудитора.

5. Классификация мероприятий аудита

Общая классификация мероприятий аудита ИБ, с учетом вышепредставленной декомпозиции некоторых из этих мероприятий, приведена на рис. 2.

Основаниями, по которым могут быть классифицированы мероприятия аудита ИБ объекта могут быть следующими:

1) по цели;
2) по объекту аудита;
3) по форме;
4) по практическому подходу к проведению аудита;
5) по теоретическому подходу к проведению аудита;
6) по степени воздействия на объект аудита;
7) по степени легальности;
8) по местонахождению аудитора по отношению к исследуемой системе;
9) по типу.

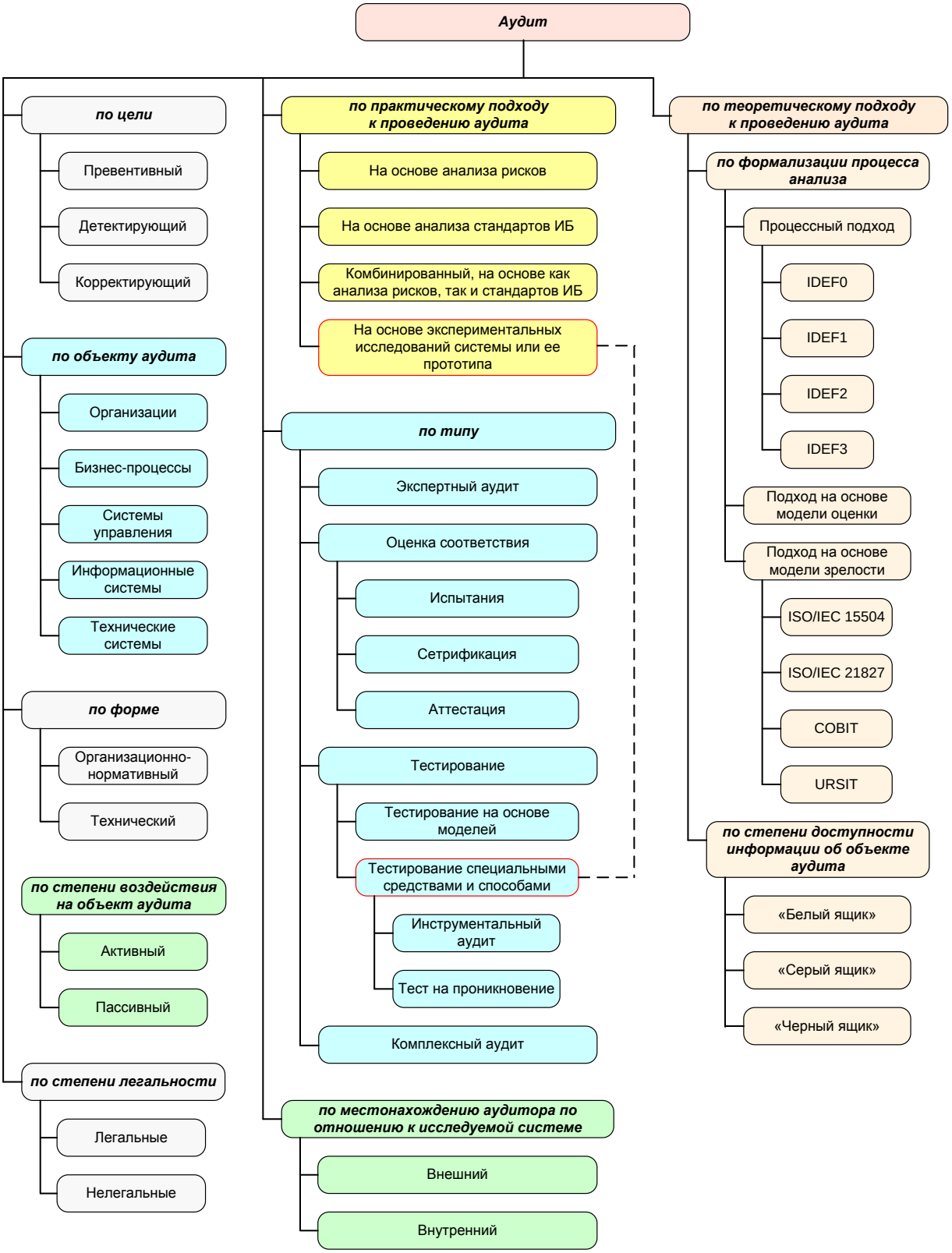

Рис. 2. Классификация мероприятий аудита

Классификация мероприятий по основаниям 1-5 была рассмотрена выше, далее будут рассмотрены мероприятия аудита, классифицированные по основаниям 6-9.

По степени воздействия на объект аудита, мероприятия могут быть классифицированы на:

- пассивные;
- активные.

Пассивный аудит, это проведение мероприятий, которые не вносят изменений в реальный объект аудита и не переводят его в другое состояние. К пассивному аудиту относятся любые типы аудита, проводимые на основе анализа стандартов ИБ, а также на основе формальных моделей анализа рисков. Если при аудите проводится тестирование на основе моделей, то такой тип аудита тоже относится к пассивному. К пассивному аудиту также можно отнести мероприятия, связанные с применением специальных средств и способов ИТВ или ИПВ разведывательного характера, ориентированных на сбор сведений об объекте аудита или его средств защиты.

Активный аудит, предусматривает проведение мероприятий, которые связанны с целенаправленным воздействием на исследуемую систему, с целью провести анализ ее реакций или перевести ее в требуемое состояние, как правило, с более низким уровнем защищенности. К активному аудиту можно отнести проведение тестирования системы целенаправленными ИТВ и ИПВ, формирование некорректных или ложных исходных данных, формирование неблагоприятной среды функционирования системы, внесение изменений в ее структуру или встраивание в нее дополнительных функциональных элементов.

В некоторых работах, например, таких как [3, 4, 13, 14], под активным аудитом понимается любое использование средств и способов сбора информации о состоянии подсистемы сетевой защиты, имитирующих действия злоумышленника/противника. Кроме того, в ряде случаев для такого активного аудита используют понятие «инструментальный аудит». Однако, на взгляд автора, такой терминологический подход неверен. К активному аудиту можно отнести не все мероприятия мониторинга сетевой защиты, а только те, которые используют или моделируют реальные воздействия на исследуемую систему.

По степени легальности мероприятия аудита могут быть классифицированы на [1, 8]:

- легальные;
- нелегальные.

Легальный мероприятия отличаются правовой безопасностью и как правило, проводятся на основании договора аудитора с заказчиком имеющим прямое отношение к обеспечению безопасности объекта аудита, с целью выработки мер направленных на повышение уровня его защиты.

Нелегальные мероприятия аудита связанны с получением информации об уязвимости исследуемой системы нелегальными способами. К таким нелегальным способам можно отнести: воровство, преднамеренный обман, несанкционированное прослушивание, подделку идентифицирующих документов, а также использование различных действий, которые содержат признаки противоправных деяний. Также к нелегальным мероприятиям можно отнести аудит проводимый при участии или заказу третьих лиц, с целью последующего ис-

пользования результатов аудита для нанесения ущерба исследуемой системе или организации.

По местонахождению аудитора по отношению к исследуемой системы мероприятия аудита могут быть классифицированы на [1, 5]:

- внешний;
- внутренний.

Внешний аудит – проводится внешними независимыми экспертами или с использованием технических средств и способов тестирования, находящихся вне исследуемой системы. Как отмечается в работах [1, 5], как правило, внешний аудит – это разовое мероприятие, проводимое по инициативе руководства организации.

Внутренний аудит – непрерывная деятельность, которая осуществляется подразделениями службы безопасности организации в соответствии с регламентирующими документами организации с использованием технических средств защиты информации и с привлечением экспертов организации.

По типу, мероприятия аудита могут быть классифицированы на [1-3]:

- экспертный аудит;
- оценка соответствия:
    - испытания;
    - аттестация;
    - сертификация;
- тестирование:
    - тестирование на основе моделей;
    - тестирование специальными средствами и способами (в т. ч. инструментальный аудит и тестирование на проникновение);
- комплексный аудит.

Экспертный аудит предполагает процесс выявления недостатков в системе мер защиты информации на основе имеющегося опыта экспертов, участвующих в процедуре аудита. При экспертном аудите, состояние ИБ системы сравнивается с некоторым «идеальным» описанием, которое базируется на:

- требованиях, которые были предъявлены руководством в процессе проведения аудита;
- описании «идеальной» системы безопасности.

В рамках экспертного аудита, как правило, производится анализ организационно-распорядительных документов, таких как политика безопасности, план защиты различного рода инструкции, проекты внедрения и совершенствования системы защиты. Эти документы оцениваются на предмет достаточности и непротиворечивости, декларируемым целям и мерам ИБ. В ходе такого анализа выявляются недостатки и уязвимости существующей системы защиты, а также предлагается комплекс мер направленных на повышение уровня безопасности. Необходимо отметить, что при экспертном аудите учитываются результаты предыдущих обследований (в том числе других аудиторов), выполняются обработка и анализ проектных решений и других рабочих материалов, касающихся вопросов создания информационной системы. Подробная информация об экспертном аудите представлена в работах [1, 6].

Оценка соответствия – доказательство того, что заданные требования к продукции, процессу, системе, лицу или органу выполнены. Допускается, что доказательство может быть прямым или косвенным, формальным или неформальным. Выдачу документально оформленного заявления (удостоверения) о соответствии заданным требованиям называют подтверждением соответствия. Примерами таких удостоверений могут быть сертификаты, аттестаты, заключения, выданные официальными органами по оценке соответствия. Наличие такого документального подтверждения отличает оценку соответствия от других типов аудита, которые могут не иметь документального подтверждения в виде документа государственного образца. При этом критерии аудита могут быть более гибкие, а способы и средства его проведения – более разнообразными. Мероприятия по оценке соответствия могут быть декомпозированы на следующие мероприятия: испытания, аттестацию, сертификацию [3].

Более подробная информация об оценки соответствия представлена в работе [3].

Испытание – экспериментальное определение количественных или качественных характеристик объекта испытаний как результата воздействия на него при его функционировании, моделировании или воздействий. Испытания проводятся на основании документа «программа и методика испытаний», а результаты испытания оформляются в виде протоколов испытаний или технического отчёта [3].

Аттестация – комплексная проверку защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню ИБ. Положительный результат аттестации оформляется в виде аттестата соответствия [3].

Сертификация – испытания технических средств защиты информации, которые проводятся независимыми испытательными лабораториями, с целью подтверждения соответствия объекта сертификации требованиям нормативных документов по защите информации [3].

Тестирование – это техническая операция, заключающаяся в определении одной или нескольких характеристик продукта, процесса или услуги соответствующей процедуре [3]. Таким образом, тестирование применительно к аудиту ИБ информационных систем – это определение одной или нескольких параметров системы характеризующих определенную категорию ИБ (например, целостность, доступность, конфиденциальность). Тестирование может проводиться с целью анализа рисков и уязвимостей. Комплекс тестов информационной системы может быть оформлен в виде программы испытания с составлением соответствующего протокола, по итогам их завершения.

В общем случае, все виды тестирования, в зависимости от использования теоретического или практического подхода к аудиту, могут быть классифицированы на:

- *тестирование на основе моделей* – теоретический подход к аудиту, когда строятся соответствующие модели и аудит проводится на основе исследования данных моделей;

- *тестирование специальными средствами и способами* – практический подход к аудиту, когда аудит проводится на основе экспериментов по воздействию средств и способов ИТВ и ИПВ на объект аудита, или его прототип.

В известной литературе по аудиту, как правило, широко рассматриваются еще два вида тестирования – инструментальный аудит и тестирование на проникновение. Однако, на взгляд автора, эти типы тестирования являются разновидностью тестирования специальными средствами и способами. Это обусловлено тем, что при инструментальном аудите используются технические средства анализа и ИТВ, при этом в данное понятие не включается средства и способы ИПВ, а также способы социальной инженерии. А понятие «тестирование на проникновение» слабо формализуемое мероприятие по комплексному применению средств и способов ИТВ и ИПВ, суть и содержание которого меняется в зависимости от требований заказчика аудита и квалификации выполняющего его эксперта.

В настоящее время в теории аудита ИБ сложилась ситуация, при которой большинство работ в этой области ориентированно на исследование экспертного аудита [1, 2, 16, 11] и оценки соответствия [3, 11], преимущественно на основе моделей анализа рисков, либо на основе анализа стандартов ИБ. При этом, тестирование, и в особенности, тестирование специальными средствами и способами, является недостаточно изученной теоретической областью аудита. Имеются отдельные работы, например [8], которые посвящены такому типу тестирования «как тест на проникновение», однако данные работы носят в большей степени практический, чем теоретический характер. При этом тестирование, 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 тестирования, а также быть более избирательном в направлении достижения цели аудита. Например, проводить тестовое исследование систем к угрозам и выявлять уязвимости, еще не описанные в базах угроз и уязвимостей. Всё это актуализирует подробное рассмотрение тестирования как отдельную важную и передовую (относительно уже действующих стандартов) область аудита информационной безопасности.

Комплексный аудит – включает в себя использование нескольких вышеперечисленные типов проведения аудита.

6. Тестирование как один из основных типов аудита

Как было показано выше, 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 [22].

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

Технология построения тестов должна, прежде всего, обеспечивать решение следующих двух задач [22]:

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.

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;
4) по местонахождению относительно объекта тестирования;
5) по степени изменения параметров тестирования;
6) по методологии тестирования;
7) по степени априорного знания об объекте тестирования;
8) по объекту тестирования;
9) по уровню структуры объекта, на которое направленно тестирование;
10) по свойству объекта, на исследование которого направленно тестирование;
11) по общему подходу к проведению тестирования.

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 во время 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 [13-15]:

- пассивное;
- активное.

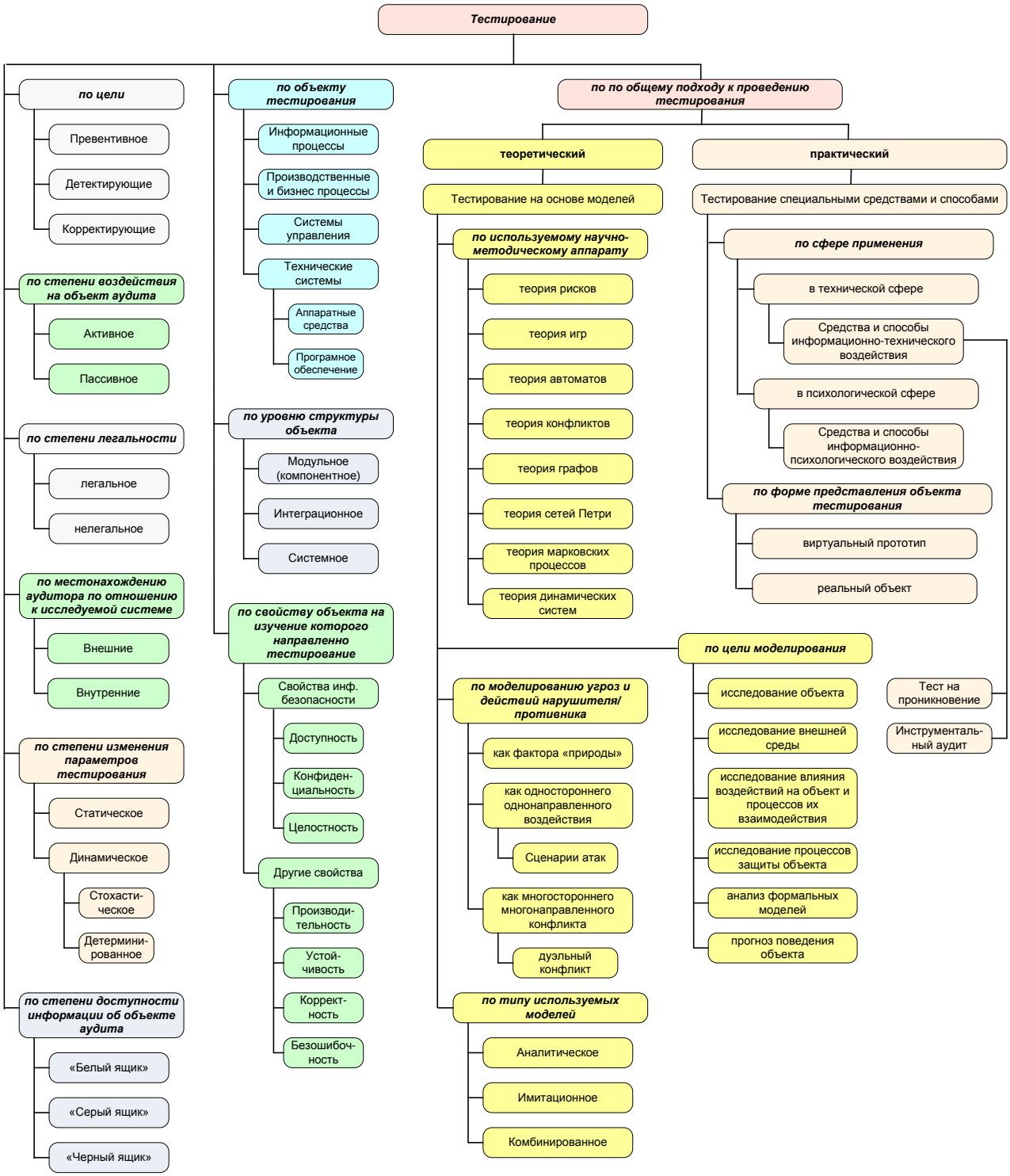

Рис. 3. Классификация мероприятий, способов и средств тестирования

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.

По степени изменения параметров тестирования различают:

- *статическое тестирование* – тестирование объекта на конкретном наборе входных данных и параметров, либо экспертный анализ схем аппаратной части и кода программной части технических средств, а также экспертный анализ политики безопасности организации;
- *динамическое тестирование* – тестирование объекта на динамически изменяющихся наборах входных данных, условиях функционирования, структуре, и т. д. При этом по принципу изменения параметров тестирования можно выделить:

- *стохастическое тестирование* – параметры тестирования изменяются по вероятностным законам;
- *детерминированное тестирование* – параметры тестирования изменяются по детерминированным законам.

По степени априорного знания об объекте тестирования различают [15]:

- тестирование по принципу «белого ящика»;
- тестирование по принципу «серого ящика»;
- тестирование по принципу «черного ящика».

При тестировании по принципу «белого ящика» имеется полная информация о структуре и функционировании тестируемого объекта. При тестировании по принципу «серого ящика» о параметрах тестируемого объекта частично известно, но информация обо всех принципах его функционирования и структуре являются скрытыми. Может быть известно: о входных и выходных данных, о самых общих принципах функционирования объекта и ее предполагаемая структура. При тестировании по принципу «черного ящика» информация о параметрах, структуре и принципах функционирования тестируемого объекта является изначально недоступной [15].

Зачастую, при использовании принципа «белого ящика» используют статическое тестирование, основанное на анализе полной информации о структуре и функционировании объекта. При использовании принципа «черного ящика» используют динамическое, или как его еще называют, функциональное тестирование, основанное на анализе поведения объекта в условиях динамических тестов с широким диапазоном изменяемых параметров [15].

В качестве объекта тестирования могут рассматриваться:

- информационные процессы;
- производственные и бизнес процессы;
- системы управления;
- технические системы, а также их подсистемы:
  - аппаратные средства;
  - программное обеспечение.

По уровню структуры объекта, выделяют:

- *модульное (компонентное) тестирование*, которое позволяет проверить функционирование отдельно взятого элемента объекта, например, программного или аппаратного модуля, подпрограммы, отработки должностных обязанностей по защите информации отдельным должностным лицом и т. д.;
- *интеграционное тестирование* путем проверки взаимодействия между элементами объекта (например, путем реализации методов тестирования «сверху вниз», «снизу вверх», распределения потоков управления и данных и т. д.);
- *системное тестирование*, которое охватывает целиком весь объект и его внешние интерфейсы, а также среду функционирования.

По свойству объекта, на изучение которого направленно тестирование различают:

- тестирование доступности;
- тестирование конфиденциальности;
- тестирование целостности;
- тестирование устойчивости;
- тестирование производительности;
- тестирование корректности;
- тестирование безошибочности;
- нагрузочное тестирование;
- интегральное тестирование (одновременно тестируется несколько свойств объекта) и т. д.

В самом общем случае, можно выделить два подхода к проведению тестирования:

- *теоретический*;
- *практический.*

Этим двум подходам соответствует следующие варианты тестирования:

- *тестирование на основе моделей* – теоретический подход к аудиту, когда строятся соответствующие модели и аудит проводится на основе исследования данных моделей;
- *тестирование специальными средствами и способами* – практический подход к аудиту, когда аудит проводится на основе экспериментов по воздействию средств и способов ИТВ и ИПВ на объект аудита, или его прототип.

6.1 Тестирование на основе моделей

Рассмотрим тестирование на основе моделей (MBT – Model Based Testing) более подробно на основании анализа работ [7, 14, 15, 17-19].

Данный вид тестирования является одной из наиболее интенсивно развивающихся областей программной инженерии. Одна из причин такого активного развития – тот факт, что тестирование на основе моделей находится на пересечении нескольких теоретических областей. Эти области включающие, в себя теоретические подходы к формализации и моделированию требований, методы анализа формальных моделей, методы статического и динамического анализа систем, методы управления уровнем абстракции и трансформации моделей. Такая высокая абстрактность данного подхода к тестированию дает возможность данному подходу быстро совершенствоваться за счет использования последних достижений в различных теоретических областях.

Подразумевается, что тестирование на основе моделей использует различные модели для построения тестов. Однако, у подобного утверждения очень много различных толкований т. к. большинство исследователей, использующих этот подход на практике, подразумевают под этим термином различные специфические теоретические подходы к исследованию объекта тестирования.

Целями тестирования могут быть:
- исследование объекта;
- исследование внешней среды объекта;
- исследование влияния воздействий на объект и процессов их взаимодействия;
- исследование процессов защиты объекта;
- анализ формальных моделей;
- прогноз поведения объекта.

Моделирование угроз и действий нарушителя/противника могут быть представлено в виде:
- фактора природы (в виде отдельных детерминированных или стохастических факторов в составе модели);
- как одностороннего однонаправленного воздействия (в этом случае нарушитель/противник представляется в виде активного дестабилизирующего воздействия на объект, который в свою очередь реализует различные сценарии защиты [7]);
- как многостороннего многонаправленного конфликта (в этом случае рассматривается конфликт нескольких объектов, каждый из которых реализует собственные стратегии нападения и защиты, которые могут быть не только различными по отношению к другим сторонам конфликта, но и реализовываться через дополнительные стратегии кооперации и нейтралитета [20, 21]).

Наиболее распространенными частными случаями моделирования вариантов угроз является моделирование сценария атак как частного случая одностороннего однонаправленного воздействия, а также моделирование дуэли как частного случая многостороннего многонаправленного конфликта с двумя сторонами, реализующими нападение на противоположную сторону и собственную защиту.

Для формализации и моделирования процессов защиты могут быть использован различный научно-методический аппарат. Так для моделирования сценария атак может быть использовано его представления на основе: графов атак, формальных грамматик, сетей Петри, марковских процессов, методов дискретно-событийного моделирование и т. д. [7]. В свою очередь дуэльный конфликт может быть формализован на основе: теории игр, теории марковских процессов, теории конфликтов, теории сетей Петри и т. д. [21]. Таким образом, еще одним основанием по которому может быть классифицировано тестирование на основе моделей является используемый научно-методический аппарат.

По используемому научно-методическому аппарату тестирование на основе моделей, может быть классифицировано:
- на основе теории рисков;
- на основе теории игр;
- на основе теории автоматов;
- на основе теории конфликтов;
- на основе теории графов;
- на основе теории сетей Петри;

- на основе теории марковских процессов;
- на основе теории динамических систем.

В зависимости от общего подхода к моделированию можно выделить следующие типы тестирования:

- на основе аналитических моделей;
- на основе имитационных моделей;
- на основе комбинированных моделей.

6.2 Тестирование специальными средствами и способами

В настоящее время сложился подход к аудиту, когда подавляющая часть процессов оценивания безопасности системы основывается на анализе соответствия формальным требованиям, а также путем тестирования на основе моделей.

Вместе с тем наблюдается тенденция наращивания 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. Дальнейшее развитие данного подхода к тестированию привело к разработке, так называемых, киберполигонов, которые виртуализируют как аппаратное, так и программное обеспечение распределенной технической системы и позволяют отработать защиту от известных угроз и воздействий различных ИТВ. Сейчас это направление активно развивается и ему посвящены работы [23-25].

Вместе с тем реальные информационные системы не ограничиваются исключительно техническими средствами. Организационные процессы обеспечения ИБ, а также большие технические комплексы не могут быть протестированы на подобных киберполигонах в виду объективных ограничений на возможности виртуализации. В этом случае используется тестирование реального объекта.

В настоящее время к наиболее распространенному комплексному тесту защищенности реальной информационной системы относится «тест на проникновение». Этому способу тестирования посвящены работы [8, 26-28]. Однако, в данных работах не содержатся научно-обоснованные методики проведения тестирования (подобные тем, которые задаются для испытаний при оценке соответствия). Более того, исследователи этого типа тестирования отмечают, что выбор конкретных способов и средств тестирования остается за экспертом, 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 характерно еще и субъективность как в отношении ожидаемых результатов со стороны заказчика, так и в отношении заинтересованности эксперта в обнаружении наиболее «зрелищных» уязвимостей с целью склонения заказчика к организации определенной конфигурации защиты. Вы-

шеуказанное актуализирует разработку четкой классификации и методологических подходов по проведению не только тестов на проникновение, но и по проведению экспериментов по тестированию реальных систем, в целом.

Предлагается сформировать классификацию тестирования реальных систем и их прототипов с использованием специальных средств и способов на основе известной классификации ИТВ и ИПВ, представленных в работе [9]. В этом случае, такие часто используемые в аудите ИБ понятия как «инструментальный аудит» и «тест на проникновение» фактически будут частными случаями данного типа тестирования. Этим понятиям можно дать следующие определения.

Инструментальный аудит – экспериментальная проверка с целью оценивания состояния ИБ объекта путем применения против него специальных средств ИТВ.

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

По сфере применения, на которую ориентированы средства и способы тестирования, их можно различать на:

- применяемые в технической сфере;
- применяемые в психологической сфере.

В соответствии с этой классификацией для тестирования в технической сфере используются ИТВ, а в психологической сфере – ИПВ. Таким образом, по типу воздействия средств и способов можно выделить:

- информационно-технические воздействия;
- информационно-психологические воздействия.

По форме представления объекта, тестирование можно классифицировать следующим образом:

- на основе изучения виртуального прототипа (за счет использования средств виртуализации);
- на основе изучения реального объекта.

Необходимо отметить, что методология и терминологический аппарат тестирования специальными средствами и способами, как формы аудита ИБ проработаны еще в недостаточной степени. В связи с этим актуальным является продолжение исследований в этом направлении с целью формализации процессов тестирования реальных систем путем использования уже имеющегося задела из теории информационного противоборства, в которой ИТВ и ИПВ традиционно рассматриваются как средства атакующего воздействия [9].

Выводы

Аудит ИБ, является важным этапом выявления угроз и уязвимостей информационных систем. Вместе с тем в подавляющем числе материалов по аудиту основной упор в них делается на этапы проведения аудита, формализацию проведения аудита на основе анализа рисков или анализа стандартов ИБ. В известных работах недостаточно внимания уделяется системной классифика-

ции мероприятий аудита, а также тестированию как одному из типов аудита ИБ. Эксперименты по тестированию реальных систем 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.

В статье систематизированы основные сведения об этапах, теоретических и практических подходах к аудиту ИБ. Проведена классификация мероприятий аудита. Подробно рассмотрено тестирование, как один из основных типов аудита. Новизной работы является авторский подход к систематизации и классификации мероприятий тестирования, с учетом возможности использования специальных способов и средств на основе ИТВ и ИПВ для экспериментального исследования объектов аудита.

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. 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. Хомяков В. А. Аудит как метод модернизации системы обеспечения информационной безопасности // Экономический вестник Ярославского университета. 2013. № 29. С. 48-52.

5. Астахов А. Введение в аудит информационной безопасности [Доклад] // GlobalTrust Solutions [Электронный ресурс]. 2018. – URL: http://globaltrust.ru (дата обращения: 29.01.2018).

6. Симонов С. Аудит безопасности информационных систем // Jet Info. 1999. № 9 (76). С. 3-24.

7. Котенко И. В., Степашин М. В. Анализ защищенности компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак // Труды Института системного анализа РАН. 2007. Т. 31. С. 126-207.

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

9. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. – СПб.: Наукоемкие технологии, 2017. – 546 с.

10. Макаренко С. И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. № 3. С. 292-376. URL: http://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf (дата обращения: 29.01.2018).

11. Курило А. П., Зефиров С. Л., Голованов В. Б. и др. Аудит информационной безопасности. – М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.

12. Moeller R. R. IT Audit, Control, and Security. – Hoboken: John Wile & Sons, Inc., 2010. – 667 p.

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

14. Пакулин Н. В. Формализация стандартов и тестовых наборов протоколов интернета. Автореф. дис. … канд. техн. наук: 05.13.11. – Уфа, 2008. – 19 с.

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

16. Котухов М. М., Кубанков А. Н., Калашников А. О. Информационная безопасность: учебное пособие. – М.: Академия ИБС - МФТИ, 2009. – 195 с.

17. Иванников В. П., Петренко А. К., Кулямин В. В., Максимов А. В. Опыт использования UniTESK как зеркало развития технологий тестирования на основе моделей // Труды Института системного программирования РАН. 2013. Т. 24. С.207-218.

18. Кулямин В. В., Петренко А. К. Развитие подхода к разработке тестов UniTESK // Труды Института системного программирования РАН. 2014. Т. 26. № 1. С. 9-26.

19. Ключников Г. В., Косачев А. С., Пакулин Н. В., Петренко А. К., Шнитман В. З. Применение формальных методов для тестирования реализации IPv6 // Труды Института системного программирования РАН. 2003. Т. 4. С. 121-140.

20. Михайлов Р. Л., Ларичев А. В., Смыслова А. Л., Леонова П. Г. Модель распределения ресурсов в информационном конфликте организационно-технических систем // Вестник Череповецкого государственного университета. 2016. № 6 (75). С. 24-29.

21. Макаренко С. И., Михайлов Р. Л. Информационные конфликты - анализ работ и методологии исследования // Системы управления, связи и безопасности. 2016. № 3. С. 95-178.

22. ISO/IEC TR 19759 Software Engineering — Guide to the Software Engineering Body of Knowledge (SWEBOK). – Geneva, Switzerland: ISO, 2005.

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

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

25. 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.

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

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

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

References

1. Averichnikov V. I., Rytov M. Iu., Kuvylkin A. V., Rudanovskii M. V. *Audit informatsionnoi bezopasnosti organov ispolnitel'noi vlasti* [Audit of information security]. Moscow, Flinta Publ., 2011. 100 p. (in Russian).

2. Kulba V. V., Shelkov A. B., Gladkov Iu. M., Pavelev S. V. *Monitoring i audit informatsionnoi bezopasnosti avtomatizirovannykh system* [Monitoring and information security audit of automated systems]. Moscow, Institute of Control Science RAS, 2009. 94 p. (in Russian).

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

4. Homyakov V. A. Audit is as a method of modernization in provision system of information security. *Ekonomicheskii vestnik Iaroslavskogo universiteta*, 2013, no. 29, pp. 48-52 (in Russian).

5. Astakhov A. *Vvedenie v audit informatsionnoi bezopasnosti* [Introduction to the information security audit]. GlobalTrust Solutions [Online Resource], 2018. Available at: http://globaltrust.ru (accessed 29 January 2018) (in Russian).

6. Simonov S. Audit bezopasnosti informatsionnykh sistem [Audit of security of information systems]. *Jet Info*, 1999, vol. 76, no. 9, pp. 3-24 (in Russian).

7. Kotenko I. V., Stepashin M. V. Analiz zashchishchennosti komp'iuternykh setei na osnove modelirovaniia deistvii zloumyshlennikov i postroeniia grafa atak [Security analysis of computer networks based on modeling of malefactors ' actions and building the attack graph]. *Trudy Instituta sistemnogo analiza Rossiiskoi akademii nauk*, 2007, vol. 31, pp. 126-207 (in Russian).

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

9. Makarenko S. I. *Informatsionnoe protivoborstvo i radioelektronnaia borba v setetsentricheskikh voinakh nachala XXI veka. Monografiia* [Information warfare and electronic warfare to network-centric wars of the early XXI century. Monograph]. Saint Petersburg, Naukoemkie Tekhnologii Publ., 2017. 546 p. (in Russian).

10. Makarenko S. I. Information Weapon in Technical Area – Terminology, Classification and Examples. *Systems of Control, Communication and Security*, 2016, no. 3, pp. 292-376. Available at: http://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf (accessed 29 January 2018) (in Russian).

11. Kurilo A. P., Zefirov S. L., Golovanov V. B. and etc. *Audit informatsionnoi bezopasnosti* [Audit of information security]. Moscow, BDTs-press Publ., 2006. 304 p. (in Russian).

12. Moeller R. R. *IT Audit, Control, and Security*. Hoboken, John Wile &

Sons, Inc., 2010. 667 p.

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

14. Pakulin N. V. *Formalizatsiia standartov i testovykh naborov protokolov interneta. Avtoref. dis.* [Formalization of standards and test sets of Internet protocols. Abstract D.Ph. thesis]. Ufa, 2008. 19 p. (in Russian).

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

16. Kotukhov M. M., Kubankov A. N., Kalashnikov A. O. *Informatsionnaia bezopasnost': uchebnoe posobie* [Information security: a training manual]. Moscow, Akademiia IBS – MFTI Publ., 2009. 195 p. (in Russian).

17. Ivannikov V. P., Petrenko A. K., Kuliamin V. V., Maksimov A. V. Opyt ispol'zovaniia UniTESK kak zerkalo razvitiia tekhnologii testirovaniia na osnove modelei [The experience of using UniTESK as a mirror of the development of technology based testing models]. *Proceedings of the Institute for System Programming of the RAS*, 2013, vol. 24, pp. 207-218 (in Russian).

18. Kuliamin V. V., Petrenko A. K. Razvitie podkhoda k razrabotke testov UniTESK [Development of an approach to the development of the UniTESK test]. *Proceedings of the Institute for System Programming of the RAS*, 2014, vol. 26, no. 1, pp. 9-26 (in Russian).

19. Kliuchnikov G. V., Kosachev A. S., Pakulin N. V., Petrenko A. K., Shnitman V. Z. Primenenie formal'nykh metodov dlia testirovaniia realizatsii IPv6 [The use of formal methods for testing the IPv6 implementation]. *Proceedings of the Institute for System Programming of the RAS*, 2003, vol. 4, pp. 121-140 (in Russian).

20. Mikhailov R. L., Larichev A. V., Smyslova A. L., Leonov P. G. Model of resource allocation in information conflict of complicated organizational and technical systems. *Cherepovets state university bulletin*, 2016, no. 6, pp. 24-29 (in Russian).

21. Makarenko S. I., Mikhailov R. L. Information Conflicts – Analysis of Papers and Research Methodology. *Systems of Control, Communication and Security*, 2016, no. 3, pp. 95-178. Available at: http://sccs.intelgr.com/archive/2016-03/04-Makarenko.pdf (accessed 17 September 2016) (in Russian).

22. ISO/IEC TR 19759 Software Engineering — Guide to the Software Engineering Body of Knowledge (SWEBOK). Geneva, Switzerland, ISO, 2005.

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

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

25. Klimov S. M., Sychev M. P. Poster polygon for training and testing facilities in the field of information security. Information counteraction to the

terrorism threats, 2015, no. 24, pp. 206-213 (in Russian).

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

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

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

Статья поступила 20 января 2018 г.

Информация об авторе

Макаренко Сергей Иванович – кандидат технических наук, доцент. Заместитель генерального директора по научной работе – главный конструктор. ООО «Корпорация «Интел групп». Область научных интересов: сети и системы связи; радиоэлектронная борьба; информационное противоборство. E-mail: mak-serg@yandex.ru

Адрес: Россия, 197372, Санкт-Петербург, пр. Богатырский, д. 32, корп. 1 лит. А, офис 6Н.

Audit of Information Security – the Main Stages, Conceptual Framework, Classification of Types

S. I. Makarenko

Purpose. *The control of adequacy of methods and means of protection is important for a process of creating of an information security system. Audit of information security perform such the control. However, the published works do not contain a system classification of audit activities. Test as one of the types of audit activities of information security is not sufficiently examined. Test of real systems are considered only as "penetration testing" or " instrumental audit". The purpose of the paper is to systematize of main stages of a information security audit, theoretical and practical methods of audit, classification of audit activities. The testing as experimental research of the information system is considered with particular attention.* ***Results and their novelty****. The author's approach to the systematization and classification of audit and testing activities is presented in the paper. The theoretical approach to the audit based on the concept of "model based testing" is considered in the paper. A new practical approach to the audit is proposed in the paper as well. This practical approach is based on a study of the information systems using special means such as cyber-attacks and information-psychological influences.* ***Methods were used****. Methods of system analysis, logical induction and deduction were used for the systematization and classification of audit activities.* ***Practical relevance****. Systematization and classification of audit and testing activities, as well as proposals for audit in the form of experimental studies can be used to creation new means of cyber-attacks and information-psychological influences for testing and audit of information security.*

Keywords*: information security, audit, information security audit, testing, model based testing, testing on the basis of special means, information warfare, cyber-attack, information-psychological influence.*

Information about Author

Sergey Ivanovich Makarenko – Ph.D. of Engineering Sciences, Docent. Chief designer. "Intel Group Corporation" ltd. Field of research: stability of network against the purposeful destabilizing factors; electronic warfare; information struggle. E-mail: mak-serg@yandex.ru

Address: Russia, 197372, Saint Petersburg, Bogatyrskiy prospect, 32, korp. 1A, office 6N.