ИСПОЛЬЗОВАНИЕ ТЕСТОВЫХ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ ВОЗДЕЙСТВИЙ ДЛЯ ПРЕВЕНТИВНОГО АУДИТА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Г.Е. Смирнов, *ООО «Корпорация «Интел групп», science.cybersec@yandex.ru;*
С.И. Макаренко, *д.т.н., доцент, Санкт-Петербургский федеральный исследовательский центр РАН, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина), mak-serg@yandex.ru.*

УДК 004.7.056.53

Аннотация. В статье рассмотрены информационно-телекоммуникационные сети (ИТКС), в частности ИТКС специального назначения. Показано, что эти ИТКС являются объектами критической информационной инфраструктуры. В соответствии с законодательством Российской Федерации такие объекты должны быть подключены к центрам Государственной системы обнаружения и предупреждения компьютерных атак (ГосСОПКА), которые осуществляют аудит состояния их информационной безопасности (ИБ). Показано, что существующие центры ГосСОПКА, осуществляющие аудит состояния ИБ ИТКС, не предусматривают такой функциональности как оценку защищенности ИТКС тестовыми информационно-техническими воздействиями, аналогичными воздействиям, которые прогнозируются к применению злоумышленниками. Обоснована целесообразность применения такой разновидности аудита, а также предложен вариант совершенствования типовой архитектуры центра ГосСОПКА за счет включения в его состав автоматизированного комплекса тестирования защищенности ИТКС. Представлены предложения по составу и порядку функционирования такого автоматизированного комплекса тестирования.

Ключевые слова: информационная безопасность; аудит; тестирование; информационно-техническое воздействие; критическая информационная инфраструктура; информационно-телекоммуникационная сеть; система обнаружения и предупреждения компьютерных атак.

USE OF TEST INFORMATION AND TECHNICAL IMPACTS FOR PREVENTIVE SECURITY AUDIT OF INFORMATION AND TELECOMMUNICATION NETWORKS

Gleb Smirnov, *Head of Department, Intel Group Corporation LLC;*
Sergey Makarenko, *Ph.D., Associate Professor. St. Petersburg Federal Research Center of the Russian Academy of Sciences, Professor of the Information Security Department of the St. Petersburg State Electrotechnical University «LETI» named after V.I. Ulyanov (Lenin).*

Annotation. The article deals with information and telecommunication networks (ITCN), in particular ITCN for special purposes. It is shown that these ITCN are objects of critical information infrastructure. In accordance with the legislation of the Russian Federation, such objects must be connected to the centers of the State System for Detecting and Preventing Computer Attacks (SSPCA), which audit the state of their information security (IS). It is shown that the existing SSPCA centers that audit the state of IS ITKN do not provide for such functionality as assessing the security of information

systems by test information and technical impacts, similar to the impacts that are predicted for use by intruders. The expediency of using this type of audit has been substantiated, and a variant of improving the standard architecture of the SSPCA center by including an automated ITCN security testing complex is proposed. Proposals for the composition and operation of such an automated testing complex are presented.

Keywords: information security; audit, testing; information technology impact; critical information infrastructure; information and telecommunications network; State system for detecting and preventing computer attacks.

Введение

В 2017 г. в России был принят федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1]. Данный закон устанавливает перечень субъектов и объектов, относящихся к критической информационной инфраструктуре (КИИ) РФ, а также обязует владельцев объектов КИИ разработать комплекс мер, направленных на обеспечение их информационной безопасности (ИБ). При этом к КИИ отнесены информационно-телекоммуникационные сети (ИТКС) всех субъектов КИИ, в связи с чем актуальным является формирование новых предложений по повышению полноты аудита ИБ ИТКС как объекта КИИ.

Целью статьи является обоснование такого перспективного направления в области ИБ как превентивный аудит защищенности ИТКС тестовыми информационными-техническими воздействиями (ИТВ), которые соответствуют предполагаемым ИТВ злоумышленника. Такое тестирование, по замыслу авторов, дополнит стандартные мероприятия аудита ИТКС и повысит полноту оценки ИБ. При этом отметим, что стандартные мероприятия аудита ИТКС, как правило, не включают практические элементы проверки состояния ИБ, и проводятся путем проверки соответствия спецификациям и требованиям руководящих документов по обеспечению ИБ.

Анализ ИТКС как объекта КИИ и задач обеспечения ее защищенности

Федеральным законом № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1] к КИИ отнесена единая сеть электросвязи (ЕСЭ) РФ, а также ИТКС следующих субъектов:

- государственных органов и государственных учреждений;
- организаций здравоохранения;
- организаций науки;
- организаций транспорта;
- организаций связи;
- организаций энергетики;
- организаций банковской сферы и иных сфер финансового рынка;
- организаций топливно-энергетического комплекса;
- организаций атомной энергии;
- организаций оборонной промышленности;
- организаций ракетно-космической промышленности;
- организаций горнодобывающей промышленности;
- организаций металлургической промышленности;
- организаций химической промышленности;
- российских юридических лиц, которые обеспечивают взаимодействие указанных субъектов.

Одним из наиболее значимых субъектов КИИ является ЕСЭ, особенность которой заключается в том, что именно она объединяет различные ИТКС всех субъектов КИИ в единую информационную систему.

Единая сеть электросвязи (ЕСЭ) – сеть связи, обеспечивающая электросвязь при помощи электромагнитных систем [2].

ЕСЭ РФ состоит из сетей следующих категорий [2]:

- сети связи общего пользования (СС ОП);
- сети связи специального назначения (СС СН);
- выделенные сети связи;
- технологические сети связи, присоединенные к сети связи общего пользования;
- другие сети связи для передачи информации.

Таким образом, ЕСЭ РФ фактически представляет собой объединение отдельных категорий сетей, которые классифицируются по их предназначению. Одним из наиболее важных субъектов КИИ в составе ЕСЭ, являются СС СН.

Сеть связи специального назначения (СС СН) – сеть связи, предназначенная для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка [2].

При этом, технически понятие СС СН может быть определенно следующим образом.

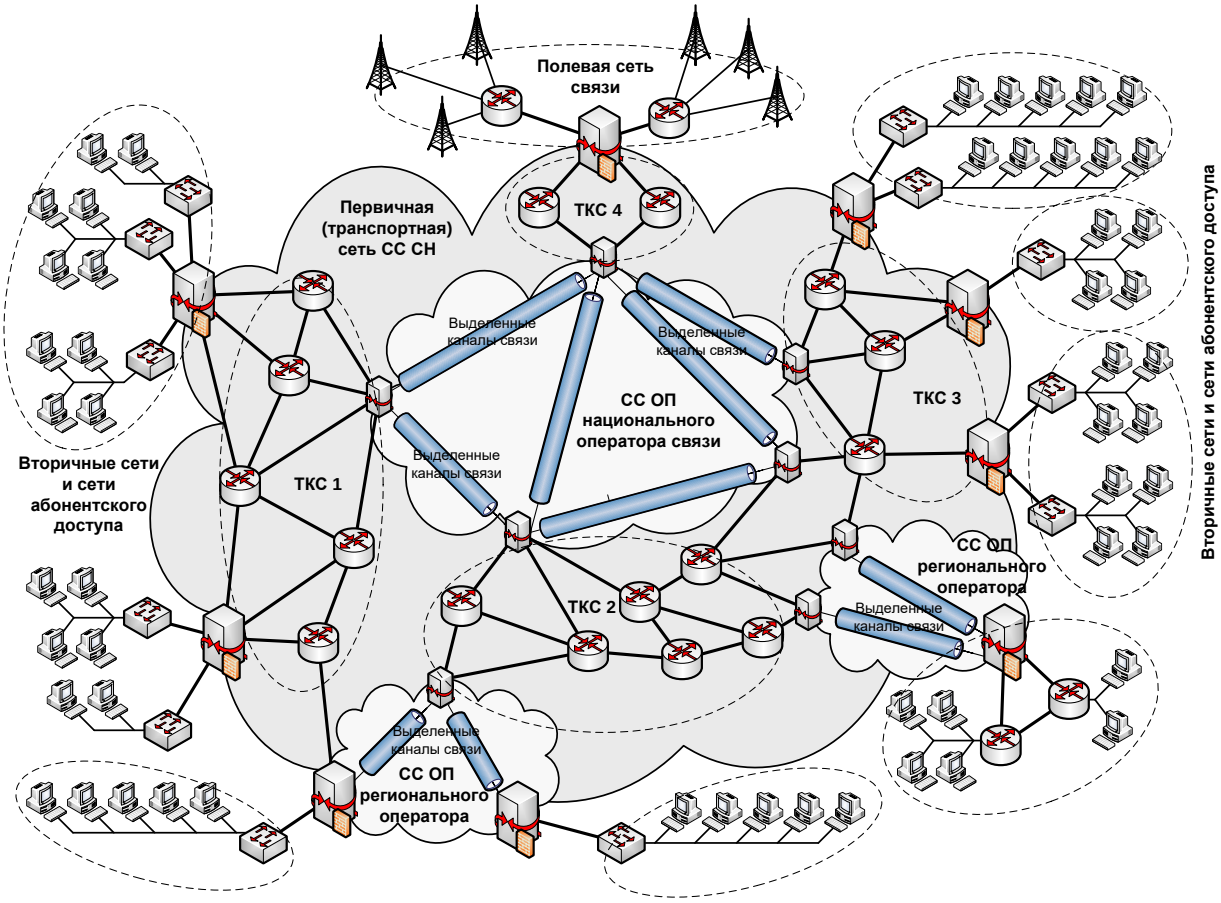

Рисунок 1

Система связи специального назначения (СС СН) – это совокупность распределенных в пространстве взаимосвязанных технических средств и

обслуживающего персонала, выполняющих задачи по обеспечению информационного обмена в системах государственного и военного управления, а также в системах управления обеспечением безопасности и правопорядка [3]. На рис. 1 изображена обобщенная структурная схема СС СН.

Анализ структуры СС СН и принципов ее функционирования, представленных в работах [3-6], показал, что СС СН является сложной организационно-технической системой (ОТС), состоящей из совокупности разнородных ИТКС специального назначения (ИТКС СН).

При этом под ИТКС СН будем понимать следующее.

Информационно-телекоммуникационная сеть (ИТКС) – это совокупность связанных линиями связи сетевых узлов, которая основана на единой транспортной технологии и эксплуатируется в соответствии с едиными принципами маршрутизации, адресации и управления, при этом в ее составе имеются граничные узлы, ответственные за допуск информации в сеть и направление ее в другие смежные информационно-телекоммуникационные системы, а также узлы, ответственные за формирование, передачу, хранение и обработку информации.

Обобщая вышеуказанное, отметим, что в данной статье в качестве прототипа объекта КИИ рассматривается некоторая абстрактная ИТКС СН, как составная часть СС СН, которая в свою очередь входит в состав ЕСЭ РФ.

Анализ структуры и принципов функционирования СС СН, проведенный на основе работ [4-6], показал, что на современном этапе своего развития СС СН претерпевают ряд существенных изменений. К основным таким изменениям относятся:

- переход от сопряжения отдельных СС СН в различных органах государственного и военного управления к единой СС СН, основанной на многоэшелонированном принципе построения (как правило СС СН включает в свой состав космический, воздушный, наземный и морской эшелоны);
- широкая интеграция в состав СС СН сегментов СС ОП и коммерческих ИТКС;
- активное замещение в СС СН технологий коммутации каналов на технологии коммутации пакетов;
- массовое использование коммерческих протоколов и технологий в составе СС СН, прежде всего, протоколов *IP (Internet Protocol)* и *MPLS (Multiprotocol label Switching);*
- конвергенция отдельных сетей и систем связи в единое информационное пространство на основе концепции *NGN;*
- широкое использование спутниковых систем связи (ССС) в качестве основы, обеспечивающей глобальную связность СС СН и глобальную управляемость во всех звеньях государственного управления, при этом в состав СС СН могут включаться ССС гражданских операторов спутниковой связи из состава СС ОП;
- использование в сетях СС СН тактического звена технологий адаптивных мобильных радиосетей *Mesh/MANET*-сетей *(Mobile Ad hoc Network);*
- использование методов обработки «больших данных», а также облачных и *Grid*-технологий для организации распределенного хранения и обработки больших массивов данных.

При этом для ИТКС СН, как «базового элемента» СС СН, эти тенденции ведут к следующей фундаментальной уязвимости ИТКС СН, которая существенно снижает уровень ее информационной безопасности (ИБ). Построение ИТКС СН на основе коммерческих протоколов и технологий связи, а также их технологическая и информационная интеграция с коммерческими ИТКС из состава СС ОП, делают возможным реализацию информационно-технических воздействий (ИТВ) через СС ОП. Наличие данной уязвимости в ТКС СН и важность защиты от нее отмечается в работах С.И. Макаренко [4-6], С.П. Воробьева, В.И. Курносова, А.Ю. Рунеева [7, 8], А.Е. Давыдова [7-9], Р.В. Максимова, О.К. Савицкого [9], А.Н. Буренина [8, 10-12], К.Е. Легкова [10-12].

Анализ протокольного базиса ТКС СН, выполненный в работе [73], позволил установить те основные коммерческие протоколы, которые получили широкое распространение в ТКС СН и уязвимости которых могут быть использованы для реализации ИТВ на сеть. К таким протоколам относятся: *IPv*4*; IPv*6*; DNS; MPLS; RIP; OSPF, PNNI, IGRP, EIGRP, BGP* 4 и некоторые другие. Особенностью большинства вышеуказанных коммерческих протоколов, является их низкая устойчивость к различного рода преднамеренным дестабилизирующим факторам, в том числе и к целенаправленным (таргетированным) ИТВ, эксплуатирующим известные уязвимости коммерческих протоколов. Это отмечается в исследованиях С.И. Макаренко [4-6, 14-16], С.М. Климова [13], М.А. Шнепс-Шнеппе [17], Н.А. Соколова [18-20], Б.С. Гольдштейна [19-21], В.А. Нетеса [22], Р.Л. Михайлова [23, 24], Р.В. Максимова [25, 26], И.И. Иванова [27], С.С. Семенова, А.С. Белова [28].

Таким образом, использование в качестве сегментов СС СН арендуемых каналов и сетей СС ОП, а также массовое использование в ИТКС СН коммерческих протоколов связи делает ИТКС СН уязвимыми к атакам средств и способов ИТВ. Эти атаки могут проводиться на ИТКС СН через сетевые сегменты, общие с СС ОП, так как СС ОП, как правило, подключены к глобальной информационно-телекоммуникационной сети интернет. При этом, как показывают результаты известных исследований, коммерческие сетевые протоколы, которые широко используются в ИТКС СН, являются не устойчивыми к третированным ИТВ, реализующихся путем эксплуатации известных уязвимостей этих протоколов.

Анализ существующей системы аудита защищенности ИТКС в рамках системы ГосСОПКА и выявление ее недостатков

Вопросы обеспечения ИБ объектов КИИ являются чрезвычайно актуальными, что отмечается не только в результатах научных исследований [29-33]. Важность проблематики ИБ объектов КИИ признана в РФ на государственном уровне, что побудило с начала 2010-х гг. начать работы по созданию системы ГосСОПКА, которая бы обеспечила аудит состояния ИБ и защиту объектов КИИ в РФ. Система ГосСОПКА основана на централизованном использовании взаимоувязанных систем обнаружения вторжений *IDS (Intrusion Detection System),* систем предотвращения *вторжений IPS (Intrusion Prevention System)*, систем предотвращения утечек конфиденциальных *данных DLP (Data Leak Prevention)*, а также систем управления инцидентами информационной безопасности *SIEM (Security Information and Event Management).*

В составе ГосСОПКА создается система государственных и частных центров, которые обслуживают субъекты КИИ. Такой центр берет на себя часть функций безопасности, необходимых для противодействия ИТВ на ИС субъектов КИИ. Как правило, к таким функциям относится:

- выявление и анализ уязвимостей, обслуживаемых ИС, координация действий по устранению выявленных уязвимостей;
- анализ событий, регистрируемых компонентами обслуживаемых ИС, и средств их защиты для поиска признаков ИТВ, направленных на эти системы;
- координация действий по реагированию на обнаруженный ИТВ, а если атака привела к инциденту – по ликвидации последствий такого инцидента;
- расследование инцидентов и ретроспективный анализ ИТВ, которые не удалось предотвратить;
- информирование персонала обслуживаемых ИТВ, проведение киберучений.

Для выполнения вышеуказанных функций, центры ГосСОПКА тесно интегрируются с защищаемыми ИС – они получают полные инвентаризационные данные ИС, контролируют их защищенность и анализируют события, регистрируемые их средствами защиты. При этом данные центры не заменяют собой собственные системы защиты ИС, т.к. владельцы объектов КИИ должны обеспечивать их ИБ самостоятельно, а центр ГосСОПКА своей деятельностью лишь компенсирует возможные ошибки.

Именно в таком виде концепция системы ГосСОПКА была утверждена Указом Президента РФ № К 1274 от 12.12.2014 г. «О Концепции ГосСОПКА», а первые технические решения были опробованы в рамках пилотного проекта в Министерстве экономического развития в 2016 г. В 2018 г. – сформирован головной центр, отвечающий за обеспечение ИБ КИИ в масштабе РФ, а также за взаимодействие с другими объектами КИИ – Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

В работе [34] проведен анализ роли ГосСОПКА в нормативных документах о безопасности КИИ. Показано, что владельцы значимых объектов КИИ обязаны выполнять требования ФСТЭК РФ по обеспечению безопасности этих объектов (ч. 3 ст. 9 ФЗ-187) и создавать системы защиты этих объектов (ст. 10 ФЗ-187). В соответствии с требованиями ФСТЭК (Приказ ФСТЭК России от 25.12.2017 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ») в системе защиты должны быть реализованы базовые меры, многие из которых непосредственно направлены на противодействие ИТВ злоумышленников [34]:

- инвентаризация компонентов ИТКС и анализ их уязвимостей;
- контроль и анализ сетевого трафика;
- мониторинг безопасности;
- антивирусная защита;
- предотвращение вторжений;
- реагирование на инциденты и т.п.

При этом владелец имеет право самостоятельно решать, как именно будут реализованы эти меры защиты (ч. 1 ст. 9 ФЗ-187). Более того, эти меры защиты являются всего лишь базовыми, то есть необходимыми, но не достаточными для обеспечения безопасности объекта КИИ. В соответствии с существующими процедурами, владелец объекта КИИ должен самостоятельно провести анализ угроз, актуальных для объекта, самостоятельно определить, как должны быть реализованы базовые меры защиты, а если их окажется недостаточно для защиты от угроз – самостоятельно усилить базовые меры защиты или разработать дополнительные [34]. В таких условиях именно аудит ИБ является тем основным

инструментом, который позволяет оценить уровень угроз для объекта КИИ и уровень его защищенности.

Ядром центра ГосСОПКА является *SIEM*-система. Именно на нее возлагаются основные задачи по аудиту ИБ – сбору данных о событиях в ИТКС, их анализу и выявлению инцидентов. Вопросам повышения эффективности *SEIM*-систем при аудите состояния ИБ посвящены работы [35-39]. Анализ этих работ показывает, что основными перспективными направлениями совершенствования *SEIM*-систем аудита объектов КИИ являются:

- повышение полноты и своевременности сбора данных о событиях в элементах и подсистемах ИТКС;
- повышение интеллектуальности обработки данных о событиях в элементах и подсистемах ИТКС, в том числе за счет использования технологий многомерного корреляционного анализа и технологий искусственного интеллекта;
- формирование положительной обратной связи в системе за счет своевременного обнаружения ИТВ и оперативного формирования сценариев защиты от него;
- моделирование действий злоумышленников с автоматической генерацией на основе результатов моделирования как высоковероятных сценариев действий злоумышленников, так и адекватных и эффективных сценариев защиты;
- повышение интеллектуальности человеко-машинного интерфейса системы в части адаптации визуализации представления информации о событиях в системе по отношению к системе зрительного восприятия человека-оператора с целью повышения информативности и эргономичности системы.

Вместе с тем вышеуказанные направления повышения эффективности *SIEM*-систем в составе центров ГосСОПКА не устраняют один из главных, по мнению авторов, недостатков этих систем – центры ГосСОПКА по своему принципу функционирования ориентированы на сбор данных об уже произошедших инцидентах ИБ, а также на сбор доказательств для оперативного исследования этих инцидентов.

Такая ориентированность центров ГосСОПКА на фиксирование инцидентов в режиме «постфактум» обусловлена общими недостатками существующих подходов к аудиту состояния ИБ ИС.

Проведенный анализ современных теоретических подходов в области аудита ИБ, представленный в работах [40, 41], показал, что задачей аудита является проверка и оценивание ИТКС на соответствие критериям, которые определяют требования к уровню ИБ. При этом, 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. При этом, тестирование и, в особенности, тестирование специальными ИТВ, является недостаточно изученной областью аудита. Имеются отдельные работы, например, [42-49], которые посвящены такому типу тестирования «как тест на проникновение», однако данные работы носят в большей степени практический, чем теоретический характер.

Вместе с тем, как показано в работах [40, 41], тестирование является более гибким инструментом аудита чем, например, мероприятия оценки соответствия, так как его проведение не ограничено рамками действующих стандартов и

регламентов. Это позволяет выбирать более широкий диапазон средств и способов тестирования, а также быть более избирательным в направлении достижения цели аудита. Например, проводить тестовое исследование ИТКС к угрозам и выявлять уязвимости, еще не описанные в базах угроз и уязвимостей. При тестировании ИТКС целесообразно сформировать и придерживаться системного подхода к проведению тестирования специальными средствами и способами ИТВ. При этом такое тестирование необходимо рассматривать как основную форму контроля устойчивости объектов КИИ к целенаправленным ИТВ сил информационных операций («кибервойск») недружественных стран [50].

Обобщая вышесказанное, можно сделать вывод о том, что функциональность существующих центров ГосСОПКА, предназначенных для аудита ИБ ИТКС субъектов КИИ, не позволяет реализовать практический превентивный аудит состояния ИБ этих ИТКС к воздействию прогнозируемых ИТВ нарушителей. Способом устранения этого недостатка является, во-первых, разработка теоретических основ испытаний ИТКС тестовыми ИТВ, с целью практического аудита состояния их ИБ, во-вторых, внесение в состав центров ГосСОПКА автоматизированного комплекса оценки тестирования ИТКС субъектов КИИ.

Предложения по использованию тестовых ИТВ для аудита защищенности ИТКС

Тестирование – проверка выполнения требований к системе при помощи наблюдения за ее работой в конечном наборе специально выбранных ситуаций [41]. Отдельное мероприятие по исследованию системы или способ изучения процессов ее функционирования называется *тестом* [41].

Тестовое ИТВ – воздействие на информационный ресурс, информационную систему, информационную инфраструктуру, на технические средства или на программы, решающие задачи получения, передачи, обработки, хранения и воспроизведения информации с целью выявить уязвимости объекта на которое производится воздействие [41].

Общая классификация мероприятий, способов и средств тестирования, используемых при аудите ИБ, представлена на рис. 2.

В настоящее время сложился подход к тестированию, когда подавляющая часть процессов оценивания безопасности систем основывается на анализе соответствия формальным требованиям по ИБ или же путем тестирования на основе моделей. Вместе с тем, требования по ИБ, как правило, формулируются по итогам анализа инцидентов, что приводит к тому, что они регулярно отстают от современных возможностей и практики действий злоумышленников.

Работы [42-43], посвященные вопросам экспериментального тестирования реальных информационных систем, рассматривают такие способы и сценарии исключительно как «тестирование на проникновение» или как «инструментальный аудит», при этом проведение такого типа аудита в отечественной практике не регламентируется 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, выполняющей аудит.

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 [51]. Как правило, для этого используются виртуальные машины, на

которых осуществляется контролируемое выполнение тестируемого программного обеспечения [52-54]. 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 [55-57].

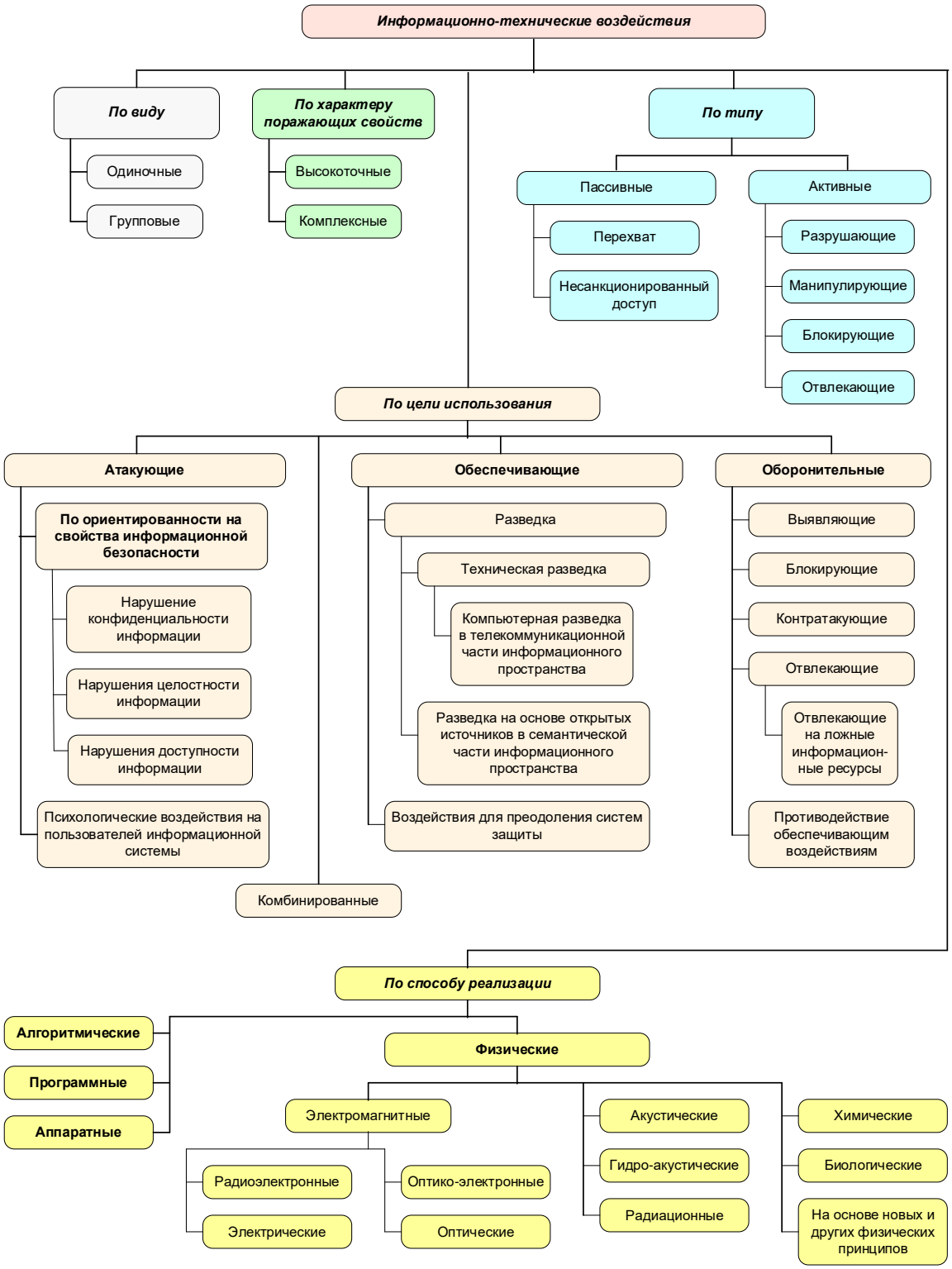

Рисунок 2

Анализ [42-43] зарубежных и отечественных методик тестирования на *проникновение (OSSTMM, ISSAF, OWASP, PTES, NIST SP* 800-115, *BSI, PETA*, методики от *Positive Technology*, методики от *Digital Security*), показывает, что они содержат достаточно развитые методические приемы проведения аудита ИБ, но не содержат исчерпывающего обоснования параметров и критериев выбора тестовых ИТВ, особенно применительно к тестированию ИТКС как объекта КИИ.

Обобщая вышесказанное, можно сделать следующие выводы:

1) для повышения полноты и адекватности аудита состояния ИБ ИТКС к прогнозируемым ИТВ злоумышленников, целесообразно включить в состав соответствующих центров ГосСОПКА автоматизированные комплексы тестирования защищенности ИТКС. На рис. 3 показана предлагаемая модернизация типовой архитектуры центра ГосСОПКА за счет добавления автоматизированного комплекса тестирования защищенности ИТКС.

2) целесообразно провести научно-теоретические исследования в интересах формирования методик выбора тестовых ИТВ с учетом особенностей ИТКС, подвергающейся тестированию, полноты тестирования, и затрат ресурсов на него.

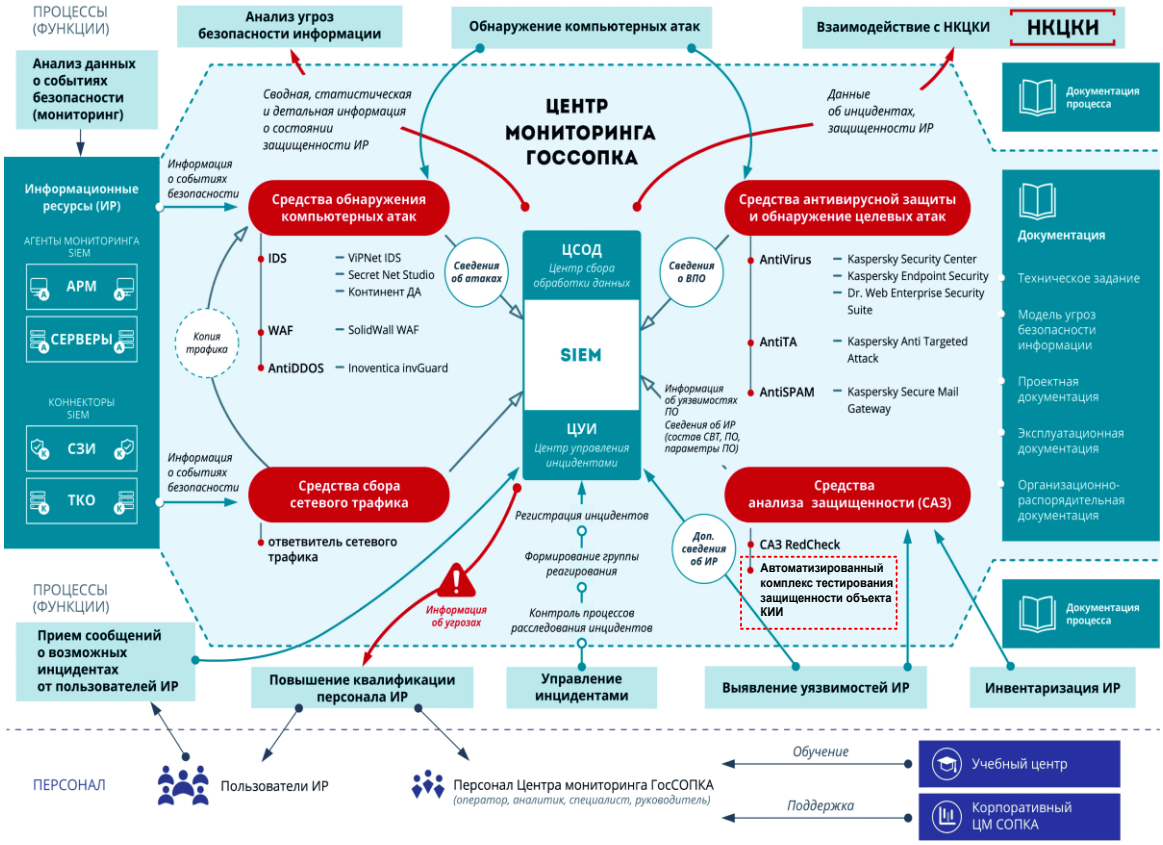

Рисунок 3

Внесение в состав центра ГосСОПКА автоматизированных комплексов тестирования защищенности позволит решить одну из основных задач обеспечения защищенности ИТКС субъектов КИИ – задачу превентивного аудита, когда уязвимость ИТКС к определенному типу ИТВ будет обнаруживаться до того, как это ИТВ будет использовано злоумышленниками.

Автоматизированный комплекс тестирования защищенности ИТКС должен включать следующие основные программные модули (рис. 4):

- модуль – база данных ИТВ, которые потенциально могут быть реализованы злоумышленниками против конкретной ИТКС;
- модуль – база сценариев проведения конкретных ИТВ;
- программный модуль, обеспечивающий автоматизированное формирование модели оценки защищенности ИТКС, на основе данных вводимых операторами центра ГосСОПКА;
- программный модуль, обеспечивающий автоматический расчет и формирование множества тестового набора ИТВ, оптимизированного по критерию «полнота тестирования / стоимость тестирования».
- программный модуль, обеспечивающий автоматизированное формирование множества ИТВ для тестирования ИТКС на основе данных, вводимых операторами центра ГосСОПКА.

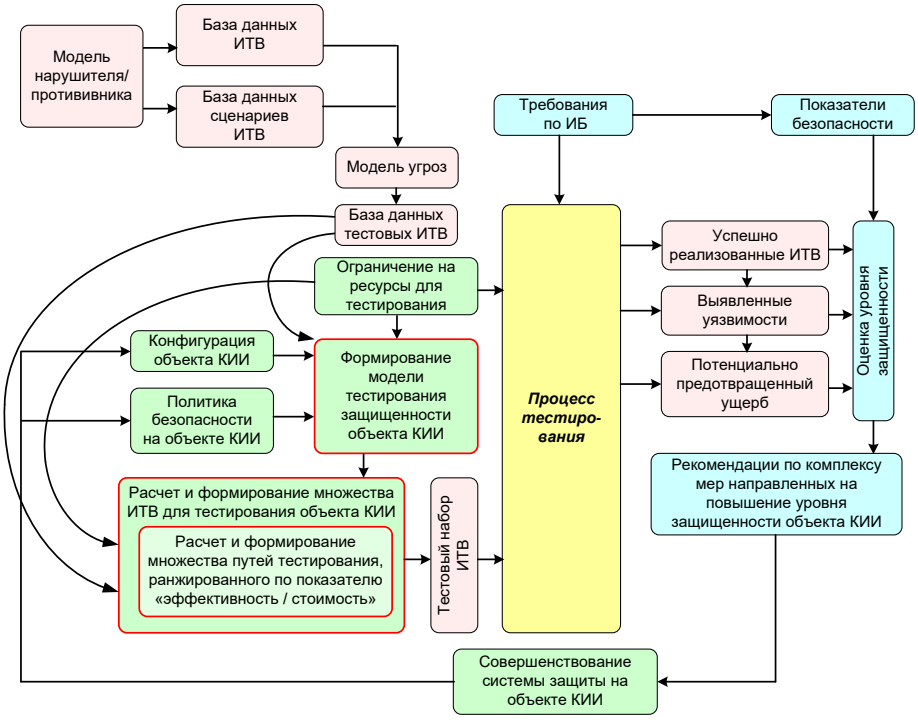

Рисунок 4

Вышеуказанные модули на практике обеспечат превентивный аудит состояния ИБ ИТКС центром ГосСОПКА путем его тестирования выбранными ИТВ и заблаговременное принятие мер по повышению уровня защищенности ИТКС до того, как злоумышленники смогут причинить ей невосполнимый критический ущерб.

Заключение

В статье рассмотрены ИТКС, как объекты КИИ, более подробно рассмотрены ИТКС СН. Обоснована необходимость обеспечения их защиты как объекта КИИ, а также проведен краткий анализ нормативных документов, регламентирующих обеспечение аудита их ИБ со стороны системы ГосСОПКА. Показано, что способы аудита состояния ИБ ИТКС, осуществляющиеся соответствующими центрами системы ГосСОПКА, не предусматривают такой

функциональности как практический аудит ИБ ИТКС тестовыми ИТВ, аналогичными ИТВ, которые прогнозируются к применению злоумышленниками. Обоснована целесообразность применения такого аудита, а также предложен вариант совершенствования типовой архитектуры центра ГосСОПКА за счет включения в его состав автоматизированного комплекса тестирования защищенности ИТКС. Представлены предложения по составу и порядку функционирования такого автоматизированного комплекса тестирования.

Предложенный подход к использованию аудита ИБ тестовыми ИТВ является, на взгляд авторов, перспективным, но в настоящее время мало распространенным способом практической оценки ИБ. Однако такой способ аудита ИБ весьма перспективен, что подтверждается научными публикациями других ученых, в частности работами [13, 58-61]. Авторы планируют продолжить исследования в данном направлении, в теоретическом плане – в направлении разработки методик выбора тестовых ИТВ с учетом особенностей ИТКС, подвергающейся тестированию, полноты тестирования и затрат ресурсов на него, а в практическом плане – в направлении обоснования аппаратно-программных решений для автоматизированных комплексов тестирования защищенности ИТКС центров ГосСОПКА, обеспечивающих высокую полноту и адекватность практического аудита состояния ИБ ИТКС.

Исследование выполнено в рамках госбюджетной темы НИР СПИИРАН № 0073-2019-0004.

Литература

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». – М., 2017.
2. Федеральный закон РФ от 07.07.2003 № 126-ФЗ «О связи». – М., 2003.
3. Боговик А.В., Игнатов В.В. Эффективность систем военной связи и методы ее оценки. – СПб.: ВАС, 2006. – 183 с.
4. Макаренко С.И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Наукоемкие технологии, 2020. – 337 с.
5. Макаренко С.И. Перспективы и проблемные вопросы развития сетей связи специального назначения // Системы управления, связи и безопасности, 2017. – № 2. – С. 18-69. DOI: 10.24411/2410-9916-2017-10202.
6. Макаренко С.И. Описательная модель сети связи специального назначения // Системы управления, связи и безопасности, 2017. – № 2. – С. 113-164. DOI: 10.24411/2410-9916-2017-10205.
7. Воробьев С.П., Давыдов А.Е., Ефимов В.В. и др. Инфокоммуникационные сети: энциклопедия. Том 1. Инфокоммуникационные сети: классификация, структура, архитектура, жизненный цикл, технологии / Наукоемкие технологии, – Изд. 2-е, перераб и доп. – СПб.: 2019. – 739 с.
8. Буренин А.Н., Воробьев С.П., Давыдов А.Е. и др. Инфокоммуникационные сети: энциклопедия. Том 2: Основы управления и обеспечения безопасности связи и информации в инфокоммуникационных сетях // Наука. Под ред. А.Ю. Рунеева. – М.: 2015. – 611 с.
9. Давыдов А.Е., Максимов Р.В., Савицкий О.К. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. – М.: Воентелеком, 2015. – 520 с.
10. Буренин А.Н., Легков К.Е., Первов М.С. Вероятностно-временные характеристики функционирования защищенной агрегативной автоматизированной системы управления сложной организационно-технической

системой в условиях интенсивных кибератак // Наукоемкие технологии в космических исследованиях Земли, 2018. – Т. 10. – № 5. – С. 56-63.
11. Емельянов А.В., Легков К.Е., Оркин В. В. Анализ проблем информационной безопасности информационных систем специального назначения при управлении ими // Проблемы технического обеспечения войск в современных условиях. Труды II межвузовской научно-практической конференции, 2017. – С. 122-126.
12. Буренин А.Н., Легков К.Е. Вопросы безопасности инфокоммуникационных систем и сетей специального назначения: основные угрозы, способы и средства обеспечения комплексной безопасности сетей // Наукоемкие технологии в космических исследованиях Земли, 2015. – Т. 7. – № 3.
13. Климов С.М. Модель бескомпроматного аудита информационной безопасности сети спутниковой связи // Двойные технологии, 2013. – № 3 (64). – С. 15-20.
14. Макаренко С.И., Афанасьев О.В., Баранов И.А., Самофалов Д.В. Экспериментальные исследования реакции сети связи и эффектов перемаршрутизации информационных потоков в условиях динамического изменения сигнально-помеховой обстановки // Радиоэлектроники, 2016. – № 4. – С. 2 – URL: http://jre.cplire.ru/jre/apr16/4/text.pdf (дата обращения 09.04.2019).
15. Макаренко С.И. Подавление сетецентрических систем управления радиоэлектронными информационно-техническими воздействиями // Системы управления, связи и безопасности, 2017. – № 4. – С. 15-59. DOI: 10.24411/2410-9916-2017-10402.
16. Макаренко С.И. Проблемы и перспективы применения кибернетического оружия в современной сетецентрической войне // Спецтехника и связь, 2011. – № 3. – С. 41-47.
17. Шнепс-Шнеппе М.А. Телекоммуникации Пентагона: цифровая трансформация и киберзащита. – М.: Горячая линия – Телеком, 2017. – 272 с.
18. Соколов Н.А. Системные аспекты построения и развития сетей электросвязи специального назначения // International Journal of Open Information Technologies. 2014. – Т. 2. – № 9. – С. 4-8.
19. Гольдштейн Б.С., Соколов Н.А. Потенциальные угрозы для сетей специального назначения // Вестник связи, 2015. – № 1. – С. 28-31.
20. Гольдштейн Б.С., Пинчук А.В., Соколов Н.А. Минимизация рисков устойчивости функционирования современных ССН // Вестник связи, 2015. – № 6. С. 49-51.
21. Гольдштейн Б.С. 10 лет эволюции коммутационной техники // Вестник связи, 2007. – № 5. – С. 1-6.
22. Нетес В.А. Надежность сетей связи в период перехода к NGN // Вестник связи, 2007. – № 9. – С. 1-8.
23. Михайлов Р.Л. Помехозащищенность транспортных сетей связи специального назначения. Монография. – Череповец: ЧВВИУРЭ, 2016. – 128 с.
24. Михайлов Р.Л. Базовая модель координации подсистем наблюдения и воздействия информационно-телекоммуникационной системы специального назначения в информационном конфликте // Системы управления, связи и безопасности, 2019. – № 4. – С. 437-450. DOI: 10.24411/2410-9916-2019-10418.
25. Шерстобитов Р.С., Шарифуллин С.Р., Максимов Р. В. Маскирование интегрированных сетей связи ведомственного назначения // Системы управления, связи и безопасности, 2018. – № 4. – С. 136-175.
26. Максимов Р.В., Орехов Д.Н., Соколовский С.П. Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки // Системы управления, связи и безопасности, 2019. – № 4. – С. 50-99. DOI: 10.24411/2410-9916-2019-10403.

27. Иванов И.И. Модель функционирования распределенных информационных систем при использовании маскированных каналов связи // Системы управления, связи и безопасности, 2020. – № 1. – С. 198-234. DOI: 10.24411/2410-9916-2020-10107.
28. Семенов С.С., Белов А.С., Воловиков В.С., Скубьев А.В. Методика обоснования требуемого уровня стойкости оборудования сетей связи в условиях внешних деструктивных воздействий // Системы управления, связи и безопасности, 2019. – № 1. – С. 33-53. DOI: 10.24411/2410-9916-2019-10102.
29. Забегалин Е.В. Логическая модель деятельности по комплексному техническому диагностированию информационной безопасности организаций и значимых объектов критической информационной инфраструктуры // Системы управления, связи и безопасности, 2019. – № 3. – С. 145-178. DOI: 10.24411/2410-9916-2019-10308.
30. Гайфулина Д.А., Котенко И.В., Федорченко А.В. Методика лексической разметки структурированных бинарных данных сетевого трафика для задач анализа протоколов в условиях неопределенности // Системы управления, связи и безопасности, 2019. – № 4. – С. 280-299. DOI: 10.24411/2410-9916-2019-10411.
31. Котенко И.В., Левшун Д.С., Саенко И.Б. Верификация политик разграничения доступа на основе атрибутов в облачных инфраструктурах с помощью метода проверки на модели // Системы управления, связи и безопасности, 2019. – № 4. – С. 421-436. DOI: 10.24411/2410-9916-2019-10417.
32. Захарченко Р.И., Королев И.Д., Саенко И.Б. Синергетический подход к обеспечению устойчивости функционирования автоматизированных систем специального назначения // Системы управления, связи и безопасности, 2018. – № 4. – С. 207-225.
33. Еделев А.В., Сендеров С.М., Береснева Н.М., Сидоров И.А., Феоктистов А.Г. Распределенная вычислительная среда для анализа уязвимости критических инфраструктур в энергетике // Системы управления, связи и безопасности, 2018. – № 3. – С. 197-231.
34. Кузнецов Д. ГосСОПКА: что такое, зачем нужна и как устроена // Anti-Malware [Электронный ресурс], 02.04.2019. – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/gossopka-what-is-it-how-it-works (дата доступа 25.11.2019).
35. Котенко И.В., Саенко И.Б. SIEM-системы для управления информацией и событиями безопасности // Защита информации. Инсайд, 2012. – № 5 (47). – С. 54-65.
36. Дойникова Е.В., Котенко И.В., Чечулин А.А. Динамическое оценивание защищенности компьютерных сетей в SIEM-системах // Безопасность информационных технологий, 2015. – Т. 22. – № 3. – С. 33-42.
37. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН, 2012. – № 1 (20). – С. 27-56.
38. Шабуров А.С., Борисов В.И. Разработка модели защиты информации корпоративной сети на основе внедрения SIEM-системы // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления, 2016. – № 19. – С. 111-124.
39. Фадин А.А., Авезова Я.Э. SIEM-решения по управлению и консолидации средств защиты информации // Автоматика. Информатика, 2015. – № 1 (36). – С. 27-31.

40. 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.
41. Макаренко С.И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. – СПб.: Наукоемкие технологии, 2018. – 122 с.
42. Скабцов Н. Аудит безопасности информационных систем. – СПб.: Питер, 2018. – 272 с.
43. Penetration Testing. Procedures & Methodologies. – EC-Council Press, 2011. – 237 p.
44. Kennedy D., O'Gorman J., Kearns D., Aharoni M. Metasploit. The Penetration Tester's Guide. – San Francisco: No Starch Press, 2011. – 299 p.
45. Cardwell K. Building Virtual Pentesting Labs for Advanced Penetration Testing. – Birmingham: Pact Publishing, 2016. – 518 c.
46. Makan K. Penetration Testing with the Bash shell. – Birmingham: Pact Publishing, 2014. – 133 p.
47. Baloch R. Ethical hacking and penetration testing guide. – London: CRC Press, 2017. – 492 c.
48. Богораз А.Г., Пескова О. Ю. Сравнительный анализ методик оценки межсетевых экранов // Труды объединенной научной конференции «Интернет и современное общество». – СПб.: НИУ ИТМО, 2013. – С. 202-209.
49. Klíma T. PETA: Methodology of information systems security penetration testing // Acta Informatica Pragensia, 2016. – Т. 5. – № 2. – С. 98-117.
50. Макаренко С.И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. № 3. С. 292-376. DOI: 10.24411/2410-9916-2016-10311.
51. 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.
52. Бородин М.К., Бородина П.Ю. Тестирование на проникновение средства защиты информации VGATE R2 // Региональная информатика и информационная безопасность. – СПб., 2017. – С. 264-268.
53. 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.
54. Кадан А.М., Доронин А.К. Инфраструктурные облачные решения для задач тестирования на проникновение // Ученые записки ИСГЗ, 2016. – Т. 14. – № 1. С. 296-302.
55. Климов С.М. Имитационные модели испытаний критически важных информационных объектов в условиях компьютерных атак // Известия ЮФУ. Технические науки, 2016. – № 8 (181). – С. 27-36.
56. Климов С.М., Сычев М. П. Стендовый полигон учебно-тренировочных и испытательных средств в области обеспечения информационной безопасности // Информационное противодействие угрозам терроризма, 2015. – № 24. – С. 206-213.
57. Петренко А.А., Петренко С.А. Киберучения: методические рекомендации ENISA // Вопросы кибербезопасности, 2015. – № 3 (11). – С. 2-14.
58. 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.

59. 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.
60. 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.
61. 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.