Макаренко С.И.

Аудит безопасности критической инфраструктуры специальными информационными воздействиями

Монография

С.И. Макаренко

Аудит безопасности критической инфраструктуры специальными информационными воздействиями

Монография

Санкт-Петербург
Наукоемкие технологии
2018

УДК 004.056
ББК 32.81
М15

Рецензенты:

Климов С. М., доктор технических наук, профессор;
Марков А. С., доктор технических наук, старший научный сотрудник;
Михайлов Р. Л., кандидат технических наук;
Саенко И. Б., доктор технических наук, профессор;
Сергеев С. Ф., доктор психологических наук, профессор.

М15 **Макаренко С.И.**
Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. – СПб.: Наукоемкие технологии, 2018. – 122 с.

ISBN 978-5-6041427-8-3

УДК 004.056
ББК 32.81

В монографии представлен авторский подход к систематизации основных сведений об этапах, теоретических и практических подходах к аудиту информационной безопасности критической информационной инфраструктуры. На основе этой систематизации сформирован оригинальный подход к тестированию информационных систем, как одного из основных типов аудита, в том числе с учетом возможности использования специальных способов и средств на основе информационно-технических и информационно-психологических воздействий.

Материалы работы могут помочь аудиторам информационной безопасности сформировать новые способы выявления уязвимостей в объектах аудита, а разработчикам средств и способов информационных воздействий, методически правильно скорректировать полученные ими научные и практические результаты с целью приведения их в соответствие с научными специальностями 05.13.19 «Методы и системы защиты информации, информационная безопасность» и 19.00.03 «Психология труда, инженерная психология, эргономика».

ISBN 978-5-6041427-8-3

Научное издание.
Напечатано с оригинал-макета, подготовленного автором.

С чувством глубокой благодарности посвящаю свою работу моим учителям, которые способствовали моему научному становлению и росту, а также определили направления моих исследований:

учителю математики гимназии № 25
г. Ставрополя
Юлии Марковне Кудриной;

кандидату технических наук доценту
Александру Васильевичу Кихтенко;

кандидату технических наук профессору
Анатолию Вячеславовичу Баженову;

доктору технических наук профессору
Владимиру Ильичу Владимирову;

доктору технических наук профессору
Александру Григорьевичу Ломако;

доктору военных наук профессору
Юрию Ивановичу Стародубцеву.

С.И. Макаренко

Оглавление

Введение

Один торговец, нахваливая свой товар покупателю, говорил: «Мои щиты не пробьет ни один меч! Мои мечи пробьют любой щит!». На это покупатель ему ответил: «Зачем мне нужен твой щит, если он не защитит от твоего меча? И зачем мне нужен твой меч, если он не пробьет твоего щита?»

Современное развитие информационных систем, их революционное внедрение в различные сферы повседневной жизни остро ставят вопросы обеспечения информационной безопасности (ИБ). Одной из составляющих процесса всестороннего обеспечения ИБ является аудит информационных систем. Именно аудит позволяет оценить правильность и адекватность принимаемых мер защиты, внедрения новых способов и средств обеспечения ИБ, и в итоге – дать окончательную оценку достигаемому уровню защищенности.

В настоящее время имеется значительное количество работ, посвященных аудиту ИБ. Однако в подавляющем большинстве этих работ аудит рассматривается как процесс проверки информационных систем на соответствие заранее определенным требованиям ИБ. Вместе с тем, требования по ИБ, как правило, формулируется по итогам анализа инцидентов, что приводит к тому, что они регулярно отстают от современных возможностей и практики действий нарушителей. Более того, существующая практика проведения аудита зачастую не предусматривает использование для проверки защищенности информационных систем известных способов, средств и сценариев действий реальных нарушителей. Незначительное количество работ, посвященных вопросам экспериментального тестирования реальных информационных систем, рассматривают такие способы и сценарии исключительно как «тестирование на проникновение» или как «инструментальный аудит», при этом проведение такого типа аудита не регламентируется каким-либо системным или хотя бы общетеоретическим подходом. Таким образом, существующий уровень развития теории и практики аудита защищённости информационных систем не предполагает проведение полномасштабных экспериментальных исследований анализируемой системы путем применения тестовых информационных воздействий, аналогичных тем, которые применяют реальные нарушители.

Серьезнее дело обстоит, когда речь идет о критической информационной инфраструктуре государства. В большинстве технически развитых стран мира уже сформированы силы информационных операций («кибервойска»), одной из задач которых является целенаправленное нарушение функционирования критической информационной инфраструктуры (КИИ) стран-противников. В этом случае уже нельзя говорить о неких одиночных «нарушителях», а необходимо рассматривать такие «кибервойска» как высокоразвитого и технически подготовленного «противника», который с началом военных действий будет проводить непрерывные изощренные атаки в информационном пространстве, без

оглядки на бескомпроматность и используя весь возможный арсенал доступных средств и способов информационного воздействия. В таких условиях уровень защищенности КИИ государства, оцененной по стандартам ИБ, ориентированным на отдельных «нарушителей», может оказаться чрезмерно завышенным, а реальное состояние защищенности КИИ – недостаточным для устойчивого функционирования этой инфраструктуры в условиях целенаправленных информационных воздействий. Подводя итог, можно сделать вывод о том, что перспективным направлением аудита КИИ является ее экспериментальная проверка путем тестирования целенаправленными информационными воздействиями, аналогичными тем, которые будут применяться потенциальным противником.

Цель работы – систематизировать основные сведения об этапах, теоретических и практических подходах к аудиту ИБ объектов КИИ, и на их основе сформировать оригинальный подход к тестированию информационных систем, как одного из основных типов их аудита, в том числе с учетом возможности использования специальных способов и средств на основе информационно-технических (ИТВ) и информационно-психологических воздействий (ИПВ). Именно этот авторский подход и отличает данную работу от других работ по тематике аудита ИБ.

Дополнительно хотелось бы отметить и еще один, методический аспект данной работы. К сожалению, разработка способов и средств информационных воздействий, семантически, в явном виде не укладывается в текущие формулировки паспортов научных специальностей 05.13.19 «Методы и системы защиты информации, информационная безопасность» и 19.00.03 «Психология труда, инженерная психология, эргономика». Автору хотелось бы обратить внимание на то, что разработка ИТВ и ИПВ с акцентом на их применимость именно для аудита информационных систем с учетом рассмотрения последних как сложных человеко-технических или организационно-технических систем, соответствует паспортам вышеуказанных специальностей. Таким образом, представленные в данной работе материалы должны помочь специалистам, которые занимаются вопросами разработки средств и способов информационных воздействий, методически правильно скорректировать полученные ими научные и практические результаты с целью приведения их в соответствие с научными специальностями 05.13.19 и 19.00.03.

В основу монографии положено развитие более ранних работ автора [1-3], а также известные работы в области аудита ИБ [4-12]. С учетом того, что акцент в данной работе сделан именно на аудит специальными информационными воздействиями, автором глубоко изучались и использовались работы, посвященные практическому тестированию систем на проникновение и так называемому инструментальному аудиту [13-17, 83-87, 97, 105, 108-118]. Кроме того, для рассмотрения относительно новой области аудита ИБ путем тестирования персонала ИПВ автором использовались работы [49-67, 73-78, 80-82, 124]. Дополнительно, для уточнения отдельных частных вопросов аудита ИБ автором были использованы работы [88-96, 98-104, 106, 107, 199-123].

В первой главе монографии – «Аудит критической информационной инфраструктуры» – показано, что аудит является важной формой контроля и проверки состояния ИБ. Такой контроль позволяет проверить адекватность выбранных мер и средств защиты, а также выявить уязвимости в существующих информационных системах. Выявлено, что объекты КИИ являются основными целями для воздействия со стороны сил информационных операций недружественных стран. Эти силы обладают высоким уровнем технических, организационных, временных и других возможностей для проведения профессиональных ИТВ и ИПВ против объектов КИИ. В связи с этим, субъекты таких воздействий в моделях ИБ нельзя рассматривать как «нарушителей», а необходимо рассматривать их как «противников». В настоящее время основными подходами к проведению аудита ИБ являются анализ рисков и анализ соответствия требованиям стандартов ИБ. В таких условиях уровень защищенности КИИ государства, оцененной по стандартам ИБ, ориентированным на отдельных «нарушителей», может оказаться чрезмерно завышенным, а реальное состояние защищенности КИИ – недостаточным для устойчивого функционирования этой инфраструктуры в условиях целенаправленных информационных воздействий. При этом перспективным направлением аудита ИБ объектов КИИ является ее экспериментальная проверка путем тестирования специальными информационными воздействиями, аналогичными тем, которые будут применяться потенциальным противником по сценариям проведения реальных информационных операций.

Во второй главе – «Тестирование как один из основных типов аудита критической информационной инфраструктуры» – показано, что тестирование является одним из типов проведения аудита, которое, однако, является недостаточно изученной теоретической областью. 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 избирательным в направлении достижения цели аудита. Например, проводить тестовое исследование объектов КИИ к угрозам и выявлять уязвимости, еще не описанные в базах угроз и уязвимостей. При тестировании объектов КИИ целесообразно сформировать и придерживаться системного подхода к проведению тестирования специальными средствами и способами ИТВ и ИПВ. При этом такое тестирование необходимо рассматривать как основную форму контроля устойчивости объектов КИИ к целенаправленным воздействиям сил информационных операций недружественных стран. «Тестирование на основе моделей» является теоретической формой проведения тестирования объектов КИИ и обоснования соответствующего инструментария для проведения экспериментальных исследований информационных воздействий. Средства и способы специальных ИТВ и ИПВ, используемые на практике в соответствующих экспериментальных исследованиях, относятся к прикладному инструментарию тестирования объектов КИИ. При проведении тестирования объекты КИИ могут быть формализованы в виде организационно-технических систем, каждая из которых декомпозируется на

информационно-организационную подсистему (которую составляют персонал, операторы, лица, принимающие решения, и т. д.) и информационно-техническую подсистему (которая включает в себя технические средства обеспечения ИБ). Тестирование уровня ИБ информационно-технической подсистемы целесообразно проводить специальными ИТВ, а тестирование информационно-организационной подсистемы – специальными ИПВ.

В третьей главе монографии – «Тестирование критической инфраструктуры специальными информационно-техническими воздействиями» – показано, что для аудита уровня защищенности объектов КИИ в технической сфере может быть использовано тестирование аппаратно-программных средств КИИ путем воздействия на них специальными средствами и способами ИТВ. При этом данные средства и способы ИТВ, а также сценарий их применения должен соответствовать тем средствам и способам ИТВ, а также тем сценариям, которые предполагаются к применению потенциальным противником. Средства и способы специальных ИТВ, предназначенные для тестирования объектов КИИ, могут быть классифицированы на: оборонительные, обеспечивающие и атакующие. В рамках тестирования объектов КИИ должны реализовываться сценарии поэтапного интегрального применения указанных типов ИТВ для всеобъемлющего анализа аппаратно-программной инфраструктуры объектов КИИ, вскрытия ее уязвимостей в технической сфере, а также для формирования предложений по модернизации оборонительных средств и способов ИТВ, повышающих устойчивость объектов КИИ в условиях ведения информационного противоборства. В настоящее время оборонительные средства (средства антивирусной защиты, системы обнаружения и предотвращения вторжений, средства криптографической защиты и т. д.) в подавляющем числе работ рассматриваются как основной элемент обеспечения ИБ, но не как средства оборонительных ИТВ. Вместе с тем, на взгляд автора, оборонительные средства ИТВ должны рассматриваться не как самодостаточные, а как важная, но при этом, только составная часть системы защиты КИИ, которые должны действовать совместно с обеспечивающими и атакующими средствами ИТВ, использующимися для тестирования эффективности обороны. В идеальном случае, оборонительные, обеспечивающие и атакующие ИТВ должны быть интегрированы в единый комплекс тестирования защищенности КИИ.

В четвертой главе – «Тестирование критической инфраструктуры специальными информационно-психологическими воздействиями» – показано, что для аудита уровня защищенности объектов КИИ в организационной и психологической сферах может использоваться тестирование отдельных лиц и персонала КИИ путем воздействия на них специальных средств и способов ИПВ. При чем, данные средства и способы ИПВ, а также сценарий их применения должны соответствовать тем средствам, способам и сценариям, которые предполагаются к применению против персонала КИИ со стороны потенциального противника. Средства и способы специальных ИПВ, предназначенные для тестирования объектов КИИ, целесообразно классифицировать на информационные, лингвистические, психотронные, психофизические, психотропные и соматопсихологические. В рамках тестирования объектов КИИ должны реализовы-

ваться сценарии поэтапного интегрального применения указанных типов ИПВ для всеобъемлющего анализа информационно-организационной подсистемы объектов КИИ, вскрытия ее уязвимостей в организационной и психологических сферах, а также для формирования предложений по повышению информационно-психологической безопасности, в интересах обеспечения устойчивости объектов КИИ в условиях ведения информационного противоборства.

Итоговую цель, на которую направлена разработка специальных средств и способов тестирования на основе ИТВ и ИПВ, можно сформулировать как формирование научно-практического задела и методологических основ для создания единого комплекса тестирования защищенности КИИ к актуальным информационным воздействиям потенциального противника в технической, организационной и психологической сферах, а также формирование научно-обоснованной стратегии совершенствования средств обеспечения ИБ для объектов КИИ, с учетом наиболее актуальных угроз.

Материал монографии ориентирован на неподготовленного читателя, интересующегося вопросами аудита информационных систем. Кроме того, материал может быть полезен специалистам, научным работникам, соискателям ученой степени, ведущим исследования в области аудита информационной безопасности и оценки защищенности информационных систем в условиях информационного противоборства.

Автор не претендует на окончательную верность и всеобъемлющее изложение всей затронутой проблематики. Вместе с тем автор, надеется, что данная работа найдет своего читателя, а для кого-то, возможно, окажется своеобразной отправной точкой в дальнейших исследованиях, связанных с аудитом ИБ путем тестирования информационных систем специальными способами и средствами информационных воздействий.

Благодарности

Автор выражает благодарность рецензентам: доктору технических наук профессору С.М. Климову, доктору технических наук старшему научному сотруднику А.С. Маркову, кандидату технических наук Р.Л. Михайлову, доктору технических наук профессору И.Б. Саенко, доктору психологических наук профессору С.Ф. Сергееву, за поиск ошибок и неточностей при рецензировании монографии, за ценные замечания, которые способствовали значительному улучшению качества работы, ее полноты и ясности, ориентированности на широкого читателя, а также кандидату технических наук К.В. Ушаневу – за стилистическую правку материала и помощь при подготовке рукописи к изданию.

Автор благодарит кандидата технических наук профессора А.В. Баженова, кандидата технических наук доцента А.В. Кихтенко, доктора технических наук профессора В.И. Владимирова, доктора технических наук профессора А.Г. Ломако, доктора военных наук профессора Ю.И. Стародубцева, за то, что именно они способствовали становлению автора как ученого, и я безмерно горжусь тем, что имел возможность работать рядом с такими людьми, и особенно – учиться у них.

Кроме того, выражаю огромную признательность моему коллеге – доктору технических наук профессору В.И. Емелину, чьи смелые и новаторские идеи в области анализа информационно-психологической безопасности технических систем еще ждут своих исследователей. Именно общение с ним и знакомство с его работами привело автора к осознанию важной роли «человеческого фактора» в сложных организационно-технических системах.

Также хочется отметить, что эпатажная критика исследований автора в их начальный период доктором технических наук профессором И.И. Сныткиным способствовала росту научного кругозора автора, его творческого потенциала, а также способности вести научные дискуссии, отстаивать свою точку зрения и просто волю к победе. А совместная работа с доктором технических наук профессором К.Ю. Цветковым, воспитала у автора глубокое отвращение к недобросовестным методам проведения исследований, фабрикации и фальсификации научных результатов, что в итоге позволило выработать собственные этические нормы при проведении научных исследований, которых автор старается придерживаться. Эти специалисты, в немалой степени способствовали развитию автора по вышеуказанным направлениям, за это я выражаю им свою благодарность.

Плодотворные исследования в области информационной безопасности стали возможными благодаря тем людям, которые помогали, поддерживали, направляли, критиковали и всячески способствовали автору в его исследованиях. Автор выражает благодарность за доброжелательную критику, научную и организационную поддержку, а также за плодотворное общение всем тем, с кем он обсуждал вопросы информационной безопасности на встречах, семинарах, конференциях, а также в процессе выполнения совместных НИОКР. Кроме того, автор считает своим долгом поблагодарить всех тех специалистов, которые внесли свой научный и исторический вклад в развитие теорий информационной безопасности и информационного противоборства.

Особую признательность хочется выразить коллективу кафедры эксплуатации и ремонта бортового авиационного радиоэлектронного оборудования (радионавигации и радиосвязи) Ставропольского ВВАИУ, коллективу кафедры радионавигации и радиолокации ВУНЦ ВВС «ВВА имени проф. Н.Е. Жуковского и Ю.А. Гагарина», коллективу кафедры сетей и систем связи космических комплексов ВКА имени А.Ф. Можайского, на которых автору посчастливилось проходить службу, а также коллективам научных отделов и центров НИИ «Вектор» и НИИ «Рубин», с которыми автору посчастливилось совместно работать над созданием новых технических систем. Творческая атмосфера этих коллективов всегда способствовала плодотворной деятельности и определила области научных интересов и направления исследований автора.

Автор будет рад сотрудничеству в рассматриваемой области исследований, а также конструктивным замечаниям и предложениям. Замечания и предложения прошу направлять по адресу: mak-serg@yandex.ru.

С.И. Макаренко

1. Аудит критической информационной инфраструктуры

1.1. Особенности проведения аудита критической информационной инфраструктуры

В 2017 г. в России был принят федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Данный закон устанавливает перечень объектов и субъектов, относящихся к КИИ РФ, а также обязует специальные службы разработать комплекс мер направленных на обеспечение их защищённости.

К объектам КИИ относятся [26]:

- информационные системы субъектов КИИ;
- информационно-телекоммуникационные сети субъектов КИИ;
- автоматизированные системы управления субъектов КИИ;
- единая сеть электросвязи, обеспечивающая взаимодействие вышеуказанных объектов.

К субъектам КИИ относятся [26]:

- государственные органы и государственные учреждения;
- организации здравоохранения;
- организации науки;
- организации транспорта;
- организации связи;
- организации энергетики;
- организации банковской сферы и иных сфер финансового рынка;
- организации топливно-энергетического комплекса;
- организации атомной энергии;
- организации оборонной промышленности;
- организации ракетно-космической промышленности;
- организации горнодобывающей промышленности;
- организации металлургической промышленности;
- организации химической промышленности;
- российские юридические лица, которые обеспечивают взаимодействие указанных субъектов.

Одновременно с этим, как показано в работе [1], ведущие зарубежные страны уже сформировали или в ближайшее время сформируют силы информационных операций («кибервойска»). Основными задачами данных сил является:

- обеспечение защищенности КИИ собственной страны;
- проведение информационных операций, в том числе и с использованием ИТВ и ИПВ, против КИИ стран-противников.

В условиях роста геополитической напряженности вокруг России, решение задачи обеспечения безопасности КИИ от ИТВ и ИПВ со стороны сил информационных операций недружественно настроенных стран является актуальной и важной задачей государственного значения.

При обеспечении 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 существующих системах КИИ. Среди процессов контроля и проверки ИБ особое положение занимает аудит ИБ, основным назначением которого является формирование независимой оценки уровня ИБ.

В настоящее время имеется значительное количество работ, посвященных аудиту ИБ, например, работы [4-12]. Однако, материалы, представленные в подавляющем большинстве этих работ, не учитывают специфики аудита систем КИИ, которая заключается в следующем. Если раннее отдельные инциденты ИБ были связанны с действиями нарушителей, то сейчас с развитием концепции информационного противоборства (ИПб), аудит КИИ должен проводиться с учетом возможностей проведения ИТВ и ИПВ силами информационных операций («кибервойсками»). В этом случае уже нельзя говорить о неких одиночных «нарушителях», а необходимо рассматривать такие силы как высокоразвитого «противника», обладающего практически неограниченными ресурсами для проведения информационных операций в мировом информационно-телекоммуникационном пространстве, задача которых – целенаправленное нарушение функционирования КИИ, без оглядки на бескомпроматность, с использованием всего возможного арсенала доступных средств и способов информационного воздействия. В таких условиях уровень защищенности КИИ государства, оцененной по стандартам ИБ, ориентированным на отдельных «нарушителей», может оказаться чрезмерно завышенным, а реальное состояние защищенности КИИ – недостаточным для устойчивого функционирования этой инфраструктуры в условиях целенаправленных информационных воздействий. Таким образом, перспективным направлением аудита КИИ является ее экспериментальная проверка путем тестирования целенаправленными информационными воздействиями, аналогичными тем, которые будут применяться потенциальным противником.

Вместе с тем, анализ известных работ по аудиту ИБ [4-12] показал, что этим работам свойственны общие недостатки. К их числу относится то, что основной упор в них делается на следующие аспекты:

- специфику отдельных этапов 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.

При этом в известных работах [4-12] недостаточно внимания уделяется 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 связи с этим, проведем анализ существующих подходов к аудиту ИБ с формированием новых положений по аудиту ИБ там, где это необходимо, с учетом целесообразности аудита систем КИИ, основанного на их экспериментальном исследовании и тестировании за счет использования специальных способов и средств ИТВ и ИПВ, имитирующих способы и средства потенциального противника.

1.2. 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 [4].

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 и формирование технических предложений [9].

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 [10].

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 [18].

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 [4].

Аудит информационной безопасности – системный процесс получения объективных качественных и количественных оценок о текущем состоянии ИБ компании в соответствии с определенными критериями и показателями безопасности [18].

Аудит информационной безопасности – комплекс организационно-технических мероприятий, проводимых независимыми экспертами, имеющих целью оценить состояние ИБ объекта аудита и степени его соответствия критериям аудита [19].

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

Аудит информационной безопасности – систематический, независимый и документируемый процесс получения оценок состояния ИБ объекта аудита и

объективного их анализа с целью установления степени соответствия критериям аудита.

1.3. 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 [4, 19]:

- 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 [19]:

- превентивные – направленные на превентивное выявление угроз и уязвимостей, а также на формирование мер по предотвращению 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 [10]:

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

По форме аудит может быть [10]:

- 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 проводится 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.

1.4. Этапы проведения аудита

При проведении аудита ИБ обычно проводится следующая последовательность мероприятий [4, 9]:

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 подходов, основанных на анализе стандартов ИБ и оценке соответствия, достаточно подробно описана в известной литературе [4, 10, 20], поэтому далее подробно не рассматривается.

1.4. Схема проведения 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 ИБ [4, 19]:
- 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 [9]:
- 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 [18]:

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

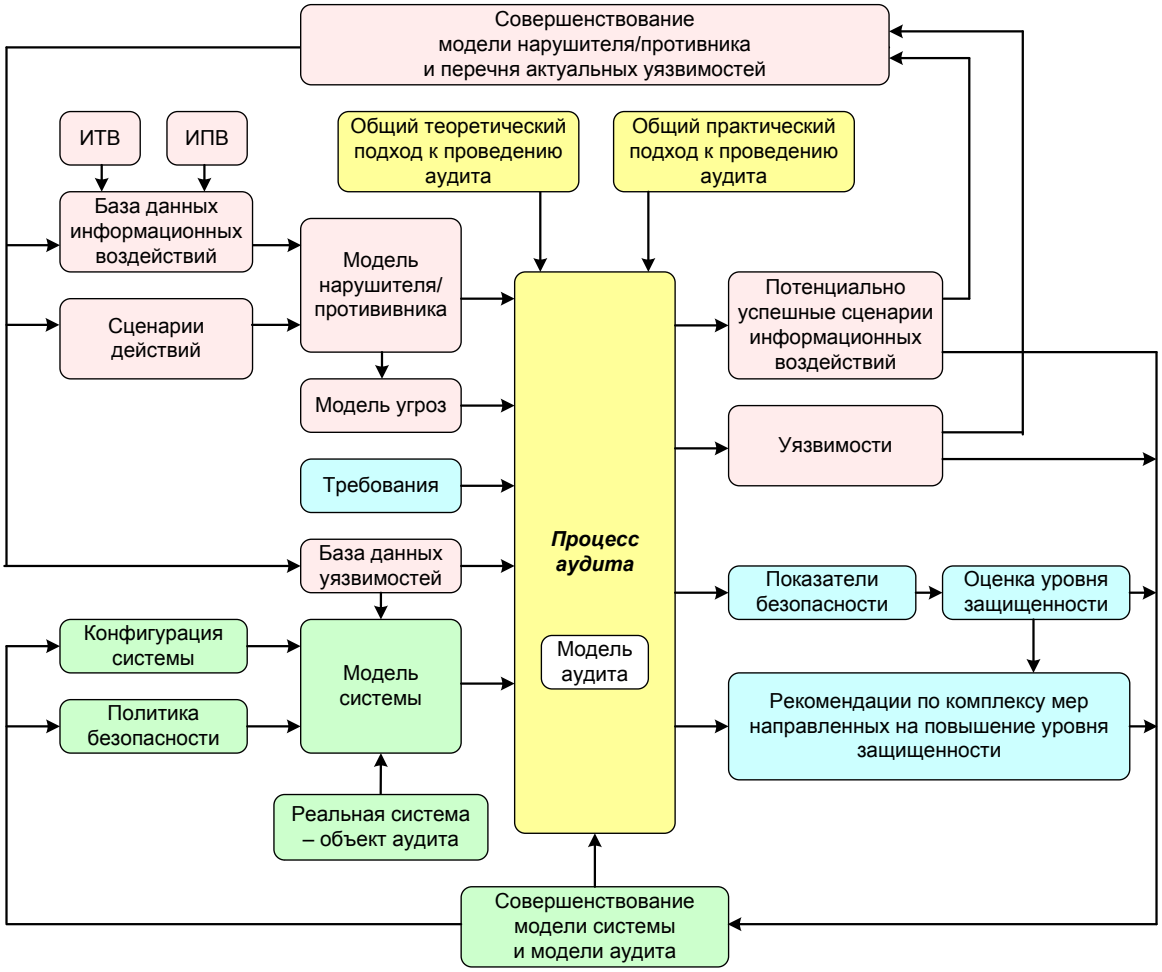


Рис. 1. Схема процесса аудита

Модель нарушителя/противника включает в себя [19]:

- формализованное описание 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.

Модель угроз включает в себя формализованное описание [19]:

- 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 ИТВ [1];
  - угрозы, реализуемые с использованием средств и способов ИПВ или социальной инженерии [1].

1.5. Общие подходы к проведению аудита

На основании анализа работ по аудиту ИБ [4-12] можно выделить следующие основные подходы к проведению аудита:

- практический подход к проведению аудита;
- теоретический подход к проведению аудита.

Общая классификация подходов представлена на рис. 2. Рассмотрим данные подходы более подробно.

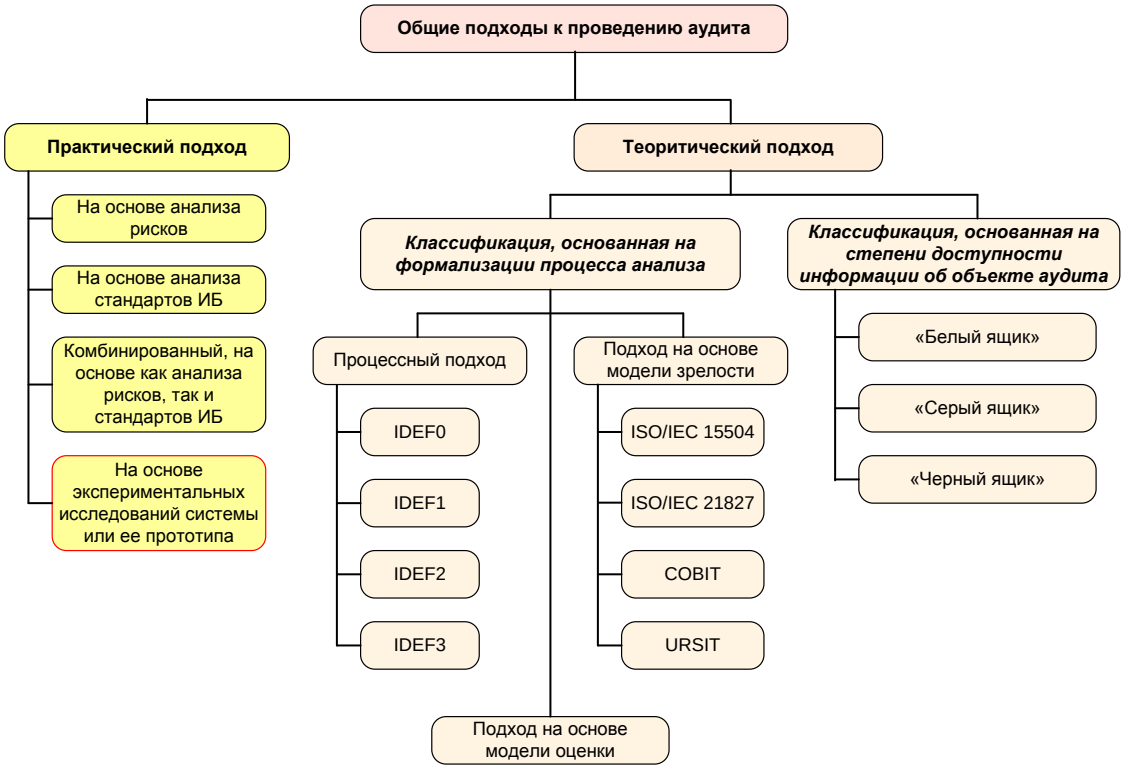


Рис. 2. Классификация общих подходов к проведению аудита ИБ

1.5.1. Практические подходы к проведению аудита

Общими практическими подходами к проведению аудита являются следующие [19]:

- 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 исследуемой системы индивидуальный набор требований ИБ, в наибольшей степени учитывающий особенности данной системы, среды ее функционирования и характерные 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 [10]. Методы анализа риска могут быть качественными, полуколичественными и количественными. Необходимо отметить, что полный количественный анализ систем не всегда возможен вследствие сложности современных ИС, затрудненности получения адекватной статистики инцидентов и др. Анализ риска включает этапы [10].

- инвентаризации и категорирования ресурсов системы;
- идентификации значимых угроз и уязвимостей;
- оценку вероятностей реализации угроз и уязвимостей.

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 [9-11].

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 по-

дробная информация об аудите на основе анализа стандартов ИБ представлена в работах [4, 10, 20].

Комбинированный аудит, с использованием 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 ИБ. 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 работ по аудиту [4, 5, 9, 10, 20, 21], указываются только эти три подхода. Вместе с тем, отдельно выделяют так называемый «тест на проникновение» [13]. От вышеуказанных подходов его отличает то, что это разновидность именно экспериментального исследования объекта, проводимого 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 – аудита 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 [10, 13, 18], 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 любых «инструментальных средств», под которыми в известной лите-

ратуре 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 [1, 3].

1.5.2. Теоретические подходы к проведению аудита

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 взаимодействующих 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).

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 их проверку на соответствие заранее определенным критериям.

Подход, основанный на модели зрелости (Capability Maturity Model – CMM) был разработан в индустрии создания программного обеспечения (ПО) для оценки зрелости процессов разработки ПО и определения ключевых действий, необходимых для дальнейшего его развития. Исходная модель CMM стала стандартом де-факто для оценки и совершенствования процессов создания ПО. 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 профиль-

ных стандартов, таких, как COBIT (Control Objectives for Information and related Technology – Задачи управления для информационных и смежных технологий) и URSIT (Uniform Interagency Rating System for Information Technology – Единая рейтинговая система для информационных технологий) [11].

В зависимости от степени доступности информации об объекте аудита выделяют следующие теоретические подходы [22]:

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

Аудит на основе «белого ящика» основан на том, что 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.

Аудит на основе «серого ящика» основан на том, что аудитору частично известно о параметрах исследуемой системы, но информация обо всех принципах ее функционирования и структуры являются скрытыми от аудитора. Например, может быть известно о входных и выходных данных, о самых общих принципах функционирования системы и ее предполагаемая структура. 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.

Аудит на основе «черного ящика» основан на том, что информация о параметрах, структуре и принципах функционирования исследуемой системы является изначально недоступной для аудитора.

1.6. Классификация аудита

Общая классификация аудита ИБ, с учетом вышепредставленной декомпозиции некоторых из этих мероприятий, приведена на рис. 3.

Аудит ИБ может быть классифицирован по следующим основаниям:

1) по цели аудита;
2) по объекту аудита;
3) по форме аудита;
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 аудита.

Классификация аудита по основаниям 1-5 была рассмотрена выше, далее будут рассмотрена классификация аудита по основаниям 6-9.

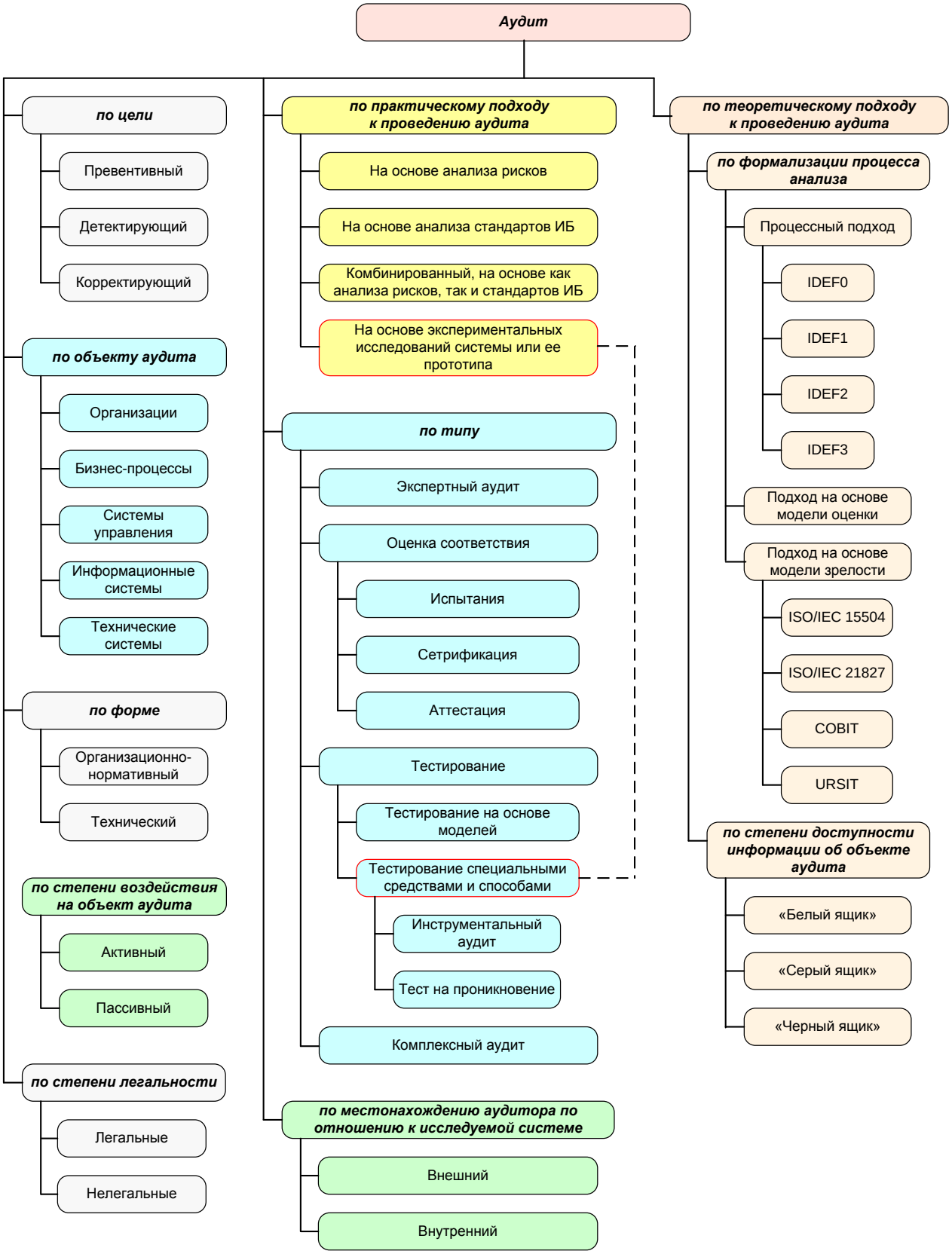


Рис. 3. Классификация мероприятий аудита

По степени воздействия на объект, аудит может быть классифицирован как:

- пассивный;
- активный.

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 связаны 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 [1, 10, 23, 24], 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, аудит может быть классифицирован как [4, 13]:

- легальный;
- нелегальный.

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

Нелегальный аудит основан на получении информации об уязвимости исследуемой системы нелегальными противозаконными 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 использования результатов аудита для нанесения ущерба исследуемой системе или организации.

При классификации аудита на легальный и нелегальный необходимо отметить следующий противоречивый момент. При проведении информационных операций соответствующими силами («кибервойсками») данные операции регламентируются внутренними уставами той стороны, которая их проводит, т.е. в отношении этой стороны аудит систем противника является легальным. Вместе с тем, проведение такого аудита, как правило, связанно с нарушением законодательства той стороны, к которой принадлежит объект аудита, соответственно по отношению к этой стороне аудит является нелегальным.

По местонахождению аудитора по отношению к исследуемой системе аудит может быть классифицирован на [4, 19]:

- внешний;
- внутренний.

Внешний аудит – проводится внешними независимыми экспертами или с использованием технических средств и способов тестирования, находящихся вне исследуемой системы. Как отмечается в работах [4, 19], 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 аудит может быть классифицирован на [4, 9, 10]:

- 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, а также 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 [4, 20].

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 [10].

Более подробная информация об оценки соответствия представлена в работе [10].

Испытание – экспериментальное определение количественных или качественных характеристик объекта испытаний в результате воздействия на него различных факторов при его функционировании или моделировании. Испытания проводятся на основании документа «программа и методика испытаний», а результаты испытания оформляются в виде протоколов испытаний или технического отчёта [10].

Аттестация – комплексная проверка 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 [10].

Сертификация – испытания технических средств защиты информации, которые проводятся независимыми испытательными лабораториями, с целью подтверждения соответствия объекта сертификации требованиям нормативных документов по защите информации [10].

Тестирование – это техническая операция, заключающаяся в определении одной или нескольких характеристик продукта, процесса или услуги соответствующей процедуре [10]. Таким образом, тестирование применительно к аудиту ИБ информационных систем – это определение одного 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 тестированию, когда строятся соответствующие модели и тестирование проводится на основе исследования данных моделей;
- *тестирование специальными средствами и способами* – практический подход к тестированию, когда тестирование проводится на основе экспериментов по воздействию средств и способов ИТВ и ИПВ на объект аудита, или его прототип.

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

Выводы по первой главе

Подводя итог материалу первой главы, можно сделать следующие краткие обобщенные выводы.

1) Аудит является важной формой контроля и проверки состояния ИБ. Такой контроль позволяет проверить адекватность выбранных мер и средств защиты, а также выявить уязвимости в существующих информационных системах.

2) Объекты КИИ являются основными целями для воздействия со стороны сил информационных операций недружественных стран. Эти силы обладают высоким уровнем технических, организационных, временных и других возможностей для проведения профессиональных ИТВ и ИПВ против объектов КИИ. В связи с этим, субъектов таких воздействий в моделях ИБ необходимо рассматривать не как «нарушителей», а как «противников», обладающих практически неограниченными ресурсами для проведения информационных операций в мировом информационном пространстве, задача которых – целенаправленное нарушение функционирования КИИ, с использованием всего возможного арсенала доступных средств и способов информационного воздействия.

3) В настоящее время основными подходами к проведению аудита ИБ являются анализ рисков и анализ соответствия требованиям стандартов ИБ. В таких условиях уровень защищенности КИИ государства, оцененный по стандартам ИБ, ориентированным на отдельных «нарушителей», может оказаться чрезмерно завышенным, а реальное состояние защищенности КИИ – недостаточным для устойчивого функционирования этой инфраструктуры в условиях целенаправленных информационных воздействий.

4) Перспективным направлением аудита ИБ объектов КИИ является ее экспериментальная проверка путем тестирования специальными информационными воздействиями, аналогичными тем, которые будут применяться потенциальным противником по сценариям проведении реальных информационных операций.

2. Тестирование как один из основных типов аудита критической информационной инфраструктуры

В известной литературе по аудиту, как правило, широко рассматриваются два вида тестирования – инструментальный аудит и тестирование на проникновение. Однако, на взгляд автора, эти типы тестирования являются разновидностью тестирования специальными средствами и способами (см. выше). Это обусловлено тем, что при инструментальном аудите используются технические средства анализа и ИТВ, при этом в данное понятие не включаются 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 ориентировано на исследование экспертного аудита [4, 9, 11, 25] и оценки соответствия [10, 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 [13-15], 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 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 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 ИБ применительно к системам КИИ.

2.1. Тестирование: определение, требования, классификация

Тестирование при аудите ИБ информационных систем – это определение одного или нескольких параметров системы, характеризующих определенную категорию ИБ (например, целостность, доступность, конфиденциальность).

Более общим определением тестирования является следующее.

Тестирование – проверка выполнения требований к системе при помощи наблюдения за ее работой в конечном наборе специально выбранных ситуаций [27].

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

Технология построения тестов должна, прежде всего, обеспечивать решение следующих двух задач [27]:

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, с 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. 4.

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

1) по цели тестирования;
2) по степени воздействия на объект тестирования;
3) по степени легальности тестирования;
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.

По цели тестирование можно классифицировать следующим образом:

- превентивное – направленное на превентивное выявление угроз, уязвимостей и предотвращение инцидентов ИБ;
- детектирующие – направленное на обнаружение новых или уточнение особенностей уже имеющихся угроз и уязвимостей системы защиты во время или после инцидентов ИБ;
- корректирующие – направленное 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 следующие виды тестирования [22-24]:

- пассивное;
- активное.

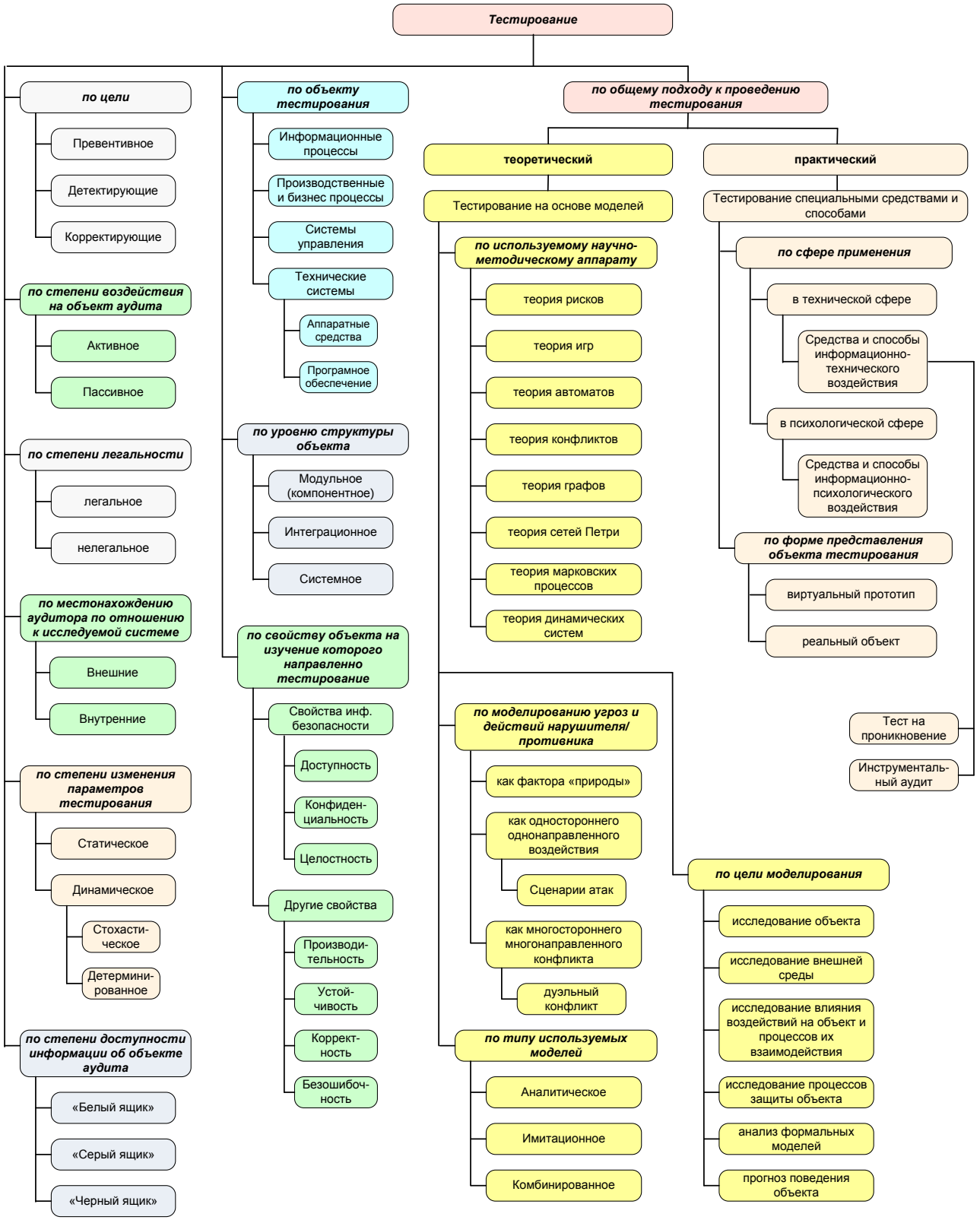


Рис. 4. Классификация мероприятий, способов и средств тестирования

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 моде-

лей когда параметр нарушителя/противника является постоянно действующим случайным фактором в модели и т. д. Также к пассивному тестированию 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 исследования, с целью провести анализ его реакций или перевести его в требуемое состояние, как правило, с более низким уровнем защищенности или эффективности функционирования. 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 как:

- 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 связано с получением информации об уязвимостях объекта тестирования с использованием способов, которые содержат признаки противоправных деяний.

По местонахождению относительно исследуемого объекта, тестирование может быть классифицировано как:

- 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 [22]:

- 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 [22].

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 [22].

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 направлено 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 типы тестирования:

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

2.2. Тестирование на основе моделей

Рассмотрим тестирование на основе моделей (MBT – Model Based Testing) более подробно на основании анализа работ [7, 22, 24, 28-30].

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 включают 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 ему возможность 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.

Общая классификация способов тестирования на основе моделей приведено на рис. 5.

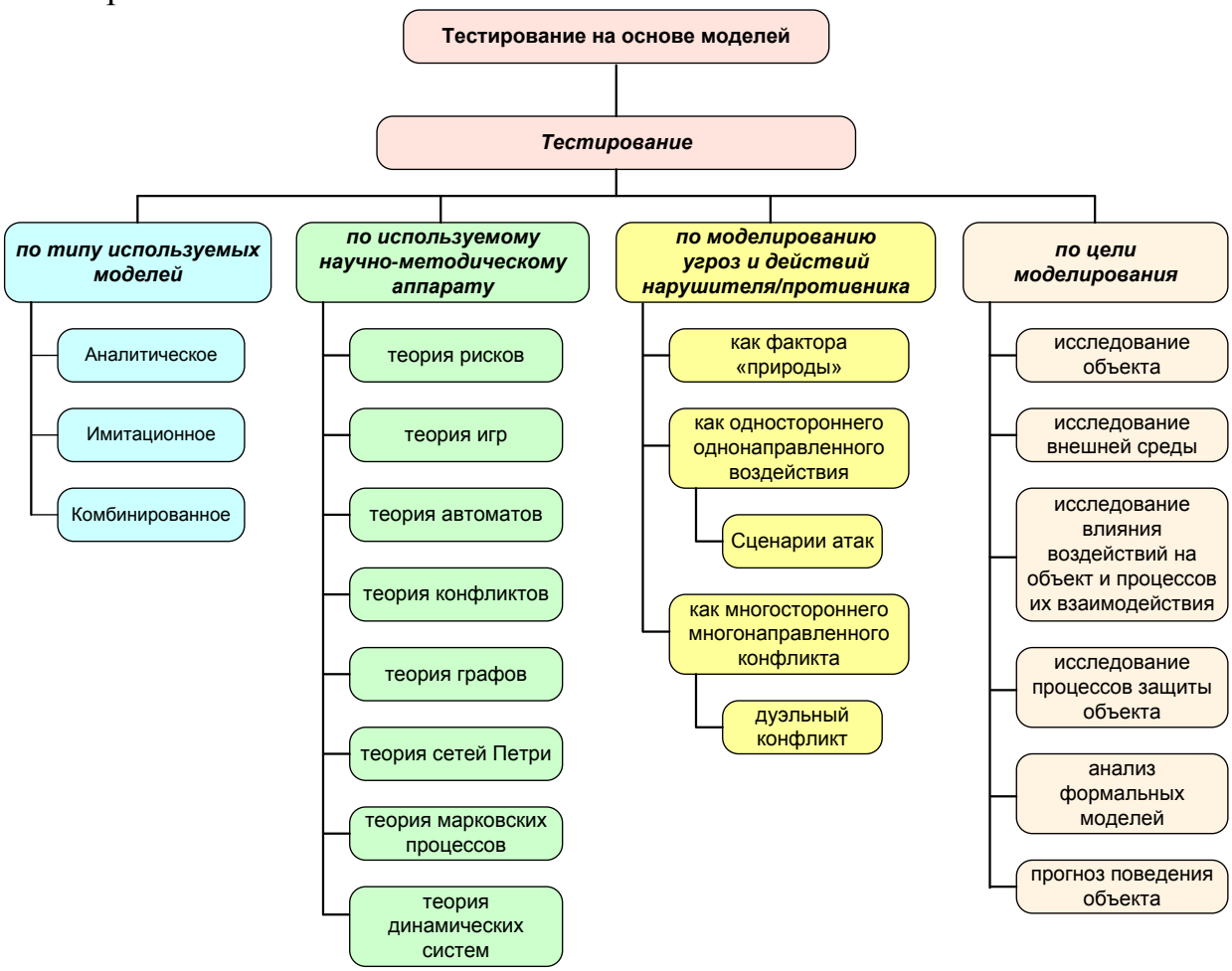


Рис. 5. Классификация способов тестирования на основе моделей

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 может быть представлено в виде:

- фактора природы (в виде отдельных детерминированных или стохастических факторов в составе модели);
- 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]);
- многостороннего многонаправленного конфликта (в этом случае рассматривается конфликт нескольких объектов, каждый из которых реа-

лизует 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 [31, 32]).

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 моделирования 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.

Тестирование на основе моделей может быть классифицировано по используемому научно-методическому аппарату:

- 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.

2.3. Тестирование специальными средствами и способами информационных воздействий

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

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 [10]. Как правило, для этого используются виртуальные машины,

на которых осуществляется контролируемое выполнение тестируемого программного обеспечения [109, 110, 113]. 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 [33-35].

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. К исследованиям, в которых развивается данное направление, относятся работы [83-87].

В настоящее время к наиболее распространенному комплексному тесту защищенности реальной информационной системы относится «тест на проникновение». Исследованию данного способа тестирования посвящены работы [13-14, 97, 105, 108-118]. Однако в подавляющем числе данных работ не содержатся какие-либо 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 характерна 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. Вышеуказанное 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, представленной в работе [1]. 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, специальные средства и способы по типу воздействия можно разделить на:

- 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.

Базовая классификация тестирования специальными средствами и способами, основанными на информационных воздействиях, приведена на рис. 6.

Рис. 6. Классификация тестирования специальными средствами и способами

Необходимо отметить, что методология и терминологический аппарат тестирования специальными средствами и способами на основе информационных воздействий как формы аудита ИБ проработаны еще в недостаточной степени. В связи с этим, актуальным является развитие этого направления с целью формализации процессов тестирования реальных систем путем использования уже имеющегося задела из теории информационного противоборства, в рамках которой ИТВ и ИПВ традиционно рассматриваются как целенаправленные информационные воздействия [1].

2.4. Особенности тестирования критической инфраструктуры информационными воздействиями в технической и в психологических сферах

В настоящее время сложился подход к тестированию ИБ отдельных систем, в котором превалирует проверка ее технических аспектов. Вместе с тем, как показал анализ работ [13, 14, 124], отправной точкой для поиска уязвимостей системы является работа с персоналом и поиск «тонких мест» в соблюдении организационных регламентов обеспечения ИБ. При этом, на начальном этапе проникновения в систему широко распространены приемы социальной инженерии, психологической манипуляции, а также шантаж и психологическое давление на сотрудников. Это позволяет сделать вывод о том, что при проведении тестирования ИБ помимо технических составляющих обеспечения безопасности в обязательном порядке необходимо учитывать психологические особенности персонала и лиц, принимающих решения (ЛПР).

С учетом вышесказанного, объект КИИ можно формализовать в виде организационно-технической системы (ОТС), представленной на рис. 7.

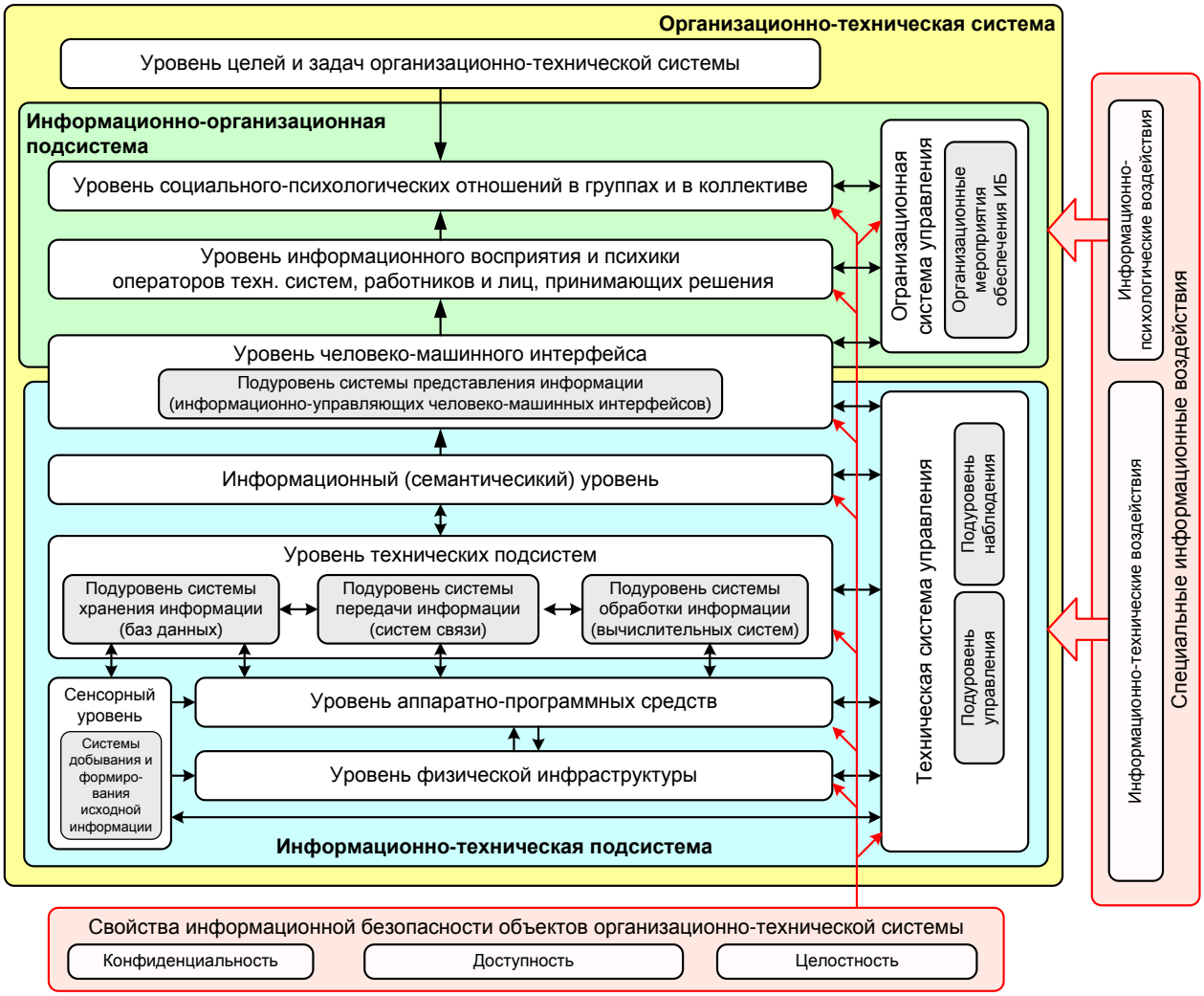


Рис. 7. Представление объекта критической информационной инфраструктуры в виде организационно-технической системы

Особенностью такой ОТС является ее декомпозиция на две основные части:

- информационно-организационную подсистему, которая включает в себя персонал, операторов технических средств, лиц, принимающих решения, их психику, когнитивную и социальную сферы, а также нормативную базу по организационным мероприятиям ИБ;
- информационно-техническую подсистему, которая включает в себя технические (аппаратные и программные) средства формирования, хранения, обработки и представления информации, а также технические средства обеспечения ИБ.

С учетом такой декомпозиции ОТС, тестирование уровня ИБ информационно-организационной подсистемы целесообразно проводить специальными ИПВ, а тестирование информационно-технической подсистемы – специальными ИТВ. При этом сценарии тестирования должны носить комплексный характер и включать в себя последовательное применение тех ИТВ и ИПВ, которые характерны для предполагаемых реальных действий нарушителя/противника при реализации воздействий на КИИ.

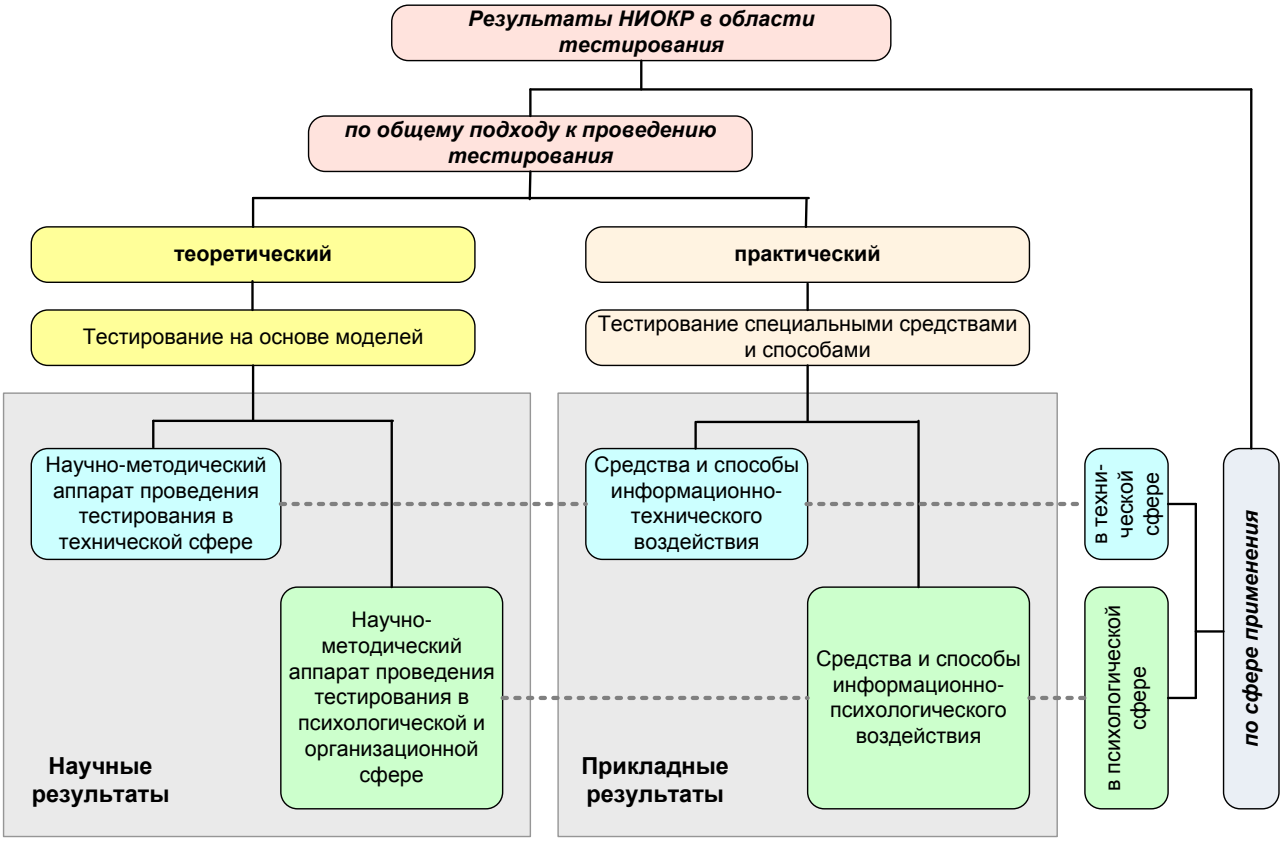


Рис. 8. Классификация результатов НИОКР в области тестирования

Вместе с тем, при указанной декомпозиции ОТС и рассмотрении ИТВ и ИПВ необходимо отметить следующее. При выполнении научных исследований в интересах обоснования информационных воздействий, как правило, формулируются два вида результатов (рис. 8).

1) Теоретические результаты, относящиеся к научно-методическому аппарату проведения тестирования и обоснования соответствующих информационных воздействий, которые, как правило, являются вкладом в развитие научного инструментария тестирования на основе моделей.
2) Практические результаты, представляющие собой новые средства и способы информационных воздействий, которые, как правило, являются вкладом в развитие прикладного инструментария тестирования.

В 3-ей и 4-ой главах более подробно будут рассмотрены специальные средства и способы ИТВ и ИПВ, которые могут быть использованы для тестирования безопасности КИИ.

Выводы по второй главе

Подводя итог материалу второй главы можно сделать следующие краткие обобщенные выводы.

1) Тестирование является одним из типов проведения аудита, которое, однако, является недостаточно изученной теоретической областью. 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 избирательным в направлении достижения цели аудита. Например, проводить тестовое исследование объектов КИИ к угрозам и выявлять уязвимости, еще не описанные в базах угроз и уязвимостей.

2) При тестировании объектов КИИ целесообразно сформировать и придерживаться системного подхода к проведению тестирования специальными средствами и способами ИТВ и ИПВ. При этом, такое тестирование необходимо рассматривать как основную форму контроля устойчивости объектов КИИ к целенаправленным воздействиям сил информационных операций недружественных стран.

3) Тестирование на основе моделей является теоретической формой проведения тестирования объектов КИИ и обоснования соответствующего инструментария для проведения экспериментальных исследований информационных воздействий. Средства и способы специальных ИТВ и ИПВ, используемые на практике в соответствующих экспериментальных исследованиях, относятся к прикладному инструментарию тестирования объектов КИИ.

4) Объект КИИ может быть формализован в виде ОТС, которая декомпозируется на информационно-организационную подсистему (персонал, операторы, ЛПР и т. д.) и информационно-техническую подсистему (технические средства обеспечения ИБ). Тестирование уровня ИБ информационно-организационной подсистемы целесообразно проводить специальными ИПВ, а тестирование информационно-технической подсистемы – специальными ИТВ.

3. Тестирование критической инфраструктуры специальными информационно-техническими воздействиями

При тестировании КИИ в технической сфере используются специальные способы и средства ИТВ.

Информационно-техническое воздействие – 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 вызвать заданные структурные или функциональные изменения.

В данном случае целевыми или структурными изменениями в объектах КИИ, на которые направленно ИТВ, является снижение уровня ИБ тестируемого объекта с целью выявления его уязвимостей и формирование мероприятий по их устранению.

Средство информационно-технического воздействия – техническое, аппаратное или программное средство, реализующее информационно-техническое воздействие или защиту от него.

Способ информационно-технического воздействия – порядок применения сил информационных операций и средств информационно-технического воздействия, вызывающий заданные структурные и/или функциональные изменения в объекте воздействия.

В рамках тестирования объектов КИИ должны реализовываться сценарии поэтапного интегрального применения средств и способов ИТВ, для всеобъемлющего анализа уязвимостей объектов КИИ в технической сфере, а также для формирования предложений по модернизации оборонительных средств в условиях ведения информационного противоборства. На взгляд автора, различные типы ИТВ (оборонительные, обеспечивающие и атакующие) должны быть интегрированы в единый комплекс тестирования защищенности объектов КИИ. Целью такого комплекса является непрерывное наращивание возможностей тестирования за счет применения обеспечивающих и атакующих средств ИТВ имитирующих передовые возможности сил информационных операций потенциального противника. В дальнейшем, по итогам анализа результатов тестирования – необходимо проводить совершенствование оборонительных средств ИТВ с учетом выявленных уязвимостей объектов КИИ.

Рассмотрим более подробно логику функционирования, классификацию и порядок применения отдельных средств и способов ИТВ, используемых для тестирования объектов КИИ, взяв за основу материал работы [1].

3.1. Общая классификация информационно-технических воздействий

Рассмотрим классификацию средств и способов специальных ИТВ, проводимых в интересах тестирования объектов КИИ, взяв за основу классификацию, представленную в работах [1, 3] – рис. 9.

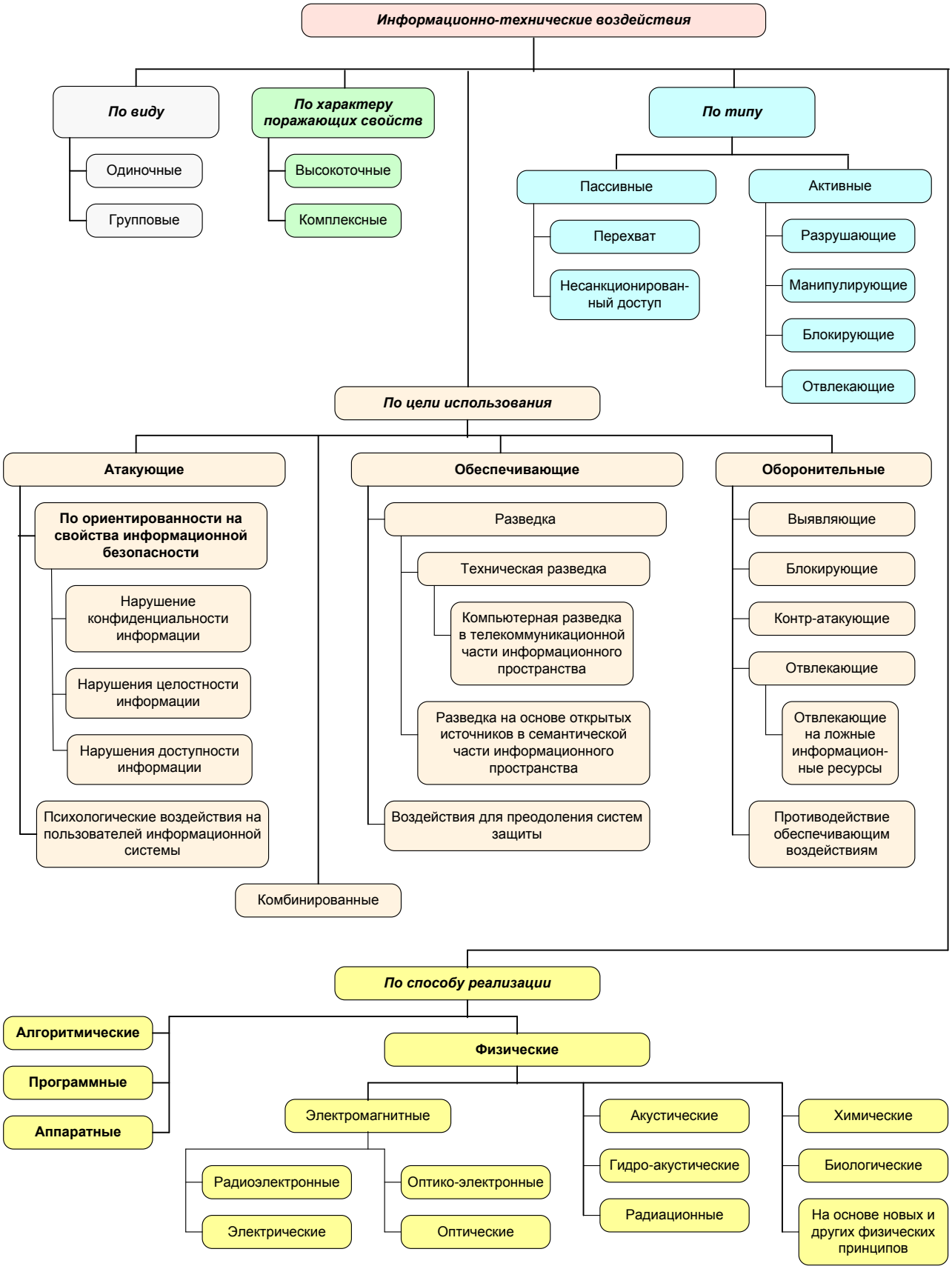


Рис. 9. Классификация специальных ИТВ,
предназначенных для тестирования объектов КИИ

Различают следующие виды ИТВ:

- одиночные;
- групповые.

По характеру поражающих свойств ИТВ классифицируют как:

- высокоточные – ИТВ, которые ориентированы на определенный информационный ресурс, процесс, технический объект или систему;
- комплексные – ИТВ, которые ориентированы на несколько информационных ресурсов, процессов, технических объектов или систем.

По типу воздействия на информацию или информационный ресурс ИТВ классифицируются следующим образом:

- пассивные:
  - перехват;
  - несанкционированный доступ;
- активные:
  - разрушающие воздействия;
  - манипулирующие воздействия;
  - блокирующие воздействия;
  - отвлекающие воздействия.

Пассивные ИТВ не оказывают непосредственного влияния на работу информационной системы, но могут нарушать ее политику безопасности. Именно отсутствие непосредственного влияния на функционирование информационной системы приводит к тому, что пассивные ИТВ трудно обнаружить. Примером пассивного ИТВ является разведка параметров информационной системы.

Активные ИТВ оказывают непосредственное влияние на функционирование информационной системы (изменение конфигурации системы, нарушение работоспособности и т. д.) и нарушают принятую в ней политику безопасности. Очевидной особенностью активных ИТВ, в отличие от пассивных, является принципиальная возможность их обнаружения, так как в результате осуществления этих ИТВ в информационной системе происходят определенные деструктивные изменения.

По цели использования ИТВ классифицируются следующим образом:

- оборонительные;
- обеспечивающие;
- атакующие;
- комбинированные.

Далее рассмотрим основные ИТВ, которые могут быть использованы для тестирования объектов КИИ именно с учетом цели их применения.

3.2. Оборонительные информационно-технические воздействия

Оборонительные ИТВ ориентированы на противодействие обеспечивающим и атакующим ИТВ нарушителя/противника. Эти оборонительные средства в подавляющем числе работ рассматриваются как основной элемент обеспечения ИБ, но не как средства оборонительных ИТВ, что на взгляд автора является не совсем правильным, так как именно эти средства играют одну из ведущих

ролей в информационном противоборстве при организации защиты объектов КИИ. К средствам оборонительных ИТВ можно отнести:

- средства антивирусной защиты;
- системы обнаружения и предотвращения вторжений;
- средства криптографической защиты;
- стеганографические средства обеспечения конфиденциальности, скрытности и целостности информационных ресурсов;
- средства технического анализа элементной базы РЭС для выявления аппаратных закладок и недекларируемых возможностей;
- средства тестирования ПО и анализа кода для выявления программных закладок и недекларируемых возможностей;
- средства создания ложных объектов и ресурсов в информационном пространстве.

Средства и способы оборонительных ИТВ можно классифицировать следующим образом:

- *выявляющие* – воздействия, ориентированные на выявление как самого факта, так и последовательности атакующих и обеспечивающих ИТВ со стороны нарушителя/противника;
- *блокирующие* – воздействия, ориентированные на блокировку атакующих ИТВ нарушителя/противника;
- *контратакующие* – воздействия на информацию, информационные ресурсы и информационную инфраструктуру нарушителя/противника с целью срыва его атакующих ИТВ;
- *отвлекающие* – воздействия, ориентированные на дезинформацию нарушителя/противника, отвлечение его атакующих или обеспечивающих ИТВ на второстепенные или ложные объекты;
- *противодействие обеспечивающим воздействиям противника* – средства и способы маскировки, обеспечения безопасности, повышения скрытности реальных режимов функционирования, а также мониторинга каналов утечки в отношении собственных информационных систем.

В целом, средства и способы вышеуказанных оборонительных ИТВ довольно широко изложены в известной литературе, поэтому здесь подробно не рассматриваются.

3.3. Обеспечивающие информационно-технические воздействия

Обеспечивающие ИТВ представляют собой воздействия, которые применяются для сбора данных, обеспечивающих эффективное применение оборонительных или атакующих ИТВ, а также преодоление средств защиты атакуемой системы.

Обеспечивающие ИТВ можно классифицировать следующим образом.

- Средства разведки:
  - традиционные средства технической разведки, классифицированные по физическим средам, в которых ведется добывание информации;
  - средства компьютерной разведки (как программные средства, так и средства доступа к физической инфраструктуре);
  - средства ведения разведки на основе открытых источников.
- Средства преодоления систем защиты.

Необходимо отметить, что при проведении практического тестирования уровня ИБ информационных систем в подавляющем числе случаев в качестве обеспечивающих ИТВ выступают средства технической разведки. Именно они позволяют получить информацию об атакующих средствах ИТВ нарушителя/противника и способах его применения, что позволяет более рационально сконфигурировать собственные средства защиты. Воздействие средств разведки проявляется как в виде пассивных действий, направленных на добывание информации и, как правило, связанных с нарушением ее конфиденциальности, так и активных действий, направленных на создание условий, благоприятствующих добыванию информации.

3.3.1. Техническая разведка

Техническая разведка – целенаправленная деятельность по добыванию с помощью технических средств соответствующих сведений.

Для ведения разведки используются различные каналы утечки информации, которые по используемой физической среде (полю) классифицируются следующим образом [37, 38]:

- радиоканалы (электромагнитные излучения радиодиапазона);
- акустические каналы (звуковые колебания в звукопроводящей среде);
- электрические каналы (напряжения и токи в токопроводящих коммуникациях);
- оптические каналы (электромагнитные излучения в инфракрасной, видимой и ультрафиолетовой частях спектра);
- материально-вещественные каналы (бумага, фото, магнитные носители, отходы, выбросы и т. д.);
- другие каналы (радиационные, магнитометрические и т. д.).

Выделяют следующие виды технической разведки, которые используют соответствующие средства и каналы утечки информации [37, 38]:

- радиоэлектронную;
- оптическую;
- оптико-электронную;
- акустическую;
- гидроакустическую;
- химическую;
- радиационную;
- сейсмическую;

- магнитометрическую;
- компьютерную;
- измерительно-сигнатурную.

Из вышеуказанных видов наибольшее распространение при проведении обеспечивающих ИТВ получили, в первую очередь, компьютерная разведка, а также радиоэлектронная и оптико-электронная разведки.

При классификации технических средств разведки используют различные признаки – рис. 10.

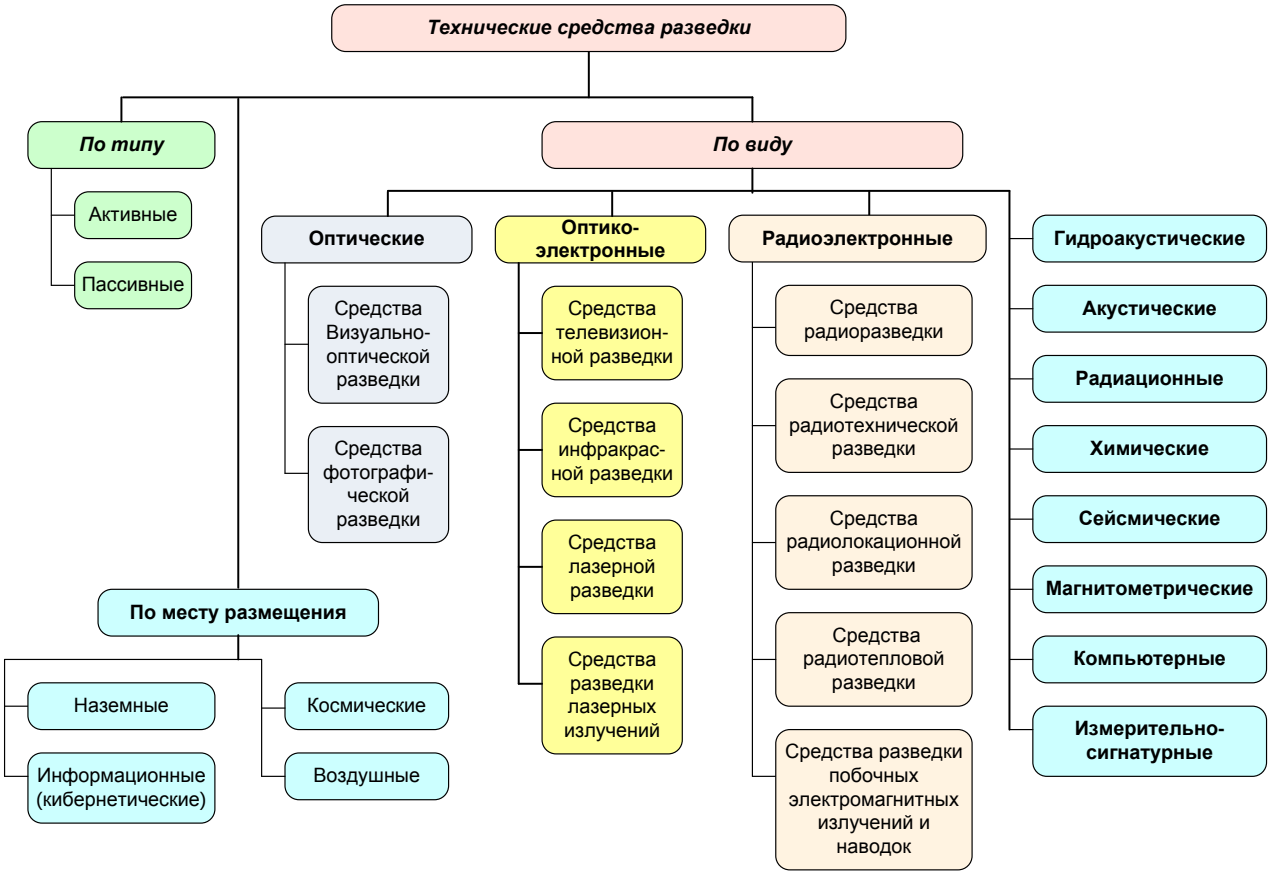


Рис. 10. Классификация технических средств разведки [36]

Радиоэлектронная разведка – процесс получения информации в результате приема и анализа электромагнитных излучений радиодиапазона, создаваемых работающими радиоэлектронными средствами [39].

Составной частью радиоэлектронной разведки является радиоразведка.

Радиоразведка – вид радиоэлектронной разведки, ориентированной на различные виды радиосвязи, основным содержанием которой является: обнаружение и перехват открытых, засекреченных, кодированных передач связных радиостанций; пеленгование их сигналов; анализ и обработка добываемой информации с целью вскрытия ее содержания и определения местонахождения источников излучения; снижение нагрузки или подрыв криптографических систем [39].

Оптико-электронная разведка – процесс добывания информации с помощью средств, включающих входную оптическую систему с фотоприемником и электронные схемы обработки электрического сигнала, которые обеспечива-

ют прием и анализ электромагнитных волн видимого и ИК-диапазонов, излученных или отраженных объектами и местностью [39].

3.3.2. Компьютерная разведка

Компьютерная разведка – добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и пользователей [1].

В настоящее время именно средства и способы компьютерной разведки составляют основу, за счет которой реализуются обеспечивающие ИТВ.

Выделяют три типа источников информации для компьютерной разведки [40]:

- данные, сведения и информация, обрабатываемые, передаваемые и хранимые в компьютерных системах и сетях;
- характеристики программных, аппаратных и программно-аппаратных комплексов;
- характеристики пользователей компьютерных систем и сетей.

По виду реализации средства и способы компьютерной разведки можно классифицировать следующим образом:

- *физические* – реализованные в виде физических или аппаратных средств, которые подключаются к инфокоммуникационной инфраструктуре, ведут анализ физических полей, побочных электромагнитных излучений и наводок (ПЭМИН) в интересах добывания данных, сведений и информации;
- *программные* – реализованные в виде программных средств, которые в виде вирусов, закладок или специализированного программного обеспечения добывают данные, сведения и информацию за счет анализа логики построения и функционирования компьютерных систем, а также информационных потоков, циркулирующих в них.

По принципам построения средств и их функциональному предназначению можно выделить следующие типы компьютерной разведки [40]:

- *семантическая* – обеспечивающая добывание фактографической и индексно-ссылочной информации путем поиска, сбора и анализа структурируемой и неструктурируемой информации из общедоступных информационных ресурсов или конфиденциальных источников компьютерных систем и сетей, а также путем семантической (аналитической) обработки полученных и накопленных массивов сведений и документов;
- *алгоритмическая* – обеспечивающая добывание информации путем использования заранее внедренных изготовителем программных или аппаратных закладок, ошибок и недекларированных возможностей компьютерных систем и сетей;
- *вирусная* – обеспечивающая добывание данных путем внедрения и применения вирусных программ в уже эксплуатируемые программные комплексы и в системы для перехвата управления компьютерными системами;

- *разграничительная* – обеспечивающая добывание информации из отдельных (локальных) компьютерных систем, которые могут не входить в состав сети, осуществляемая на основе преодоления средств разграничения доступа путем несанкционированного доступа к информации, физического доступа к компьютерной системе или к носителям информации;
- *сетевая* – обеспечивающая добывание информации из компьютерных сетей путем мониторинга сети, инвентаризации и анализа уязвимостей сетевых ресурсов и объектов пользователей, а также последующего удаленного доступа к информации путем использования выявленных уязвимостей систем и средств сетевой (межсетевой) защиты ресурсов, а также блокирование доступа к ним, модификация, перехват управления либо маскировка своих действий;
- *потоковая* – обеспечивающая добывание информации путем перехвата, обработки и анализа сетевого трафика, выявления структур компьютерных сетей, а также их технических параметров;
- *аппаратная* – обеспечивающая добывание информации путем обработки сведений, получения аппаратуры, оборудования, технических модулей и их анализа, испытания для выявления их технических характеристик и возможностей, полученных другими видами компьютерной разведки;
- *форматная* – обеспечивающая добывание информации путем агрегированной обработки, фильтрации, декодирования, а также проведения других преобразований форматов (представления, передачи и хранения) добытых данных в сведения, а затем – в информацию для последующего ее наилучшего представления пользователям;
- *пользовательская* – обеспечивающая добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также путем обеспечения им доступа к информации, циркулирующей в специально созданной ложной информационной инфраструктуре.

На данном этапе развития компьютерных систем и сетей эти типы компьютерной разведки охватывают все существующие многоуровневые «горизонтальные» и «вертикальные» каналы утечки информации из компьютерных систем и сетей. При этом внутри указанных типов возможно выделение нескольких подтипов разведки, например, по виду добываемой информации на: *фактографическую* («*видовую*») и *параметрическую*.

Общая классификация средств и способов компьютерной разведки представлена на рис. 11.

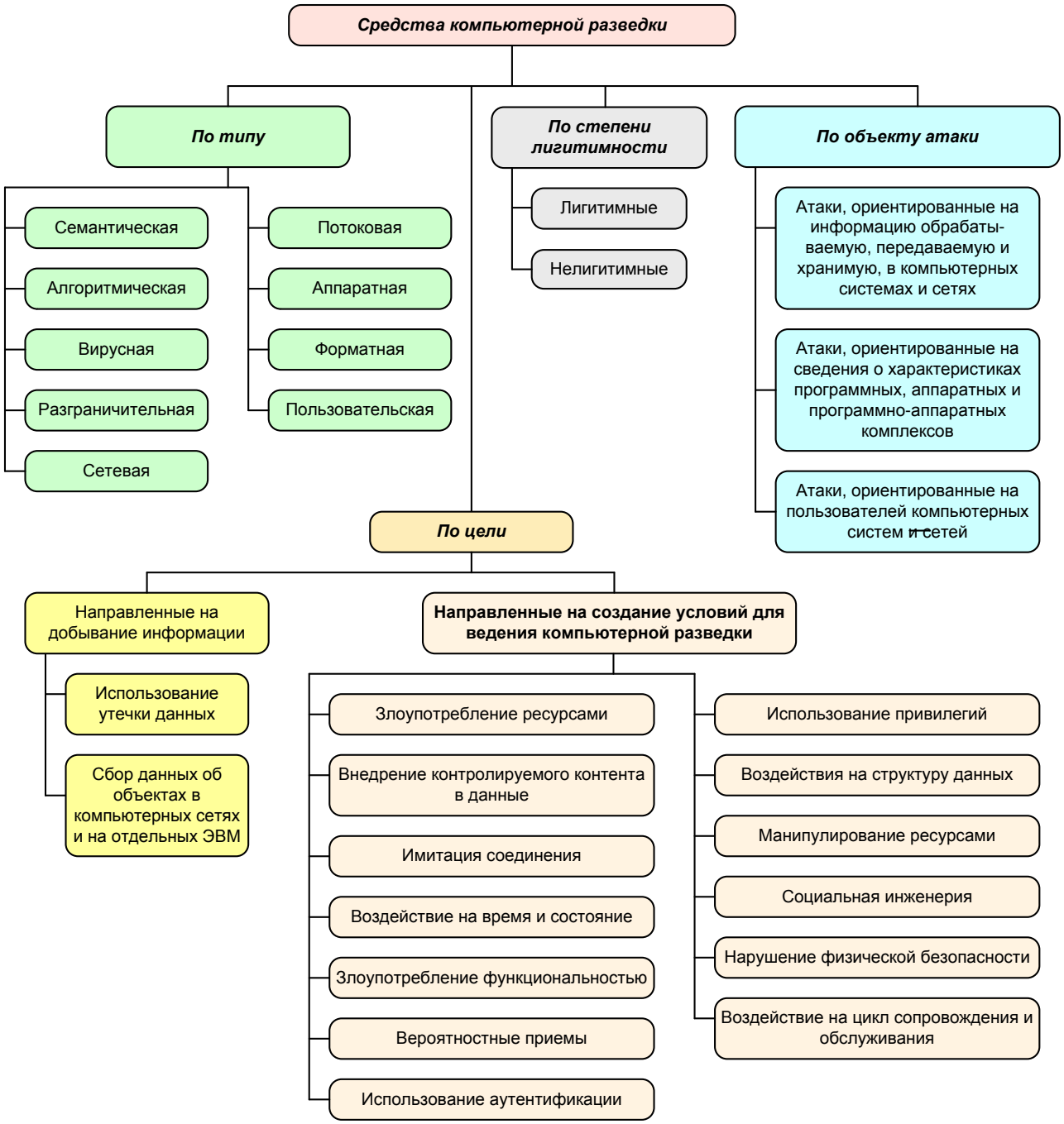


Рис. 11. Классификация средств компьютерной разведки [1]

Основным способом реализации разведки является атака средств компьютерной разведки [41, 42].

Атака средств компьютерной разведки – как пассивные действия, направленные на добывание информации и, как правило, связанные с нарушением ее конфиденциальности, так и активные действия, направленные на создание условий, благоприятствующих добыванию информации.

К настоящему времени сложился подход к описанию компьютерных атак, основанный на использовании их классификации с учетом множества признаков. Наиболее полный учет признаков реализован в классификации CAPEC [43], разработанной корпорацией MITRE. Однако классификация CAPEC не выделяет в отдельную категорию атаки средств компьютерной разведки. Учи-

тывая этот недостаток классификации CAPEC, отечественными специалистами в работе [42] была предложена классификация атак средств компьютерной разведки с включением в классификацию образцов конкретных атак. Эта классификация представлена на рис. 12.

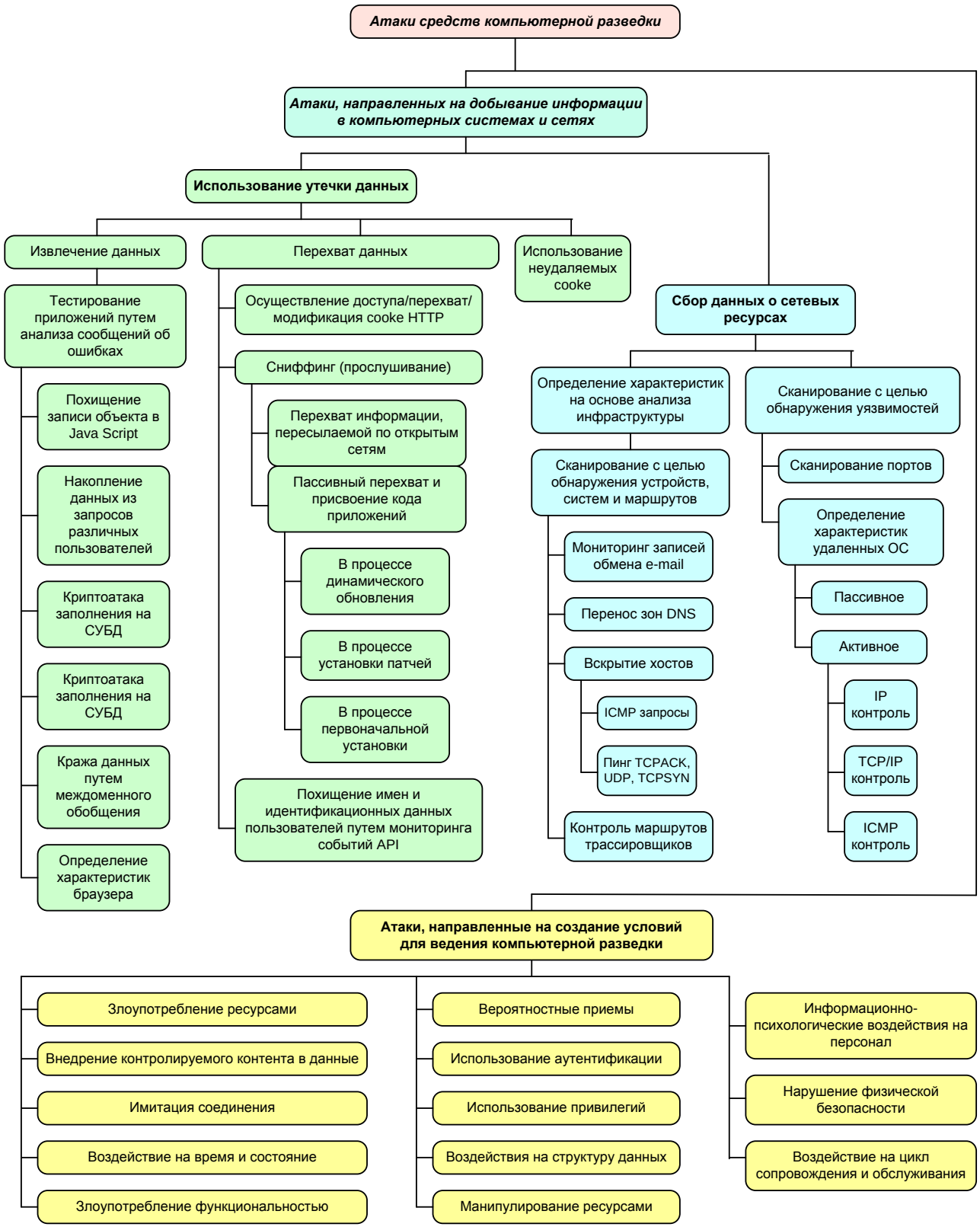


Рис. 12. Классификация атак средств компьютерной разведки [42]

3.3.3. Разведка по открытым источникам

При тестировании начальных уязвимостей информационных систем большую роль играет сбор информации об организации, в которой функционирует целевая информационная система, а также о персонале и лицах, принимающих решения. При сборе такой информации, в рамках тестирования, широко используются средства разведки по открытым источникам – в рамках проведения семантической и пользовательской компьютерной разведки. Классификация таких средств представлена на рис. 13. Более подробные данные о таких средствах представлены в работе [1].

Во многом повышение значимости разведки на основе анализа открытых источников обусловлено тем фактом, что порядка 10–15% необходимой информации имеется в Интернете уже в готовом виде (необходима только ее верификация), а остальные 85-90% информации могут быть получены в результате сравнения, анализа и синтеза разрозненных и разбросанных по разным источникам фактов. Естественно, что информация, полученная таким образом, нуждается в верификации.

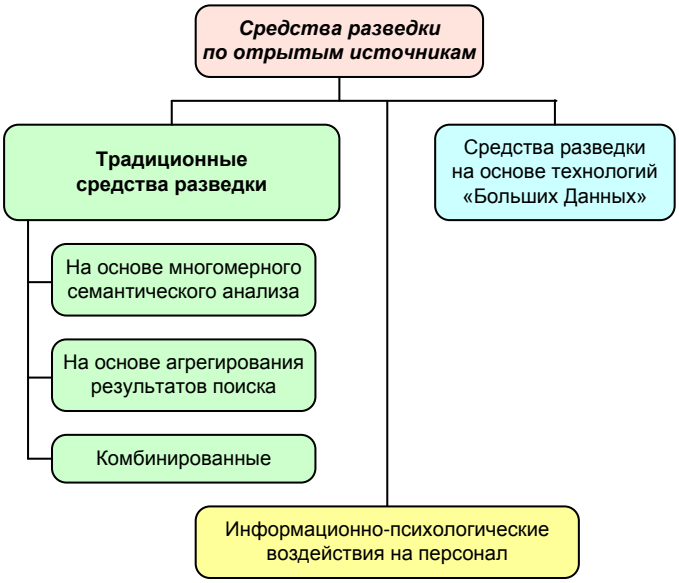


Рис. 13. Классификация средств разведки по отрытым источникам

Для решения задач анализа открытых источников используются аппаратно-программные средства, основу которых составляют алгоритмы поиска и семантического анализа. Специальные программы-роботы опрашивают сайты и извлекают из них нужную информацию, используя широкий спектр средств лингвистического, семантического и статистического анализа. Действуя автономно, такие программы анализа данных выявляют любую целевую информацию, как только она появится в Интернете.

Особенностью программ анализа данных на основе семантических поисковых алгоритмов является то, что они могут находить только ту информацию, которая в явном виде находится в документах, размещенных в сети Интернет, а уже потом, за счет анализа различных документов с совпадающим целевым

контентом, начинают «собирать» информационное наполнение запроса пользователей. Более интересным направлением развития средств разведки является анализ разнородных, изначально семантически не связанных между собой данных с целью выявления неслучайных совпадений или скрытых закономерностей и последующей их «привязкой» к объектам разведки. Такое направление получило развитие в рамках исследования проблемы «Больших данных» (Big Date).

Формирование глобального электронного, постоянно пополняющегося архива поведенческой активности самых различных субъектов, от отдельных государств и огромных компаний до небольших групп, и отдельных индивидуумов в сети Интернет послужило базисом появления Больших данных.

Анализ накопленного за последние годы опыта применения технологий Больших данных позволяет выделить несколько ключевых черт, отличающих Большие данные от всех других информационных технологий. К ним относится следующее [44].

- Огромные массивы разнородной информации о процессах, явлениях, событиях, объектах, субъектах и т. п., пополняемые непрерывно в режиме реального времени.
- Специально спроектированные программные платформы, где Большие данные любого объема могут храниться в удобном для вычислений виде. Отличительной чертой этих хранилищ является то, что структурированная и неструктурированная информация могут обрабатываться совместно, как единое целое.
- Наличие различного рода математического, прежде всего статистического инструментария для обработки Больших данных и получение результатов в виде, понятном для человека. Причем при анализе Больших данных используются не только традиционные методы математической статистики, но и интеллектуальные алгоритмы обработки данных.

Технологии Больших данных основаны, прежде всего, на методах статистического и интеллектуального анализа данных, применяемых на огромных, постоянно пополняемых массивах данных.

Технологии Больших данных позволяют [44]:

- проводить самые различные и сколь угодно подробные классификации той или иной совокупности людей, компаний, иных объектов по самым разнообразным признакам. Такие классификации обеспечивают точное понимание взаимосвязи тех или иных характеристик любого объекта – от человека до компании или организации, с теми или иными его действиями;
- осуществлять многомерный статистический математический анализ. Этот анализ позволяет находить корреляционные связи между самыми различными параметрами, характеристиками, событиями и т. п. Эти связи не отвечают на вопрос «почему?», но они указывают на вероятность, с которой при изменении одного фактора изменится и другой. В случае выявления корреляционных закономерностей в Больших дан-

ных стадия выявления первопричины отсутствует, а сразу выявляется закономерная связь различных факторов;
- прогнозировать. На основе классификаций и аналитических выкладок осуществляется прогнозирование, суть которого состоит в том, чтобы на основе выявленной корреляционной связи факторов определить наиболее целесообразный способ воздействия для того, чтобы один набор факторов, характеризующих тот или иной объект, лицо, компанию, событие и т. п., был преобразован в другой.

Более подробная информация об использовании технологий Больших данных при решении задач разведки представлена в работах [1, 44].

3.4. Атакующие информационно-технические воздействия

Атакующие ИТВ ориентированы на непосредственное воздействие на информацию, системы ее сбора, передачи, хранения, обработки и представления, а также на используемые в этих системах информационные технологии, как правило, с целью снижения уровня ИБ или эффективности функционирования. Применение атакующих ИТВ направлено на срыв выполнения информационной системой своих целевых задач.

Далее обзорно представлена классификация и основные типы атакующих ИТВ. Более подробная информация об атакующих ИТВ представлена в работе [1].

3.4.1. Классификация атакующих информационно-технических воздействий

Классификация средств и способов атакующих ИТВ представлена на рис. 14.

Атакующие ИТВ, в зависимости от их ориентированности на нарушение конкретного свойства ИБ, можно классифицировать на четыре основных типа:
- ориентированные на нарушение конфиденциальности информации;
- ориентированные на нарушение целостности информации;
- ориентированные на нарушение доступности информации;
- ориентированные на информационно-психологическое воздействие (компьютерное психотронное воздействие) на пользователей информационной системы.

По способу реализации ИТВ классифицируются на:
- алгоритмические:
  - эксплойты, ориентированные на управляющую программу информационной системы (ядро или модули операционной системы, драйвера, BIOS);
  - эксплойты, ориентированные на прикладные программы информационной системы (пользовательские приложения, серверные приложения, сетевые приложения, браузеры);
  - эксплойты, ориентированные на сетевые протоколы информационной системы;

- эксплойты, ориентированные на перевод информационной системы или управляемой ею технологической системы в нештатные или технологически опасные режимы функционирования;

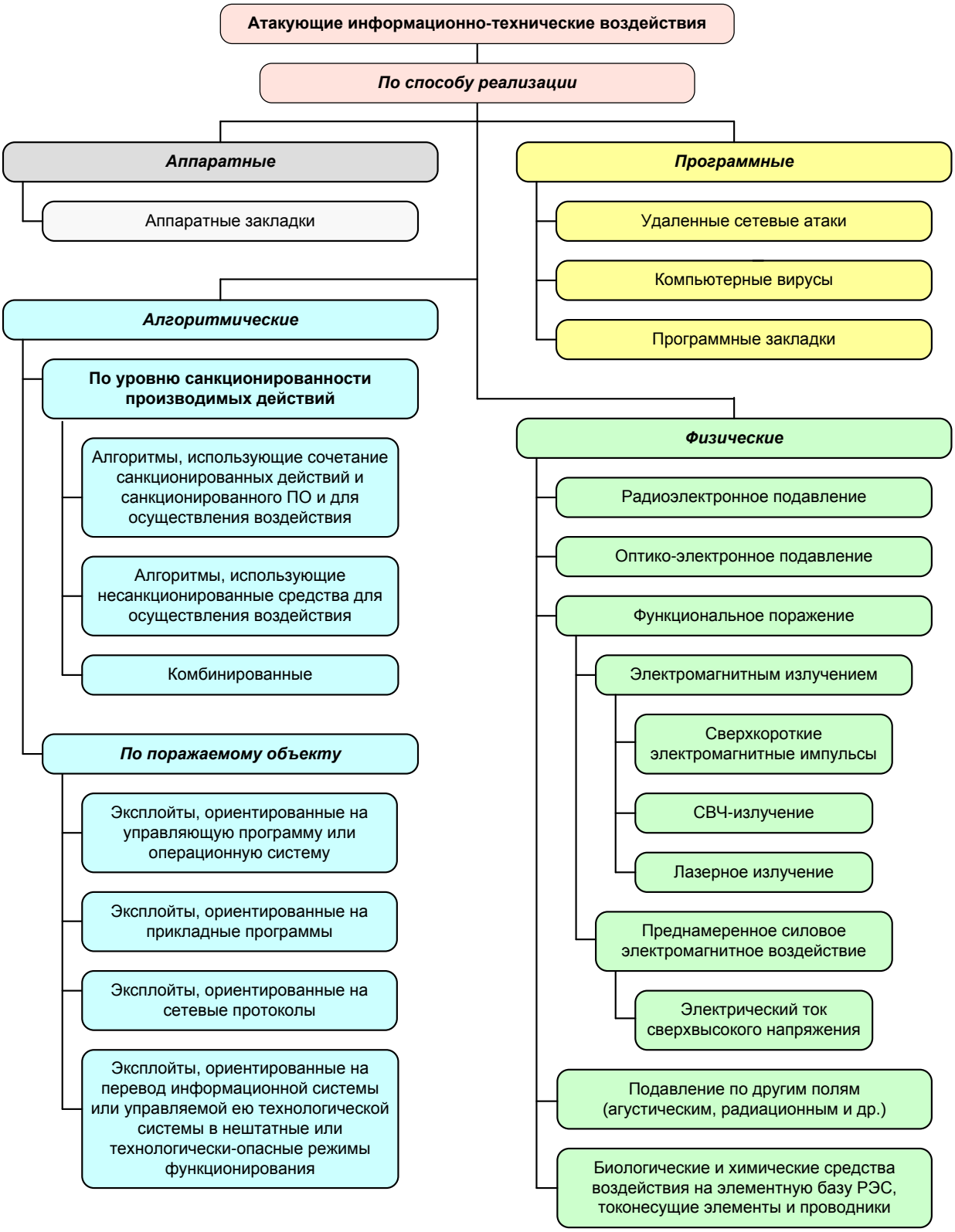


Рис. 14. Классификация средств и способов атакующих ИТВ

- программные:
  - компьютерные вирусы;
  - программные закладки;
  - нейтрализаторы тестовых программ и программ анализа кода;
- аппаратные:
  - аппаратные закладки;
- физические:
  - электромагнитные:
    - радиоэлектронное подавление;
    - оптико-электронное подавление;
    - функциональное поражение электромагнитным излучением (электромагнитные импульсы, СВЧ-излучение, лазерное излучение);
    - функциональное поражение преднамеренными силовыми электромагнитными воздействиями (электрический ток сверхвысокого напряжения);
  - по другим полям (акустическим, радиационным и др.);
  - биологические и химические средства воздействия на элементную базу РЭС, токонесущие элементы и проводники.

Рассмотрим более подробно основные широко распространенные атакующие ИТВ, которые могут быть использованы для тестирования объектов КИИ:

- удаленные сетевые атаки;
- компьютерные вирусы;
- программные закладки;
- аппаратные закладки.

3.4.2. Удаленные сетевые атаки

Удаленная сетевая атака – это атакующее информационно-техническое воздействие, осуществляемое по каналам связи, удаленным относительно атакуемой системы, субъектом и характерное для структурно- и пространственно-распределенных информационных систем.

Удаленные сетевые атаки можно классифицировать в соответствии с различными основаниями. Общая схема классификации удаленных сетевых атак представлена на рис. 15, а способов их осуществления – на рис. 16.

В настоящее время атаки типа «отказ в обслуживании» являются наиболее распространенными и наиболее опасными удаленными сетевыми атаками. Атака «отказ в обслуживании» направлена на блокировку доступа к объекту путем исчерпания его ресурсов. Классификация основных способов осуществления атаки «отказ в обслуживании» представлена на рис. 17. Подробная информация по этим атакам приведена в работе [1].

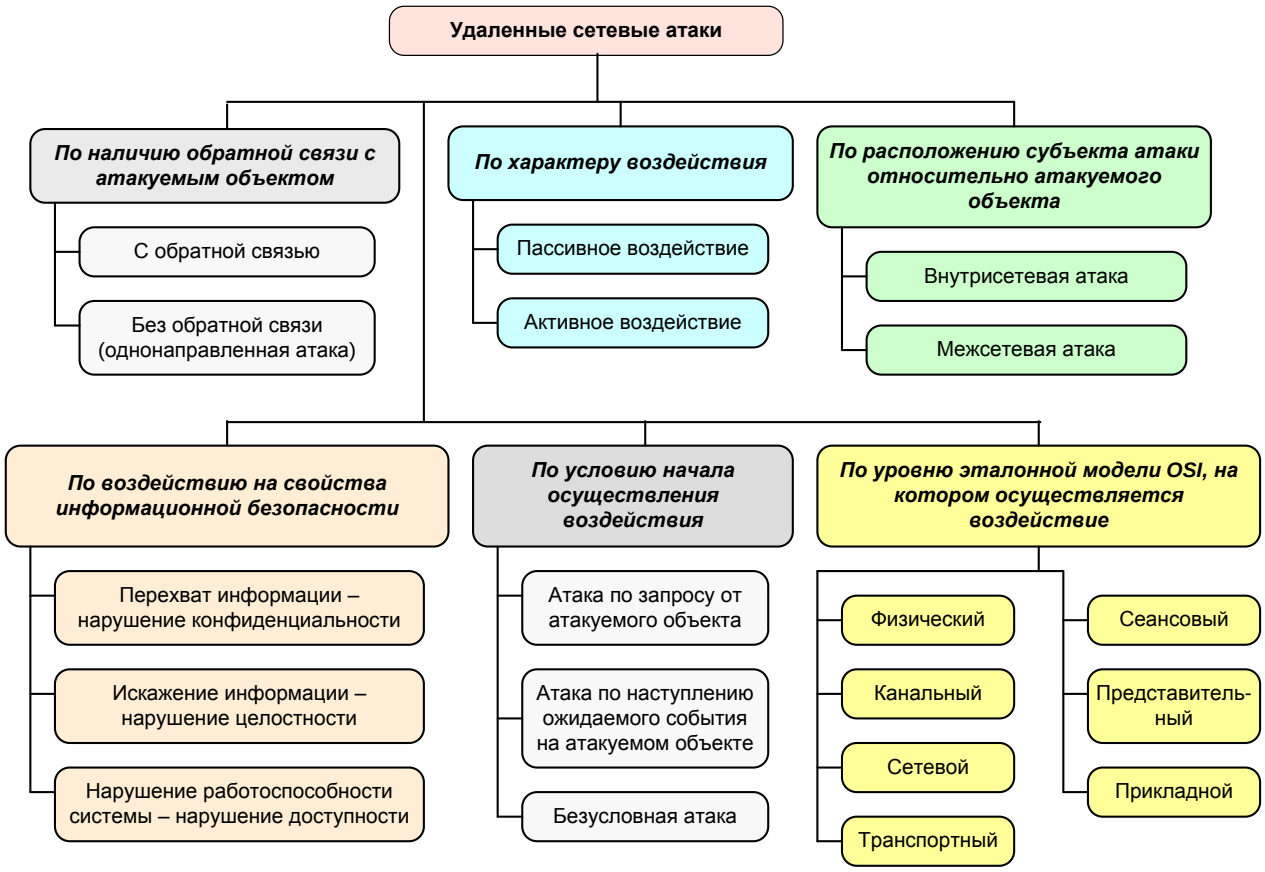


Рис. 15. Классификация удаленных сетевых атак

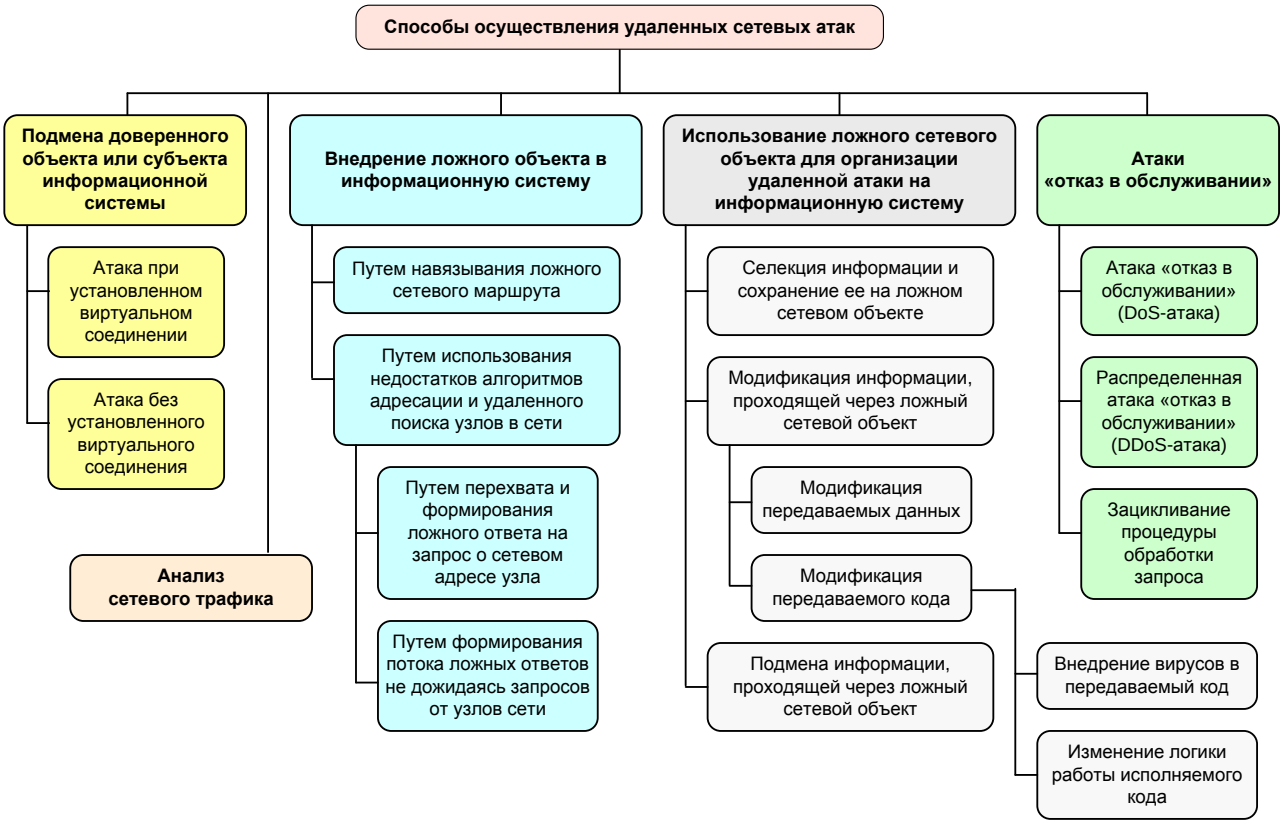


Рис. 16. Классификация способов осуществления удаленных сетевых атак

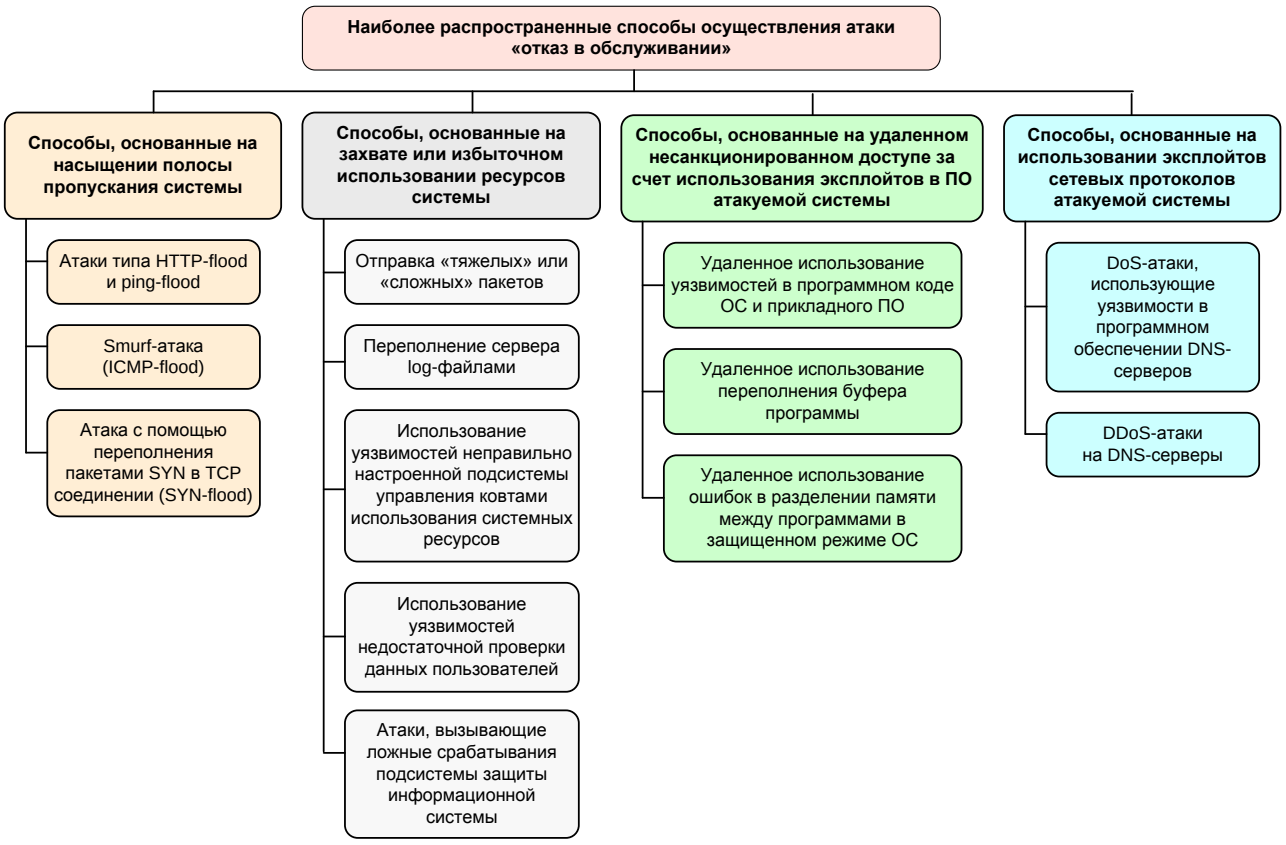


Рис. 17. Наиболее распространенные способы осуществления атаки «отказ в обслуживании»

3.4.3. Компьютерные вирусы

Несмотря на долгую историю компьютерной вирусологии, использование вирусов в качестве боевых средств информационно-технического воздействия начато сравнительно недавно. К первому случаю такого использования относится использование в 2010 г. вируса Stuxnet [1].

Вирус – программа, несанкционированно внедренная в информационную систему и способная осуществлять создание собственных дубликатов (не всегда совпадающих с оригиналом), несанкционированное самораспространение, несанкционированный доступ к информационным ресурсам, изменение логики функционирования зараженной программы, снижение качества или эффективности информационной системы.

Особенностью современных боевых вирусов является то, что они, как правило, являются комплексными продуктами и состоят из различных модулей, которые относятся к различным типам и ориентированы на решение конкретной задачи (модули типа «классический вирус» – для саморазмножения в информационной системе, модули типа «червь» – для распространения по сети, модуль типа «троян» – для организации дестабилизирующего воздействия).

Классификация атакующих средств на основе компьютерных вирусов представлена на рис. 18.

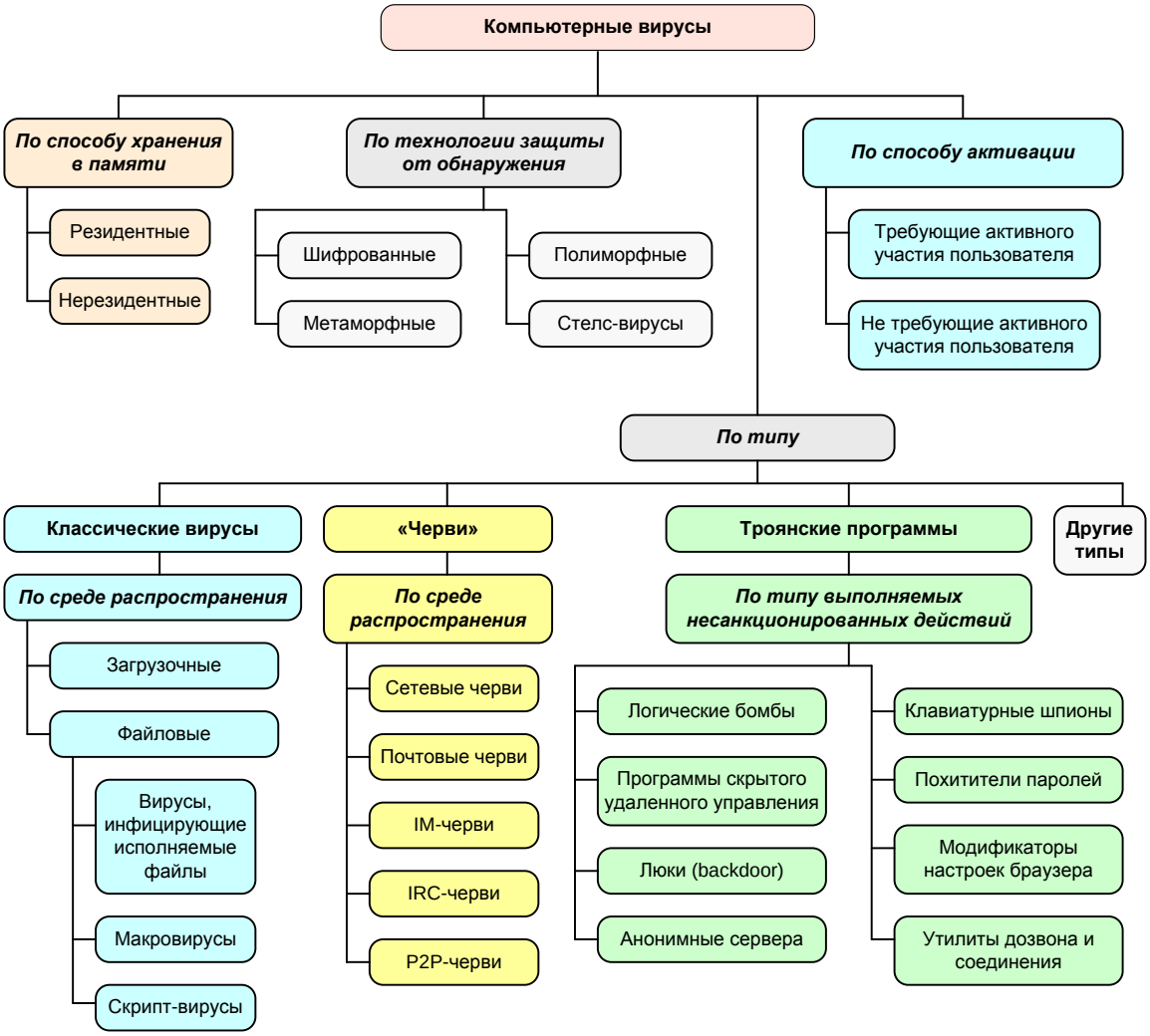


Рис. 18. Классификация компьютерных вирусов

Средства ИТВ на основе вирусов обладают следующими особенностями функционирования относительно других «непрофессиональных» вирусных средств [1]:

- избирательность цели и действий;
- использование уязвимостей, в том числе уязвимостей 0-дня, закладок и скрытых каналов;
- маскировка, скрытность, криптозащита, самоликвидация;
- широкая функциональность в плане решения целевых задач;
- гибкая система саморазмножения;
- инфраструктурная поддержка, обновление и управление;
- масштабируемость, наличие СУБД-атак;
- высокое качество кода и возможности обработки некорректных ситуаций.

Более подробная информация о вирусных средствах ИТВ представлена в работе [1].

3.4.4. Программные закладки

Программная закладка – скрытно внедренная в защищенную информационную систему программа, либо намеренно измененный фрагмент про-

граммы, которые позволяют осуществить несанкционированный доступ к ресурсам системы на основе изменения свойств подсистемы защиты [45]. При этом в большинстве случаев закладка внедряется самим разработчиком ПО для реализации в информационной системе некоторых сервисных или недекларируемых функций.

Классификация программных закладок представлена на рис. 19.

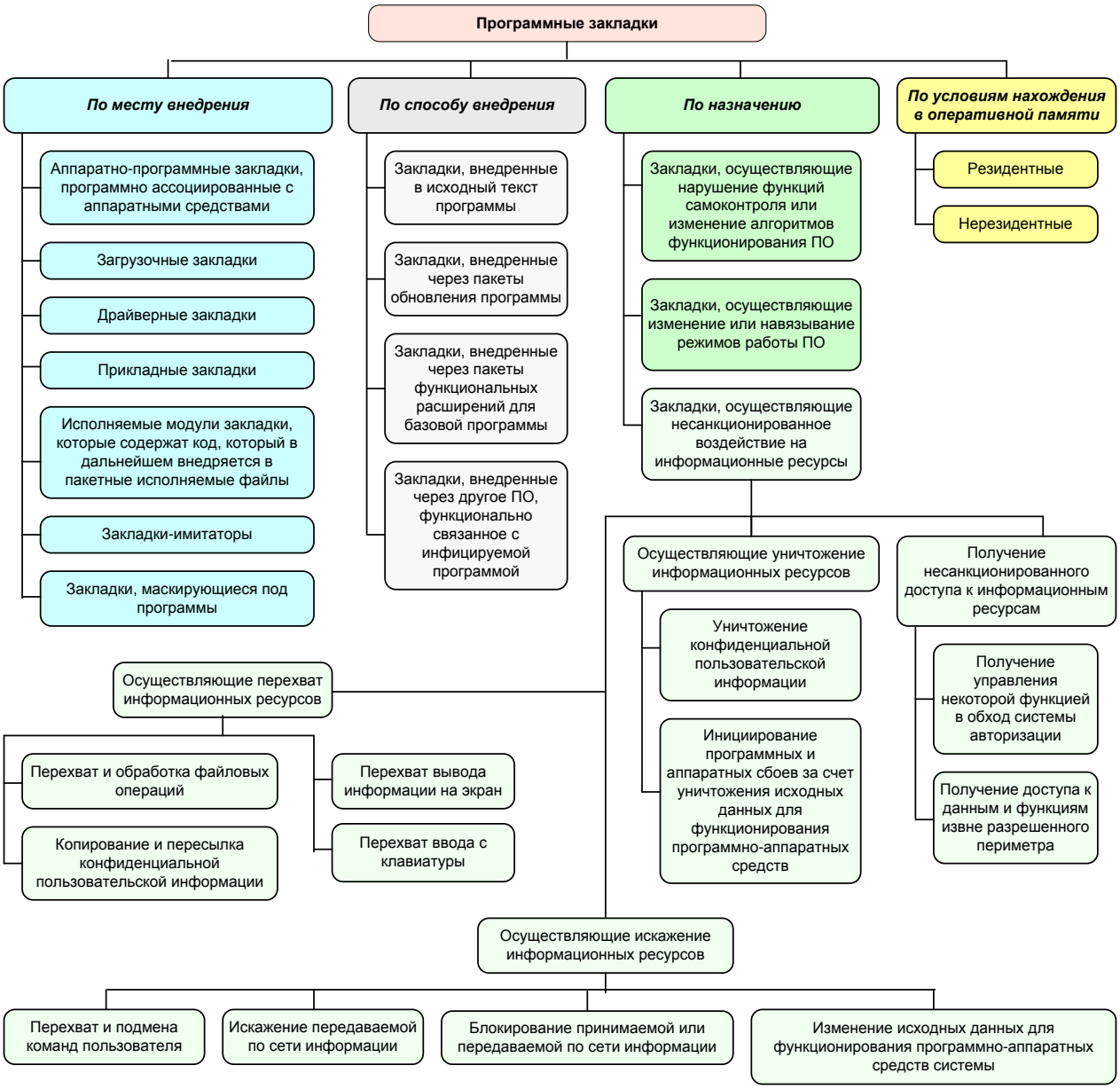


Рис. 19. Классификация программных закладок

Программные закладки, получая несанкционированный доступ к данным в памяти информационной системы, перехватывают их. После перехвата эти данные копируются и сохраняются в специально созданных разделах памяти или передаются по сети. Программные закладки, подобно вирусам, могут искажать или уничтожать данные, но, в отличие от вирусов, деструктивное действие таких программ, как правило, более выборочно и направлено на конкретные данные. Довольно часто программные закладки играют роль перехватчиков па-

ролей, сетевого трафика, а также служат в качестве скрытых интерфейсов для входа в систему. Однако, в отличие от вирусов, программные закладки не обладают способностью к саморазмножению, они встраиваются в ассоциированное с ними программное обеспечение и латентно функционируют вместе с ним. При этом особенностью закладок, внедренных на стадии разработки ПО, является то, что они становятся фактически неотделимы от прикладных или системных программ информационной системы [46].

Как и вирус, программная закладка должна скрывать свое присутствие в программной среде информационной системы. Однако программные закладки невозможно обнаружить при помощи стандартных антивирусных средств, их выявление возможно только специальными тестовыми программами, выявляющими аномальное поведение и недекларируемые возможности ПО. В связи с этим средства маскировки программных закладок преимущественно ориентированы на противодействие отладчикам программ, анализаторам кода и дисассемблерам. В качестве одного из широко применяемых способов маскировки является обфускация (запутывание) программ, в которые внедрена закладка [46].

3.4.5. Аппаратные закладки

Аппаратная закладка – электронное устройство, скрытно внедряемое к остальным элементам, которое способно вмешаться в работу аппаратных или технических средств информационной системы.

Результатом работы аппаратной закладки может быть как полное выведение системы из строя, так и нарушение ее нормального функционирования, например, несанкционированный доступ к информации, ее изменение или блокирование [47].

Классификация аппаратных закладок приведена на рис. 20 [1].

Схематическая сложность современного микроэлектронного оборудования, тенденции к миниатюризации его элементов ведут к тому, что производители такого оборудования могут бескомпроматно и практически неограниченно наращивать функциональные возможности аппаратных закладок, функционирующих в интересах тестирования такого оборудования, а при подключении устройств к глобальной сети – осуществлять обновление алгоритма их функционирования, а также условий срабатывания. Краткая характеристика технологий современных аппаратных закладок представлена в таблице 1 [48].

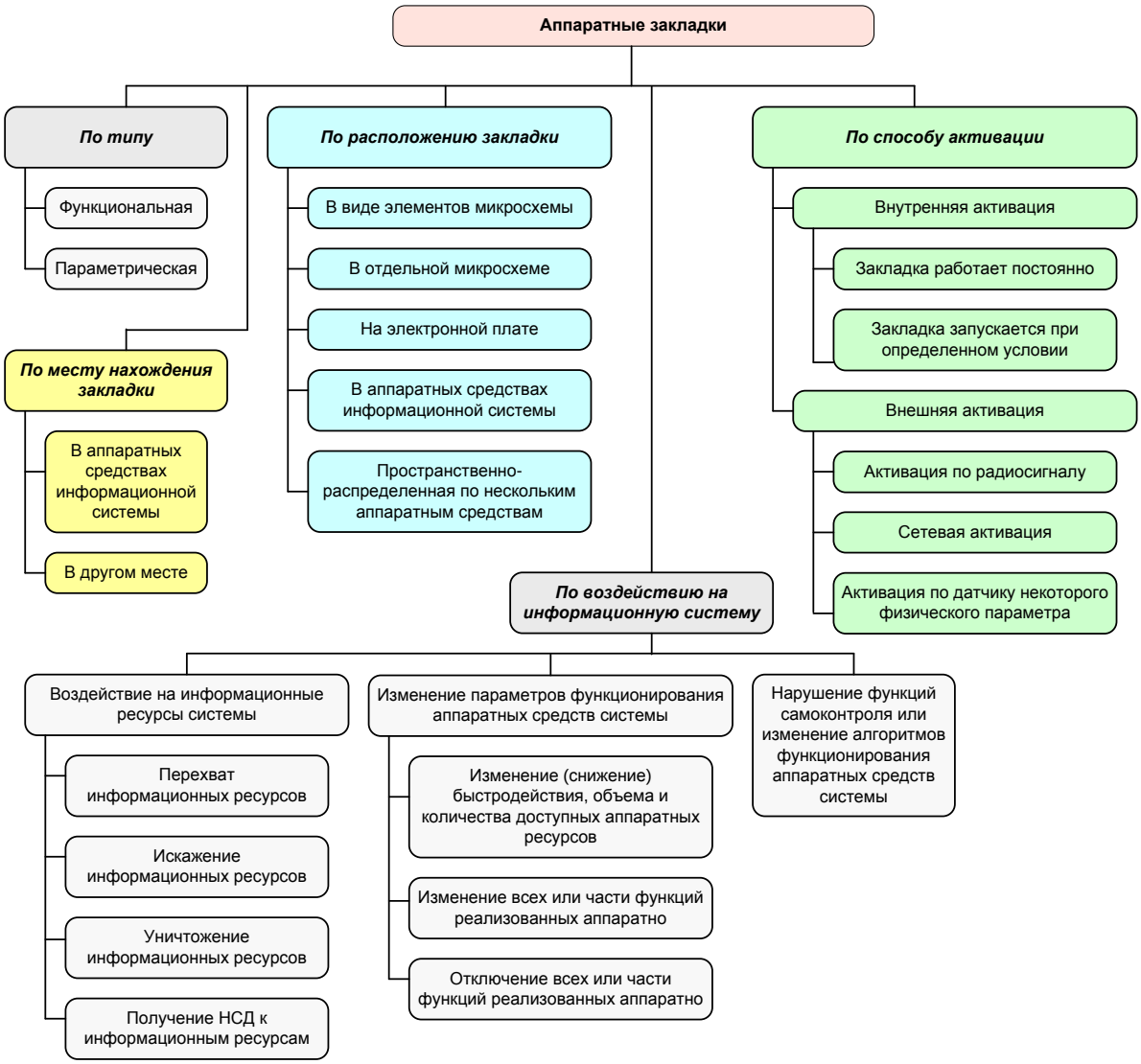


Рис. 20. Классификация аппаратных закладок

Таблица 1 – Технологии современных аппаратных закладок [48]

Методы внедрения	Методы обнаружения	Методы маскировки
Встраивание закладок в технологию микроядра управления в современных СБИС, построенного на уникальном списке команд (управление основной работой и блокировка и замена неисправных узлов для продления срока службы СБИС)	Технологии послойного сканирования кристаллов	Механизм технологической защиты топологии кристалла от послойного сканирования (впервые внедрен в i486)
	Вычитывание и дизассемблирование аппаратно доступных микрокодов	Размещение микроядер с закладками и ресурсов памяти в области, недоступной пользователю. Шифрование (мутирование) участков кода, антитрассировка
Виртуализация вычислений	Анализ контента проходящих по сети данных	
Встраивание целевых микроядер и узлов, реализующих стратегию влияния	Мониторинг аномальной активности платформы. Радио-мониторинг. Электромагнитный контроль.	

3.5. Классификация основных средств информационно-технических воздействий

Основные средства ИТВ можно классифицировать по способу реализации.

1) Алгоритмические (атакующие):
   - эксплойты, ориентированные на управляющую программу информационной системы (ядро или модули операционной системы, драйвера, BIOS);
   - эксплойты, ориентированные на прикладные программы информационной системы (пользовательские приложения, серверные приложения, сетевые приложения, браузеры);
   - эксплойты, ориентированные на сетевые протоколы информационной системы;
   - эксплойты, ориентированные на перевод информационной системы или управляемой ею технологической системы в нештатные или технологически опасные режимы функционирования.
2) Программные:
   - атакующие:
     - компьютерные вирусы;
     - программные закладки;
     - нейтрализаторы тестовых программ и программ анализа кода;
   - обеспечивающие:
     - программные средства для моделирования боевых действий;
     - программные средства компьютерной разведки в телекоммуникационной части информационного пространства;
     - программные средства ведения разведки на основе открытых источников в семантической части информационного пространства;
   - оборонительные:
     - программные средства антивирусной защиты;
     - системы обнаружения и предотвращения вторжений;
     - программные средства криптографической защиты;
     - программные стеганографические средства обеспечения конфиденциальности, скрытности и целостности информационных ресурсов;
     - средства тестирования ПО и анализа кода для выявления программных закладок и недекларируемых возможностей;
     - средства создания ложных объектов и ресурсов в информационном пространстве.

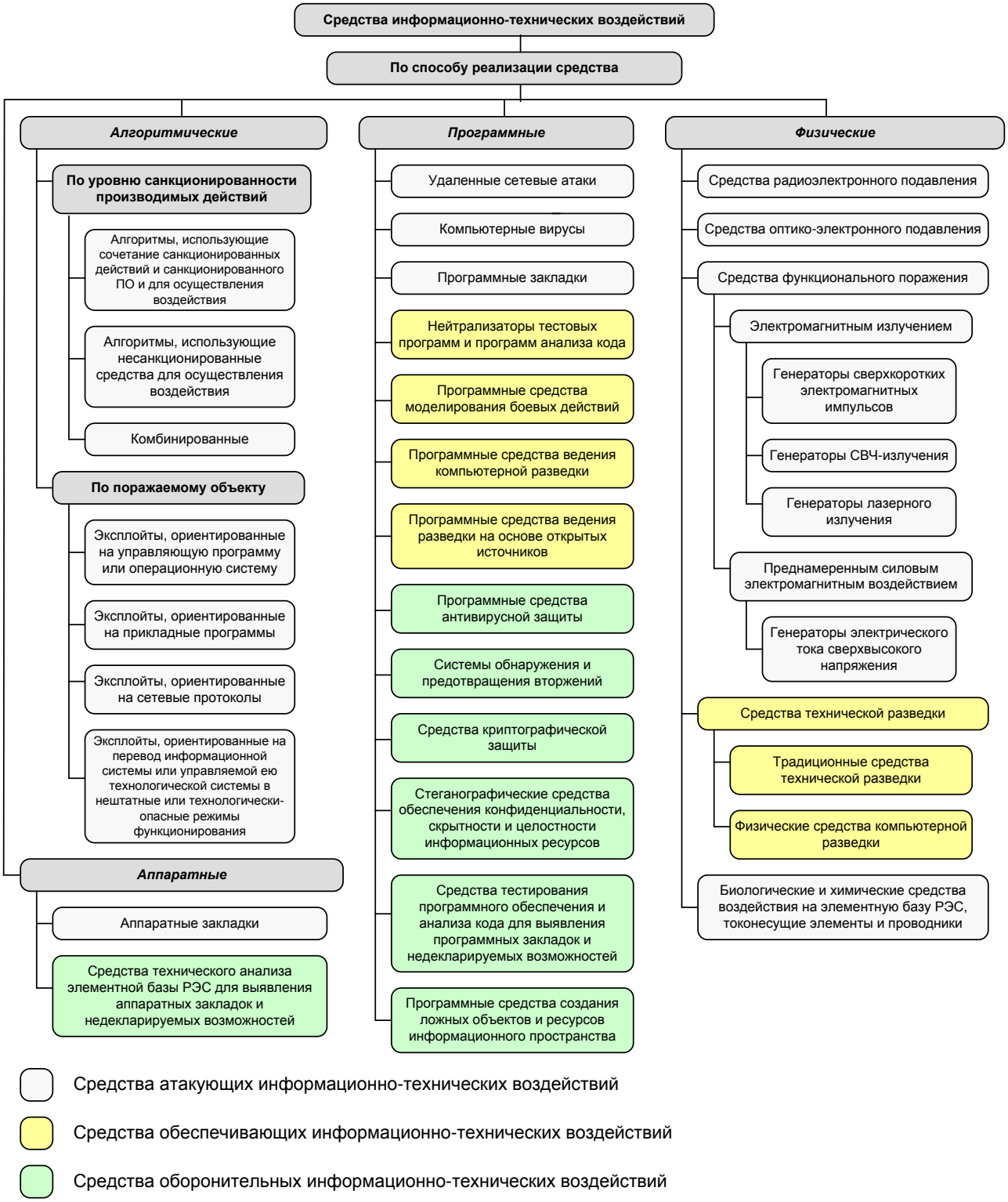


Рис. 21. Классификация средств ИТВ для тестирования объектов КИИ

3) Аппаратные:
   - атакующие:
     - аппаратные закладки;
   - оборонительные:
     - средства технического анализа элементной базы РЭС для выявления аппаратных закладок и недекларируемых возможностей.

4) Физические:
   - атакующие:
     - средства радиоэлектронного подавления;
     - средства оптико-электронного подавления;
     - средства функционального поражения электромагнитным излучением (генераторы электромагнитных импульсов, генераторы СВЧ-излучения, генераторы лазерного излучения);
     - средства и комплексы функционального поражения преднамеренными силовыми электромагнитными воздействиями (генераторы электрического тока сверхвысокого напряжения);
     - биологические и химические средства воздействия на элементную базу РЭС, токонесущие элементы и проводники (например, графитовые бомбы).
   - обеспечивающие:
     - средства технической разведки (в том числе и средства компьютерной разведки).

Общая схема классификации средств ИТВ представлена на рис. 21.

Отдельно необходимо отметить следующее. К средствам технической разведки, представленным в данной классификации, относятся те средства, которые добывают информацию об атакующих средствах ИТВ и способах его применения, т.е. являются средствами обеспечивающего ИТВ. Средства технической разведки могут оказывать воздействие на информационные системы как путем пассивных воздействий, направленных на добывание информации, что, как правило, связанно с нарушением ее конфиденциальности, так и путем активных действий (атак), направленных на создание условий, которые благоприятствуют добыванию информации.

Выводы по третьей главе

Подводя итог, можно сделать следующие краткие обобщенные выводы.

1) Для аудита уровня защищенности объектов КИИ в технической сфере может быть использовано тестирование аппаратно-программных средств КИИ путем воздействия на них специальными средствами и способами ИТВ. Причем данные средства и способы ИТВ, а также сценарий их применения должны соответствовать тем средствам и способам ИТВ, а также тем сценариям, которые предполагаются к применению потенциальным противником.

2) Средства и способы специальных ИТВ, предназначенных для тестирования объектов КИИ, целесообразно классифицировать на оборонительные; обеспечивающие и атакующие. В рамках тестирования объектов КИИ должны реализовываться сценарии поэтапного интегрального применения указанных типов ИТВ для всеобъемлющего анализа аппаратно-программной инфраструктуры объектов КИИ, вскрытия ее уязвимостей в технической сфере, а также для формирования предложений по модернизации оборонительных средств и способов ИТВ, для повышения устойчивости объектов КИИ в условиях ведения информационного противоборства.

3) Оборонительные средства (средства антивирусной защиты, системы обнаружения и предотвращения вторжений, средства криптографической защиты и т. д.) в подавляющем числе работ рассматриваются как основной элемент обеспечения ИБ, но не как средства оборонительных ИТВ. Вместе с тем, на взгляд автора, оборонительные средства ИТВ должны рассматриваться не как самодостаточные, а как важная, но при этом только составная часть системы защиты КИИ, которая должна действовать совместно с обеспечивающими и атакующими средствами ИТВ, использующимися для тестирования эффективности обороны. В идеальном случае оборонительные, обеспечивающие и атакующие ИТВ должны быть интегрированы в единый комплекс тестирования защищенности КИИ. Целью такого комплекса является непрерывное наращивание возможностей тестирования обеспечивающих и атакующих средств ИТВ в интересах имитации передовых возможностей сил информационных операций потенциального противника. В дальнейшем, по итогам анализа результатов тестирования, необходимо проводить совершенствование оборонительных средств ИТВ с учетом выявленных уязвимостей объектов КИИ.

4) Создание единого комплекса тестирования защищенности КИИ позволит гибко и своевременно оценивать уязвимость отечественной КИИ к новейшим разработкам в области обеспечивающих и атакующих ИТВ потенциального противника, своевременно выявлять новые уязвимости КИИ в технической сфере, а также формировать научно-обоснованную политику совершенствования средств защиты КИИ, с учетом наиболее актуальных угроз.

4. Тестирование критической инфраструктуры специальными информационно-психологическими воздействиями

При тестировании КИИ в организационной, социальной и психологической сферах используются специальные способы и средства ИПВ.

Исследования в области тестирования на проникновение [13-17], а также психологического состояния операторов ОТС [49-51] позволяют сделать следующий вывод. Человек (ЛПР или оператор ОТС) в структуре КИИ является, с одной стороны, «ключевым звеном» системы, т.к. именно за ним остается приоритет в принятии окончательных решений, но, с другой стороны, он же является наиболее «слабым звеном» системы, так как подвержен воздействию ИПВ, которые могут принудить его к сознательному или бессознательному нарушению политики ИБ. В связи с этим актуальным и важным направлением аудита ИБ объектов КИИ является проверка психологической устойчивости ЛПР и операторов ОТС путем их тестирования специальными средствами и способами ИПВ.

Одной из первых работ, в которой исследовались вопросы зависимости уровня ИБ объектов КИИ от ИПВ на персонал, была работа В.И. Емелина [49]. Исследования по направлению обеспечения ИБ в условиях социоинженерных атак ведет А.Л. Тулупьев [73-78]. Системный обзор вопросов информационно-психологической безопасности представлен в работе И.Ф. Кефели и Р.М. Юсупова [125]. В дальнейшем материале этой главы предложено авторское в*и*дение развития данных вопросов с учетом наработок, представленных в работе [1].

4.1. Общее понятие об информационно-психологическом воздействии

Информационно-психологическое воздействие – информационное, психотронное или психофизическое воздействие на психику человека или группы, оказывающее влияние на восприятие ими реальной действительности, в том числе на их поведенческие функции, а в некоторых случаях – и на функционирование органов и систем человеческого организма [56].

Любой человек как личность, активный социальный субъект, носитель определенного мировоззрения, обладающий определенным правосознанием и менталитетом, духовными идеалами и ценностными установками, может быть подвергнут непосредственному ИПВ, которое, трансформируясь через его поведение, действия (или бездействие), оказывает влияние на социальные объекты разного уровня общности, различной системно-структурной и функциональной организации. Таким образом, с помощью ИПВ можно влиять не только на индивидуальное сознание, но и на групповое, массовое и общественное сознание. Причем это влияние может носить как позитивный, так и негативный характер [56].

Варианты ИПВ на персонал объектов КИИ представлены на рис. 22 [79].

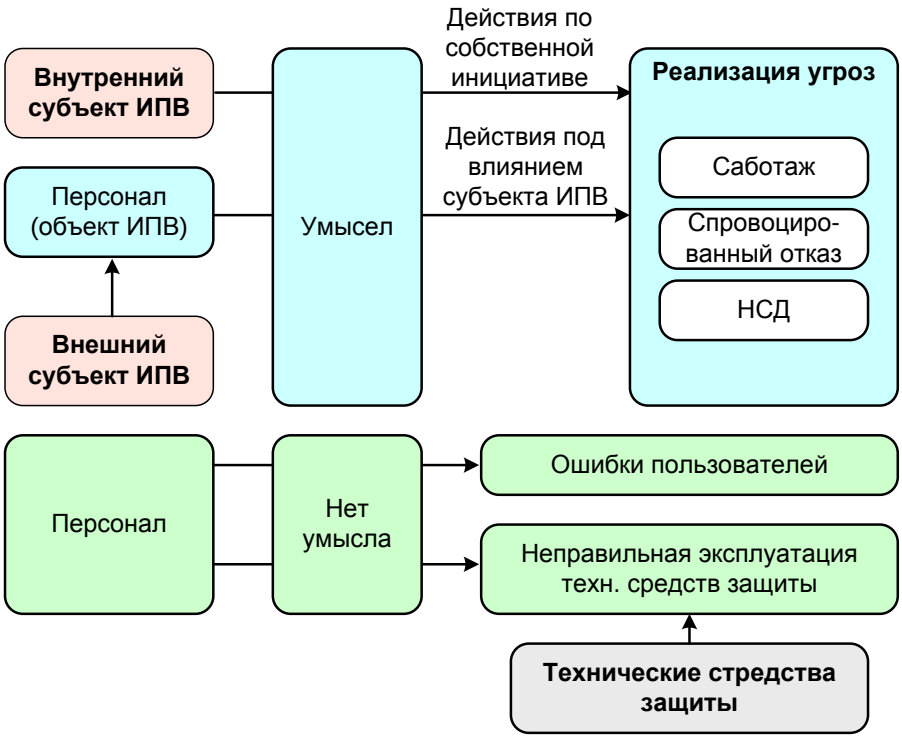


Рис. 22. Варианты ИПВ на персонал объектов КИИ [79]

Воздействие ИПВ на персонал объектов КИИ решает следующие задачи:

- принуждение к нарушению организационно-нормативных мер и политики безопасности;
- принуждение к нарушению конфиденциальности, доступности и целостности информации;
- нарушение социально-психологических процессов нормального функционирования коллективов объектов КИИ;
- дезорганизации системы управления объектами КИИ за счет подрыва авторитета ЛПР, формирование условий, направленных на отказ отдельных лиц и коллективов выполнять приказы и распоряжения вышестоящих ЛПР, склонение их к саботажу.

Объектами ИПВ могут выступать [56]:

- личность, как активный социальный субъект, в том числе конкретные представители органов управления КИИ, органов правопорядка и безопасности, работники государственных и негосударственных организаций, учреждений и предприятий, деятельность которых имеет или может иметь важные для объектов КИИ последствия;
- система формирования и функционирования духовной сферы, общественного сознания и общественного мнения, в том числе: системы образования и подготовки кадров; системы распространения социально значимой информации; системы распространения социокультурных ценностей и т. п.;
- социальные группы и объединения людей как компоненты социальной структуры КИИ, обладающие групповым сознанием, в том числе по-

литические, профессиональные, национально-этнические, демографические, религиозные и другие группы;
- органы власти, государственного и военного управления;
- общественные и политические организации, общественно-политические движения и объединения граждан на различной основе, в которые входят представители персонала объектов КИИ;
- силовые министерства и ведомства;
- государство и общество, население страны в целом как социально-историческая общность людей, обладающая своим общественным сознанием и выступающие как мета-система по отношению к объектам КИИ.

В качестве субъектов ИПВ можно рассматривать, прежде всего, силы информационных операций недружественных стран, а также лица и группы, ведущие диссидентскую и подрывную работу или сотрудничающие со специальными службами других государств.

В зависимости от преследуемых целей ИПВ, как правило, осуществляется на конкретные сферы индивидуального, группового, массового и общественного сознания [56]:

- мотивационную (убеждения, ценностные ориентации, влечения, желания), когда надо оказать влияние на людей для побуждения их к определенным действиям;
- познавательную (ощущения, восприятия, представления, воображение, память и мышление), когда необходимо изменить в нужную сторону представления, характер восприятия вновь поступающей информации и в итоге – «картину мира» человека;
- эмоциональную (эмоции, чувства, настроения, волевые процессы), когда под прицелом находятся внутренние переживания и волевая активность людей;
- коммуникативную (общение и взаимоотношения, взаимодействие, межличностное восприятие) с целью создания социально-психологического комфорта или дискомфорта, побуждения людей сотрудничать либо конфликтовать с окружающими.

Основные принципы подготовки и применения ИПВ [53]:

- подготовка ИПВ начинается заблаговременно, скрытно, тщательно, с учетом индивидуальных и социально-психологических особенностей объектов воздействия;
- ИПВ планируют и проводят с учетом выявленных слабых мест в организационно-нормативных мерах, политики безопасности, морально-психологическом состоянии отдельных лиц и коллектива, с учетом особенностей складывающейся обстановки, имеющихся сил и средств;
- различные ИПВ проводят по единому плану, согласовывают между собой, а также с общей целью;
- силы и средства ИПВ используются массированно, комплексно и разнообразно.

Мероприятия ИПВ проводят ради внедрения в сознание отдельных лиц и коллективов конкретных взглядов, убеждений или лозунгов, мотивов недоверия или неудовлетворения действиями своего руководства, осознания своего неблагоприятного положения, угрозы жизни и благополучию родственников и для введения их в заблуждение, обмана, склонения к сотрудничеству [53].

При разработке и проведении ИПВ целесообразно использовать следующие основные принципы, разработанные специалистами сил психологических операций США, в рамках концепции «стратегических коммуникаций» [55]:

- *квалифицированное руководство* – подразумевает четкое представление руководителями конечных целей и задач проводимой операции;
- *правдоподобие* – предусматривает действия, восприятие и объяснение, которые должны вызывать доверие у целевой аудитории;
- *доступность* – учет психологических особенностей, культуры, образа жизни, социальных взаимоотношений целевой аудитории, лингвистического, исторического, религиозного, природного и других объективных факторов;
- *диалог* – ИПВ, проводимое в форме многостороннего обмена мнениями, способствует взаимопониманию и установлению доверительных отношений с объектом воздействия;
- *масштабность* – предусматривает отсутствие временных или пространственных ограничений на ИПВ;
- *согласованность* – подразумевает согласованные, интегрированные на всех уровнях в единую систему действия по единому замыслу и плану на всех уровнях иерархии как по «вертикали» – от тактического до стратегического, так и по «горизонтали» – в пределах одного уровня;
- *целенаправленность* – направленность всей совокупности ИПВ на получение конкретного заданного результата;
- *непрерывность* – предполагает непрерывный процесс ИПВ, для успешного осуществления которого необходимо наличие постоянной обратной связи между планированием и действиями с одной стороны, и анализом с оценкой результатов этих действий – с другой.

Реализация совокупности ИПВ в виде единой психологической операции, в соответствии с концепцией «стратегических коммуникаций», включает в себя следующие этапы [55]:

- уточнение целей операции;
- определение целевой аудитории и желаемого поведенческого эффекта объекта воздействия;
- всесторонний анализ аудитории и определение политических, социальных и идеологических установок;
- формулирование основных целей для отдельных ИПВ;
- согласование отдельных ИПВ по времени, месту, объектам воздействия и целям операции;
- реализация согласованных ИПВ;
- оценка результатов и корректировка планов последующих ИПВ.

При этом, при проведении отдельного ИПВ выделяют три этапа [53]:

- *операциональный*, когда субъектом осуществляется ИПВ на объект;
- *процессуальный*, когда имеет место принятие (одобрение) или непринятие (неодобрение) данного воздействия объектом;
- *заключительный*, когда проявляются ответные реакции как следствие перестройки психики объекта воздействия.

Перестройка психики под влиянием ИПВ может быть различной как по широте, так и по временной устойчивости. По первому критерию различают парциальные изменения, т. е. изменения какого-нибудь одного психологического качества (например, мнения человека о конкретном явлении) и более общие изменения психики, т. е. изменения ряда психологических качеств индивида (или группы). По второму критерию изменения могут быть кратковременными и длительными [53].

ИПВ может осуществляться с помощью различных методов (приемов, форм, методик) и средств, б*о*льшая часть из которых, непрерывно развиваясь и совершенствуясь, превратилась сегодня в сложные технологии воздействия на психику людей, обобщенно называемые в специальной литературе *психотехнологиями*. Так, например, к психотехнологиям относятся современные информационные технологии воздействия на индивидуальное, групповое, массовое и общественное сознание с использованием телевизионной и радиовещательной техники, видео- и аудиопродукции, а также компьютерные технологии высокого уровня, позволяющие диагностировать и корректировать психическое и физическое состояние человека путем прямого доступа в подсознание [56].

При этом, психология, как наука, в рамках подготовки и применения ИПВ решает следующие задачи [54]:

- указывает на те особенности человеческой и групповой психики, которые целесообразно подвергнуть воздействию;
- обеспечивает эффективные методы оценки психологического состояния отдельных лиц и групп;
- дает рекомендации специалистам, применяющим ИПВ по планированию операций;
- вырабатывает критерии и методы оценки результативности ИПВ на людей.

Создавая научный фундамент ИПВ, психологи западных стран опираются на достижения различных психологических школ. При этом за основу принимаются следующие основные положения [54]:

- о решающей роли бессознательного в детерминации человеческого поведения, о функционировании механизмов психологической защиты и способах их преодоления (психоанализ);
- о рефлекторном закреплении («якорении», «зомбировании») определенным образом соотносящихся восприятий, переживаний, действий; о внушающей силе структуры, эмоционального тона, пространственно-временных характеристик информации (бихевиоризм, нейролингвистическое программирование);

- о роли «ментальных схем» в восприятии человеком окружающего мира, происходящих событий и информации (когнитивная психология);
- о структуре и динамике потребностей человека (гуманистическая психология) и др.

Психология помогает организаторам ИПВ выявлять наиболее слабые звенья в морально-психологическом состоянии отдельных лиц и групп, а также научно обоснованно строить тактику психологического давления на них. Она рекомендует широко использовать в этих целях политические, национальные, социальные, религиозные противоречия; трудности (сложные условия труда, голод, холод, плохое материально-техническое обеспечение и др.); распространять слухи и дезинформацию и др.

4.2. Общая классификация информационно-психологических воздействий

Средства и способы ИПВ могут быть классифицированы с точки зрения физической сущности, принципов и механизмов воздействия (рис. 23) [56, 57].

1) Средства и способы психотронного ИПВ.

- Генераторы электромагнитных излучений, преимущественно СВЧ- и КВЧ-излучений, средства биорезонансной стимуляции работы головного мозга.
- Генераторы специальных излучений.
- Генераторы инфразвука и ультразвука.
- Световые излучатели в видимом, инфракрасном и ультрафиолетовом диапазонах.
- Генераторы лазерного излучения.
- Компьютерные технологии, в т. ч. компьютерные игры, а также средства дополненной и виртуальной реальности.

2) Средства и способы психофизического ИПВ.

- *Средства и способы предъявления неосознаваемой акустической информации*.
- *Средства и способы предъявления неосознаваемой зрительной информации*. Предполагается, что визуальные средства, в отличие от вербальных, позволяют человеку практически мгновенно воспринимать запрограммированное информационно-психологическое воздействие (хотя сработать оно может значительно позднее). Причем это воздействие является более глубоким и долговечным, поскольку визуальные системы влияют не только на интеллект, но и на эмоционально-чувственный базис человека.
- *Средства и способы предъявления неосознаваемой комбинированной информации.*
- *Гипнотические способы ИПВ*, основанные на выявленном факте, что соответствующими внушениями в гипнотическом состоянии можно программировать человека на выполнение тех или иных действий.

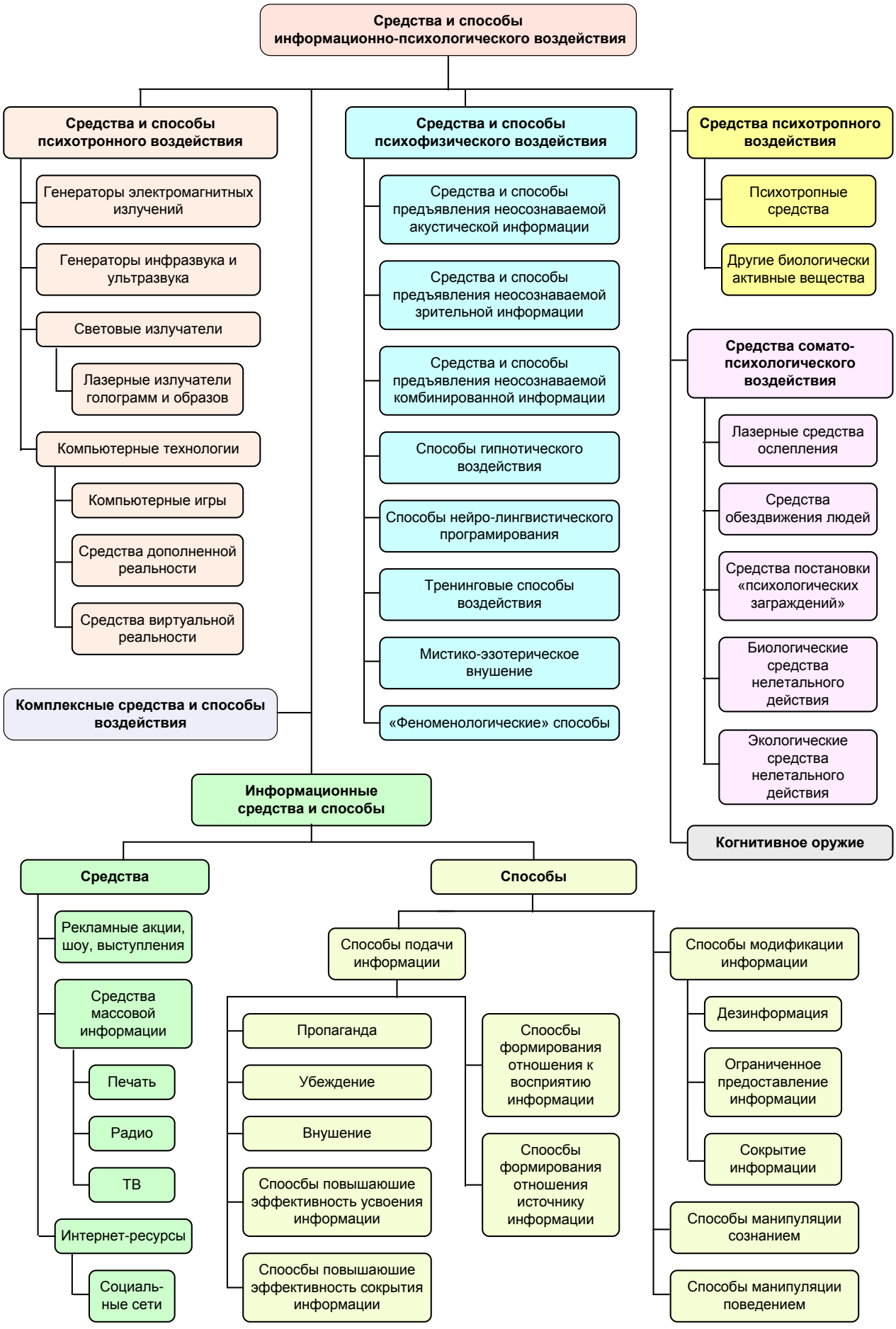


Рис. 23. Классификация средств и способов ИПВ [56, 57]

- *Способ нейролингвистического программирования* – особая психотерапевтическая техника, сутью которой является кодирование (программирование) человека как вербальными «формулами поведения», так и невербальными (мимика, пантомимика и т. д.) способами воздействия.
- *Тренинговые способы ИПВ* – способы регуляции психического состояния человека, такие как: управление вниманием, оперирование чувственными образами, словесные внушения, регуляция мышечного тонуса, управление ритмом дыхания.
- *Мистико-эзотерическое внушение*.
- *«Феноменологические» способы ИПВ* – неосознаваемое информационное взаимодействие через органы чувств путем применения методов психофизиологии и сенсорной физиологии человека.

3) Психотропные средства ИПВ:
- Психотропные средства.
- Другие биологически активные вещества, оказывающие преимущественно влияние на психические функции человека (в том числе на эмоции и поведение), а также способные переводить его в измененное состояние сознания.

4) Средства сомато-психологического воздействия.

5) Информационные способы и средства ИПВ.
- Средства:
  - Литература, зрелищные мероприятия, видеофильмы, реклама, звукозаписи и видеозаписи и т. п.
  - СМИ (печатные газеты и журналы, радиовещание, телевидение);
  - Интернет-ресурсы (сайты, новостные агрегаторы, форумы, социальные сети, чаты и.т.п.).
- Способы:
  - Способы подачи информации:
    - *Пропаганда* – распространение политических, философских, научных, художественных знаний (идей) и другой информации в обществе с целью формирования у группы людей определенного мировоззрения – обобщенной системы взглядов на окружающий мир, место и роль в нём человека, на отношение людей к объективной реальности и друг к другу, а также соответствующих этому идеалов и убеждений, принципов познания и деятельности, ценностных ориентаций;
    - *Убеждение* – способ открытого вербального (словесного) ИПВ на сознание индивида или группы людей, основу которого составляет система ясных, четко сформулированных доводов (аргументов), выстроенных по законам формальной логики и обосновывающих выдвигаемый субъектом воздействия тезис (точку зрения);
    - *Суггестия* (*внушение*) – это процесс неаргументированного ИПВ на сознание человека, связанный со снижением критично-

сти при восприятии и реализации им содержания сообщаемой информации, с отсутствием активного ее понимания, осмысления, развернутого логического анализа и оценки в соотношении с прошлым опытом. В отличие от убеждения, внушение основывается не на логике и разуме человека, а на его способности воспринимать слова другого лица как должное, как инструкцию к действию. При внушении сначала происходит восприятие информации, содержащей готовые выводы, а затем на ее основе формируются мотивы и жизненные установки определенного поведения;

- способы модификации информации:
  - дезинформация (нарушение конфиденциальности и целостности информации);
  - ограниченное предъявление информации (нарушение конфиденциальности и доступности информации);
  - сокрытие информации (нарушение доступности информации);
- способы манипуляции сознанием – специфический вид скрытого ИПВ, направленный на программирование идей, мнений, мотивов, жизненных установок, стереотипов, устремлений, настроений и даже психического состояния людей, которое нужно тем, кто владеет средствами манипуляции;
- способы манипуляции поведением – специфический вид скрытого ИПВ, направленный на программирование такого поведения людей, которое нужно тем, кто владеет средствами манипуляции.

6) Комбинированные средства и способы ИПВ – одновременное применение двух и более средств (способов) ИПВ.

7) Когнитивное оружие.

Достаточно подробно вышеуказанные средства и способы ИПВ рассмотрены в работах [1, 56, 58]. Рассмотрим далее только основные ИПВ, которые могут использоваться для тестирования персонала и отдельных лиц в рамках проведения аудита КИИ.

При рассмотрении ИПВ необходимо отметить, что, несмотря на широкую обсуждение в популярной литературе эффектов психотронного и психофизического ИПВ, профессиональные психологи указывают на необходимость осторожного отношения к результативности данных типов ИПВ, из-за неоднозначности результатов отдельных частных экспериментов, а также в связи с отсутствием в настоящее время масштабных системных исследований по данному вопросу [80].

4.4. Информационные воздействия

Информационное воздействие – воздействие на психику человека или группы за счет манипуляцией информацией и способом ее доведения.

4.4.1. Средства информационного воздействия

Классификация основных средств информационного воздействия представлена на рис. 24 по материалам работ [1, 54, 60].

Средства массовой информации (СМИ) включают в себя расширенный функционал способов воздействия на психику индивидов и масс с целью внедрения в подсознание психологических установок и формирования паттернов поведения в бессознательном психики. К средствам массовой информации относятся телевидение, пресса, радио, все зрелищные мероприятия, литература, видеофильмы, реклама, звукозаписи и видеозаписи и т.п. – всё, с помощью чего можно донести информацию. При этом из всех этих СМИ наивысшей эффективностью обладают телевидение и новостные Интернет-агрегаторы [60].

Рис. 24. Классификация средств информационного воздействия

Основными способами манипулирования информацией, используемыми в СМИ, являются:

- откровенная ложь в целях дезинформации;
- сокрытие критически важной информации;
- погружение ценной информации в массив информационного мусора;
- упрощение, утверждение и повторение (внушение);
- подмена терминологии: применение понятий и терминов, смысл которых не ясен или претерпел качественные изменения, что затрудняет формирование реальной картины события;
- введение запрета на определенные виды информации и разделы новостей;
- узнавание образа: известные политические деятели, представители шоу-бизнеса могут участвовать в заказных акциях, оказывая тем самым определенное влияние на мировоззрение их поклонников;

- подача негативной информации, которая лучше воспринимается аудиторией по сравнению с позитивными новостями.

В качестве средства информационных воздействий всё активнее и масштабнее применяются социальные сети в сети Интернет. Они являются новым современным инструментом, используемым в интересах как массового (активации протестных настроений, координации действий протестующих, информирования международной общественности о происходящих событиях), так и точечного воздействия (ведение пользовательской компьютерной разведки, установление нужных контактов, формирование сети источников и агентов влияния на отдельных пользователей). Общение в социальных сетях создает у людей чувство сопричастности и доверия, а выкладывание фотографий или видеороликов обеспечивает эффект присутствия [60].

Более подробная информация о средствах информационного воздействия представлена в работе [1].

4.4.2. Способы информационных воздействий

Несмотря на то, что вопросы информационного воздействия достаточно подробно освещены в известной литературе, основная часть современных изданий посвящена вопросам информационных воздействий через СМИ в интересах достижении определенных политических или социальных эффектов. При этом в подавляющем большинстве известной литературы отсутствуют формализованные модели информационных воздействий, что делает ее малопригодной для решения задачи разработки формальных сценариев ИПВ. К исследованиям, в которых представлены формальные модели информационного воздействия, можно отнести работы [61, 70-72]. Именно данные работы были взяты за основу при формализации способов информационных воздействий.

4.4.2.1. Стратегии информационного воздействия

Рассмотрим основные стратегии информационного воздействия. Под стратегией информационного воздействия понимается общий принцип действий субъекта на объект в рамках проведения информационной операции, которая состоит из нескольких информационных воздействий, объединенных единым замыслом с целью достижения глобальной цели.

Основные стратегии информационного воздействия [61]:

1) *стратегия устрашения* – угроза применения субъектом по отношению к объекту информационных и силовых воздействий, при одновременной демонстрации субъектом своего количественного и качественного информационного превосходства. Данная стратегия включает в себя несколько вариантов действий:
   – *стратегия ложного устрашения* – демонстрация субъектом возможности применения информационных и силовых воздействий по отношению к объекту, без реального намерения ее применения, при одновременной демонстрации субъектом своего количественного и качественного информационного превосходства;

– *стратегия реалистического устрашения* – угроза субъекта применить информационные и силовые воздействия по отношению к объекту, при одновременной демонстрации субъектом примера применения воздействий в отношении других сторон конфликта или агентов влияния;

2) *стратегия уничтожения* – применение атакующих информационных воздействий субъектом по отношению к объекту, с целью заставить последнего действовать в соответствии с намерениями субъекта или согласиться на выдвинутые условия;
3) *стратегия массированного удара* (*стратегия возмездия*) – одновременное и массированное применение субъектом атакующих информационных воздействий с целью причинения объекту воздействия максимального ущерба;
4) *стратегия измора* – применение последовательности информационных воздействий, каждое из которых ослабляет объект воздействия и приносит информационное превосходство субъекту воздействия;
5) *стратегия сдерживания* – проведение информационных воздействий с целью заставить объект воздействия воздержаться от определённых действий, нежелательный субъекту воздействия;
6) *стратегия отражения агрессии* – проведение информационных операций с целью нивелировать превосходство объекта воздействия, которое объект получает, проводя против субъекта атакующие информационные и силовые воздействия;
7) *стратегия непрямых действий* – проведение информационных операций не путем непосредственного воздействия на объект, а путем воздействий на него через агентов влияния и других сторон конфликта, реализации программ «саморазрушительного» поведения объекта, лишения его информационного превосходства по отношению к своим союзникам и т. д.;
8) *стратегия взаимных уступок* – проведение субъектом информационных воздействий в конфликте, в ходе которого ни субъект, ни объект не достигают полного выигрыша, а приходят к некой равновесной (компромиссной) ситуации, в которой каждая из сторон конфликта достигает некоторого информационного превосходства, по отношение к тому уровню, который был у сторон до начала конфликта;

В формальном виде данные стратегии информационных воздействий представлены в работе [61].

4.4.2.2. Тактические приемы информационных воздействий

Рассмотрим основные тактические приемы, применяемые при организации информационного воздействия. Под тактическим приемом понимается общий принцип действий субъекта при организации информационного воздействия на объект в рамках достижения частной (локальной) цели информационной операции.

Основные тактические приемы организации информационного воздействия [61]:

- *доминирование* – цикл информационных воздействий, направленных на поддержание субъектом своего информационного превосходства над объектом на определенном временном интервале;
- *экспансия* – цикл информационных воздействий, направленных на количественное повышение субъектом своего информационного превосходства и информационных ресурсов (агентов влияния, точек воздействия на объект, возможностей по интенсификации своих воздействий);
- *модификация* – цикл информационных воздействий, направленных на повышение качества использования субъектом своего информационного превосходства и информационных ресурсов;
- *маскировка* – цикл информационных воздействий, направленных на снижение наблюдаемости и важности субъекта, а также проводимых им информационных воздействий и используемых ресурсов для объекта воздействия;
- *устрашение* – цикл информационных воздействий, направленных на создание у объекта впечатления угрозы применения субъектом по отношению к нему информационных и силовых воздействий;
- *подавление* – цикл информационных воздействий, направленных на формирование существенного информационного превосходства субъекта над объектом;
- *изоляция* – цикл информационных воздействий, направленных на ограничение связей и возможностей объекта по информационному обмену с окружающим информационным пространством;
- *экранирование* – цикл информационных воздействий, направленных на формирование контролируемой среды, в которой объект реализует информационный обмен с окружающим информационным пространством.

В формальном виде данные тактики ведения информационных воздействий представлены в работе [61].

4.4.2.3. Основные нарушения информационной безопасности, на которые ориентированы информационные воздействия

При реализации информационных воздействий на объекты информационно-организационной подсистемы КИИ, субъекты, как правило, реализуют ограниченное число видов нарушения информационной безопасности. К этим основным видам относятся следующие.

Утечка информации – неконтролируемое распространение защищаемой информации. В результате утечки нарушается конфиденциальность информации [61].

Уничтожение информации – действие по уничтожению защищаемой информации, информационных ресурсов или физических средств ее хранения. В

результате уничтожения нарушается доступность, целостность и полнота информации [61].

Хищение информации – действие по изъятию защищаемой информации, информационных ресурсов или физических средств ее хранения с целью ее последующего использования в собственных интересах. В результате хищения нарушается конфиденциальность информации, а при использовании похищенной информации для организации информационных воздействий, основанных на ее искажении – ее целостность [61].

Искажение информации – действие по изменению защищаемой информации или информационных ресурсов. В результате искажения нарушается целостность информации [61].

Задержка информации – действия, направленные на увеличение длительности процессов формирования, накопления, обработки и представления информации. Для систем управления такая задержка приводит к снижению оперативной ценности информации – ее актуальности. Кроме того, задержка информации снижает ее доступность [61].

4.4.2.4. Базовые информационные воздействия

Основными элементами любой психологической операции являются отдельные (базовые) воздействия, проводимые субъектом по отношению к объекту. Эти базовые воздействия связаны с определенной модификацией информации, способом ее подачи или восприятия объектом. В работах [61, 62] введена классификация таких базовых информационных воздействий, последовательное применение которых позволяет достичь вышеуказанных целей нарушения ИБ.

1) *Трансинформирование* – достоверное информирование, при котором информация от субъекта к объекту передается без искажения. Рассматривают следующие варианты трансинформирования:

- *паратрансинформирование* – достоверное информирование, основанное на способности памяти объекта фиксировать и воспроизводить аналоги, которые несут дополнительную информацию, связанную с восприятием основной информации, ее эмоциональным окрасом, отношению к предмету информационного сообщения и т. д.;
- *метатрансинформирование* – многократное повторное достоверное информирование, которое направлено на формирование доверия к субъекту и предмету сообщения, на формирование информационного шума или на информационное насыщение объекта воздействия.

2) *Псевдоинформирование* – ограниченно достоверное, полуложное информирование, при котором правда и ложь логически взаимоувязаны между собой. Псевдоинформирования можно добиться путем варьирования (увеличения или уменьшения) достоверности, полноты, объема, конфиденциальности и целостности информации в следующих вариантах:

- *симуляционное информирование* – информирование объекта, при котором в информацию субъектом вносятся модификации, формирующие

ложные представления или отражение реальности у объекта воздействия;

- *диссимуляционное информирование* – информирование объекта, при котором субъектом скрывается часть информации с целью формирования у объекта семантически-нечёткого восприятия информации или неясного отражение реальности;
- *конфузное информирование* – информирование объекта, при котором субъектом скрывается часть информации, а также модифицируется или искажается семантическое значение информации с целью формирования у объекта противоречивого или ложного восприятия информации или отражения реальности;
- *метапсевдоинформирование* – многократное информирование, при котором у объекта с каждым новым сообщением постепенно подменяется восприятие информации или отражение реальности на примерно равнозначное, но отличающееся от истинного по ряду необходимых субъекту параметров.

3) *Дезинформирование* – ложное информирование. Различают следующие варианты дезинформирования:

- *симуляционное дезинформирование* – информирование объекта, при котором субъект блокирует доступ объекта к источнику достоверной информации, после чего формирует и передает объекту ложную информацию, создавая ложные оригиналы;
- *диссимуляционное дезинформирование* – информирование объекта, при котором субъект блокирует доступ объекта к источнику достоверной информации, после чего на основе сообщений с достоверной информации формирует и передает объекту неполную информацию, скрывая истинные оригиналы;
- *конфузное дезинформирование* – информирование объекта, при котором субъект частично блокирует доступ объекта к источнику достоверной информации, после чего модифицирует или искажает семантическое значение части информации с целью формирования у объекта противоречивого или ложного восприятия информации или отражения реальности;
- *парадезинформирование* – воздействие на объект, при котором субъект способствует ложной семантической интерпретации объектом поступающей к нему достоверной информации.

4) *Метадезинформирование* – это обманно-манипулятивное информирование, при котором ложь представляется в виде многократно повторяемой достоверной информации. Различают следующие варианты метадезинформирования:

- *симуляционное метадезинформирование* – семантическое искажение исходной информации за счет введения в исходное сообщение ложной информации с последующим многократным повторением искаженной информации;

– *диссимуляционное метадезинформирование* – формирование семантической неопределенности за счет сокрытия части исходной информации с последующим многократным повторением неполной информации;
– *конфузионное метадезинформирование* – частичное семантическое искажение и сокрытие исходной информации с последующим многократным повторением искаженной информации.

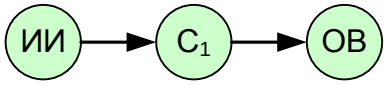
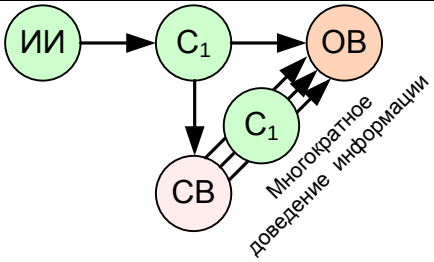
Для существенного повышения эффективности воздействия на объект используется воздействие на него по различным информационным направлениям (как правило, в режиме пространственно-временного разделения направлений). При этом субъектом используются агенты влияния, которые позволяют организовать несколько направлений информационного воздействия на объект. Реализацию такого многонаправленного информационного воздействия выделяют в отдельный класс – мультиинформирование.

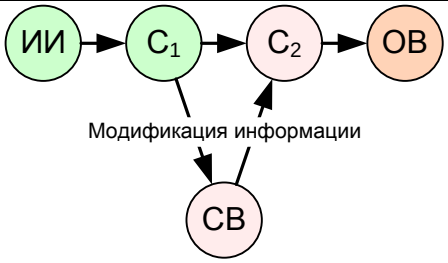
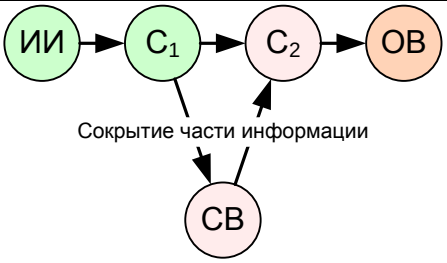
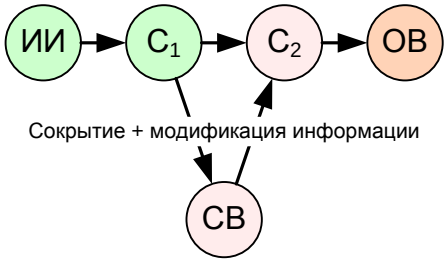
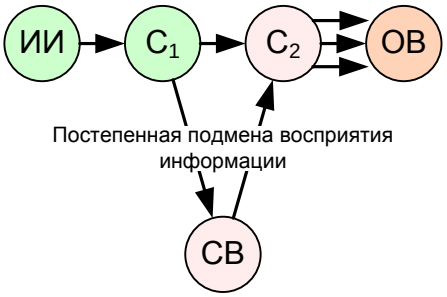
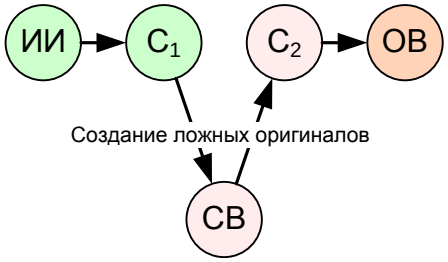
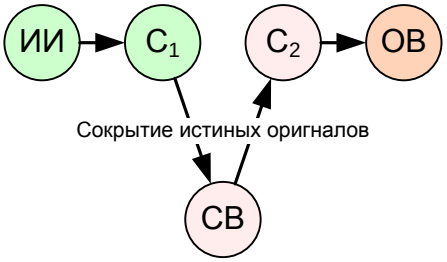
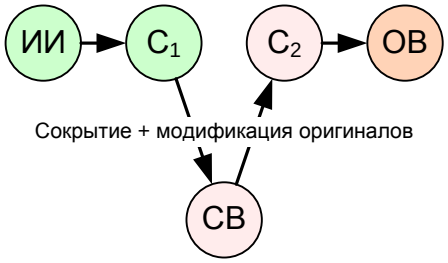
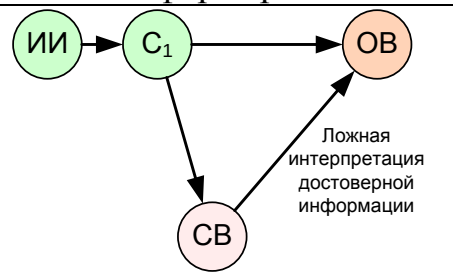
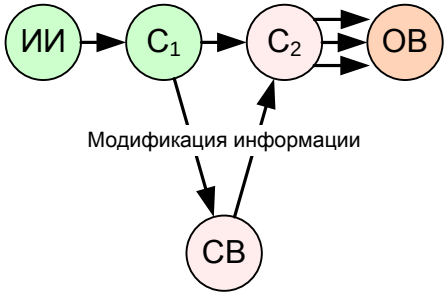
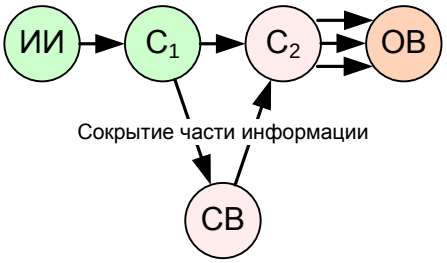
5) *Мультиинформирование* – информирование объекта по различным информационным направлениям. Различают следующие варианты мультиинформирования:

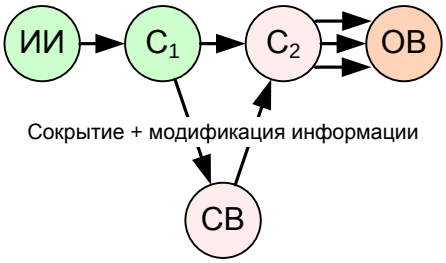
– *многократное информирование* – информирование объекта с одного информационного направления, но с многократным повторением информации;
– *веерное информирование* – информирование субъектом нескольких объектов по различным информационным направлениям;
– *многоагентное информирование* – получение объектом информации по нескольким направлениям от агентов влияния субъекта;
– *вирусное информирование* – информирование объектов с использованием способа самораспространения информации по информационным связям объектов между собой (модель распространения слухов).

Модели вышеуказанных базовых информационных воздействий представлены в таблице 2.

Таблица 2 – Модели базовых информационных воздействий

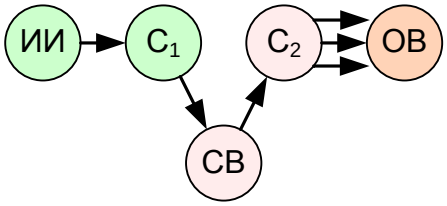
Трансинформирование	
 Паратрансинформирование	 Метатрансинформирование

Псевдоинформирование	
 Симуляционное информирование	 Диссимуляционное информирование
 Конфузное информирование	 Метапсевдоинформирование
Дезинформирование	
 Симуляционное дезинформирование	 Диссимуляционное дезинформирование
 Конфузное дезинформирование	 Парадезинформирование
Метадезинформирование	
 Диссимуляционное метадезинформирование	 Симуляционное метадезинформирование

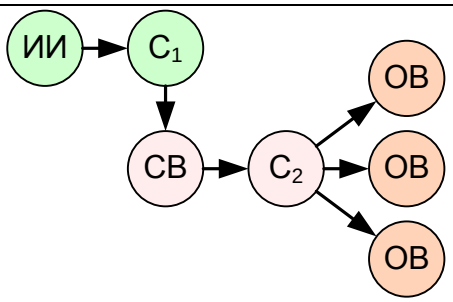


Конфузионное метадезинформирование

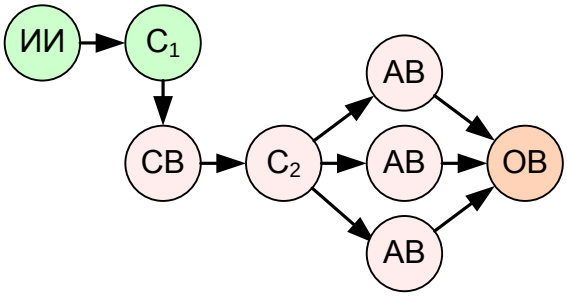
Мультиинформирование



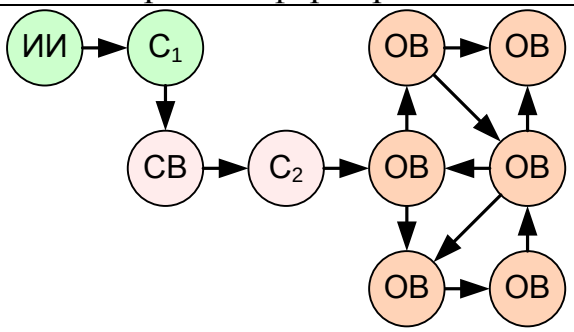
Многократное информирование



Веерное информирование



Многоагентное информирование



Вирусное информирование

Используемые в таблице 2 обозначения:
ИИ – источник информации;
СВ – субъект (источник) воздействия;
ОВ – объект (реципиент) воздействия;
C_1 – исходное информационное сообщение;
C_2 – модифицированное субъектом информационное сообщение;
АВ – агент влияния.

4.4.2.5. Способы подачи информации, направленные на повышение эффективности ее усвоения

Обобщая способы манипуляций, представленные в работах [63, 64], можно выделить следующие основные способы подачи информации, направленные на повышение эффективности ее усвоения.

Наличие «очевидцев». Субъект для организации воздействия на объект использует агентов влияния – очевидцев событий, которые с необходимой искренностью сообщают требуемую информацию, выдавая ее за свою собственную.

Формирование образа врага. Субъект предварительно формирует образ внешнего врага, на которого возлагается ответственность за реальные или мнимые неудачи объекта, кроме того объекту навязывается определенный способ действий как консолидированная совместная позиция объекта и субъекта направленная на отражение общей для них внешней угрозы.

Смещение акцентов. В данном случае происходит сознательное смещение акцентов в подаваемом материале, без изменения семантического содержания информации, при этом акцент делается на той части информации, которая выгодна субъекту, а нежелательная информация преподносится на втором плане.

Использование «лидеров мнений». В данном случае для повышения эффективности усвоения информации для ее предъявления субъектом используются лидеры мнений. Причем в качестве лидеров мнений могут выступать различные фигуры, ставшие авторитетными для определенной категории населения.

Переориентация внимания. Нежелательная (негативная) информация подается на фоне эмоционально или семантически ярко выраженных сообщений, которые маскируют подачу негативной информации и служат отвлечению внимания.

Эмоциональный окрас. В данном случае субъект воздействия формирует эмоциональный контекст для восприятия информации объектом. Этот контекст частично замещает смысловое содержание информации и навязывает объекту определенное восприятие фактов.

Показная проблематика. Формирование «мнимой новостной реальности», в которой акцент делается на информации, выгодной субъекту, причем эта информация подается как «проблематика дня», а нежелательная информация замалчивается, либо подается на фоне информационного шума.

Сокрытие информации (*информационная блокада*). Поток информации, поступающей к объекту, строго контролируется субъектом, а нежелательная информация удаляется из этого потока.

Удар на опережение. Заблаговременное доведение до объекта некоторой части негативной информации, которая вызывает максимальную психологическую реакцию. Дальнейшее доведение остальных частей негативной информации не вызывает у объекта такой ярко выраженной реакции ввиду снижения ее новизны и актуальности.

Ложный накал страстей. Формирование контекста мнимой сенсационности, повышенной важности и эксклюзивности при предъявлении информации.

Передача сакральных знаний. Данный вид манипуляции заключается в том, что субъект сообщает объекту манипуляции, что он намерен сообщить некоторую секретную и важную информацию, доступную только ограниченному доверенному кругу лиц. При этом у объекта манипуляции бессознательно возникает доверие к такого рода информации, а также ослабляются защитные механизмы психики по ее критическому осмыслению.

Формирование «информационного шума». Субъект воздействия формирует для объекта поток различных информационных сообщений, подаваемых с одинаковым форматом, эмоциональным окрасом, важностью и срочностью. В таких условиях у объекта воздействия наступает «информационное насыщение» и он неспособен распознать действительно важную информацию в общем потоке сообщений.

Формирование «обратного эффекта». Субъектом воздействия формируется поток избыточно-негативной информации, которая может содержать элементы семантической противоречивости или гротеска. Предъявление такой информации объекту дает обратный эффект – объект либо воспринимает данную информацию положительно (с юмором или рассматривая ее как ложь), либо делает положительные выводы об источнике или предмете информационного сообщения.

Будничный рассказ. Нежелательная информация подается как обыденная, с использованием нейтральной лексики и без эмоционального окраса.

Односторонность освещения событий. При предъявлении сложной многофакторной информации в нее встраивается смысловой или эмоциональный контекст формирующий «правильное» ее восприятие. При представлении информации о многосторонней конфликтной ситуации формируется контекст, направленный на положительное отношение к одной из сторон конфликта.

«Дьявол в деталях». В данном случае субъект воздействия заставляет объект заведомо критически рассматривать только незначительную часть подаваемой информации, отвлекая его от критического анализа всей информации в целом.

Принцип контраста. Выгодная субъекту информация подается в положительном аспекте на фоне другой, заведомо негативной, информации, которая отрицательно воспринимаемой объектом.

Одобрение мнимого большинства. Требуемая информация подается в контексте ее верификации и предварительном одобрении некими экспертными группами или большинством, при этом объекту фактически предлагается присоединиться к большинству без критического анализа предъявляемой информации.

Экспрессивный удар. Предъявление нежелательной информации сопровождается высоким уровнем эмоционального контекста, что вызывает у объекта психологическую реакцию отторжения и протеста против такой негативной информации.

Нарушение логики. При подаче информации лингвистическими способами подменяются причинно-следственные связи, а также логические выводы «от частного к общему» и «от общего к частному» и т. д.

Искусственное просчитывание ситуации. Субъектом заблаговременно предъявляется объекту несколько вариантов различной информации, после чего считывается реакция объекта. В дальнейшем при предъявлении объекту целевой информации, она предъявляется в том контексте и в той форме, которая максимизирует реакцию объекта, выгодную субъекту воздействия.

Манипулятивное комментирование. Посредством комментирования субъектом или мнимыми экспертами объекту навязывается определенное восприятие изначально нейтральной информации.

Эффект присутствия. Для повышения восприятия информации о некотором событии для объекта искусственно воссоздается (виртуализируется) информационная сопричастность к этому событию, формируя у объекта эффект собственного участия в нем.

Мнимые события. Объекту предъявляется информационная реконструкция мнимого (виртуального) события, якобы имевшее место в реальности.

Допуск в систему. Данный вид манипуляции основан на таком свойстве психики индивидов, как кардинальное изменение своих взглядов и интерпретации той же самой информации в зависимости от того находится ли человек внутри некой (политической, социальной, организационной) системы, на которую направлена информация или вне ее.

Повторение и утверждение. Многократное повторение какой-либо информации. При этом следует максимально упростить форму подачи информации и адаптировать ее к особенностям восприятия объектом воздействия.

Навязывание мыслей. Субъект многократно повторяет требуемую информацию, меняя форму, направление, способ и контекст ее предъявления, тем самым навязывая объекту «привыкание к правильному» восприятию информации при одновременном снижении порога ее критической оценки.

Дробление. Целостная нежелательная информация разделяется на фрагменты, отдельные события и факты и предъявляется объекту по нескольким информационным направлениям так, чтобы объект не смог соединить их в единое целое и осмыслить в целом. Таким образом, у объекта формируется мозаичное восприятие нежелательной информации.

Перескакивание тем. Субъект воздействия стремится после озвучивания целевой информации спешно перейти на другую тему, снижая вероятность того, что целевая информация будет полностью осознана, верифицирована и опротестована объектом. Более того, при повторном возврате к целевой информации, у объекта воздействия уже будет сформирована латентное положительное мнение по целевой информации, т. к. она будет ему предъявляться повторно.

Быстрый темп. В данном случае субъект воздействия навязывает объекту чрезмерно высокий темп подачи информации, чтобы не допустить формирования по подаваемой информации сознательной критической оценки, а также с целью добиться принятия информации объектом воздействия, под предлогом отсутствия времени для ее анализа.

Использование специфической терминологии. Субъект намеренно использует специфические термины и лексику для искажения семантического значения или формирование необходимого эмоционального окраса подаваемой объекту информации.

Упрощение, стереотипизация. Более простая форма представления информационного сообщения повышает эффективность его восприятия, а упро-

щенная интерпретация фактов снижает вероятность поиска их альтернативного интерпретирования.

Дополнительно к вышеуказанным способам при подаче информации требуется учитывать известные психические эффекты восприятия информации человеком [54, 65]:

- *эффект первичности* – основан на том, что первое сообщение о каком-либо событии оказывает более сильное психологическое воздействие, чем последующие. Оно как бы создает своеобразную базовую установку по восприятию последующей информации, формирует отношение к ней индивида. Изменение сформировавшейся позиции существенно сложнее. Источник информации, первым сообщивший о том или ином факте, также будет оцениваться индивидом как более предпочтительный;
- *эффект последовательности* – основан на том, что человек склонен воспринимать информацию как достоверную, если она не противоречит информации поступившей ранее;
- *эффект правдоподобия* – основывается на особенности психики человека воспринимать информацию как достоверную, если она не противоречит его ожиданиям, внутреннем убеждениям, личным стереотипам восприятия и т. д. При предъявлении информации, с которой индивид внутренне не согласен или которая противоречит его внутренней «картине мира», он воспринимает такую информацию как недостоверную;
- *эффект закона* – основывается на том, что человек склонен воспринимать информацию как достоверную, если она сформулирована в виде формализованной математической записи или сопровождается мнимым формально-математическим доказательством;
- *эффект ореола* – основан на специфике психики распространять общее положительное/отрицательное впечатление об источнике информации на восприятие о достоверности информации поступающей от этого источника;
- *эффект авторитета* – основан на специфике психики индивида доверять информации, поступающей от субъективно-достоверных источников: лиц, имеющих высокий социально-политический, научный или общественный статус; независимых СМИ; официальных информационных бюллетеней и документов и т. д.;
- *«голос пророка»* – восприятие источника информации как достоверного существенно возрастает, если он демонстрирует реальные или мнимы «прогнозные свойства». Поэтому при осуществлении воздействий подача информации производится таким образом, чтобы изложенные в ней факты воспринимались как ранее предсказанные. Для этого используются закономерности ассоциаций по смежности, подобию, контрасту, временной и пространственной близости;
- *эффект повторения* – основывается на закономерностях запоминания человеком информации. Психологический механизм многократного

повторения действует на основе принудительного привлечения внимания, подсознательного восприятия многократно предъявляемой информации, существенного снижения уровня ее критической оценки при повторном предъявлении. Считается, что целесообразно передавать одно и то же сообщение трижды: в кратком изложении, полном и снова в кратком. Затем, при необходимости, эта же информация может быть преподнесена в другой форме и по другим информационным направлениям;

- *эффект возложения ответственности* – основывается на том, что человек склонен воспринимать успешное и неуспешное развитие событий в категориях ответственности. При этом он приписывает причины успеха себе самому, а ответственность возлагает на других людей. Поэтому при формировании информационных воздействий необходимо связывать любые трудности и препятствия, неудачи с конкретными объектами (конкретные лица, политические партии, организации, правительственные круги, законодательство, моральные и этические нормы и др.). Как правило, выбирается ограниченное число таких объектов и на них настойчиво направляется негативная реакция;
- *эффект справедливости* – психологический феномен, выражающийся в вере индивида в то, что мир устроен справедливо, и люди в жизни получают то, что заслуживают в соответствии со своими личными качествами и поступками: хорошие люди вознаграждаются, а плохие — наказываются.

Использование в составе ИПВ вышеуказанных способов подачи информации, учитывающих известные психические эффекты ее восприятия, обеспечивают высокий уровень формирования у объекта ИПВ требуемых психологических установок и восприятия реальности выгодного субъекту воздействия.

4.4.2.6. Манипулятивные ситуации, направленные на навязывание объекту «правильного» восприятия информации или определенного сценария поведения

Одним из наиболее распространенных сценариев реализации информационного воздействия является информационное взаимодействие субъекта и объекта в форме диалога или спора. В этом случае в качестве способов, повышающих эффективность информационного воздействия, могут выступать специальные манипулятивные ситуации, реализующие выгодный для субъекта вариант развития ситуации.

Обобщая материалы, представленные в работах [63, 64], можно выделить следующие основные манипулятивные ситуации, направленные на навязывание объекту «правильного» восприятия информации или «правильного» сценария поведения.

1) Сценарии навязывания восприятия информации в диалоге.

– *Ложное переспрашивание или обманчивые уточнения*. Манипулятивный эффект достигается за счет того, что субъект воздействия пере-

спрашивает объект, однако повторяет достоверную информацию только вначале, а далее вносит в ранее поданную объектом информацию новый смысл изменяя семантическое значение информации в угоду себе.

– *Ложная влюбленность или благодарность обмана*. Данная ситуация основана на особенности человеческой психики, которая заключается в том, что объект, на кого направлена любовь и уважение субъекта, бессознательно чувствует обязанность отплатить тем же. К тому же подобная ситуация позволяет снять в психике объекта различного рода барьеры, направленные на критический анализ как поведения субъекта, так и поступающей от него информации.
– *Дружеская помощь.* Ситуация основана на доверии объекта той информации, которая поступает от эмоционально близких людей, таких как родственники, друзья или хорошие знакомые.
– *Поиск общих черт.* В данном случае манипулятивное воздействие достигается за счет предварительного наблюдения за объектом, оценки его психологических особенностей, после чего субъект обращает внимание или искусственно формирует некую схожесть между собой и объектом, ослабляя защитные функции психики последнего и навязывая определенное восприятие информации, используя эту мнимую схожесть.
– *Скажи «да».* Манипуляции подобного рода осуществляются за счет того, что субъект стремится так построить диалог с объектом, чтобы тот все время соглашался с его словами, тем самым умело подводя его согласию с теми фактами, которые требуют критического восприятия.

2) Сценарии навязывания восприятия информации в споре.

– *Управляемый диалог*. В таком случае субъект воздействия в споре с объектом формирует безразличную, эмоциональную или критическую позицию в восприятии информации объекта, тем самым бессознательно заставляя объект во чтобы это ни стало убедить манипулятора в своей значимости и правильности своей позиции. Субъекту остается, управляя диалогом, получать от объекта новые факты, в том числе и те, которые ранее объект воздействия не собирался предъявлять.
– *Яростный напор*. Данная ситуация эксплуатирует подсознательное желание объекта урегулировать эмоционально-дискомфортную ситуацию конфликта за счет отдельных уступок по предмету спора.
– *Вызывание вынужденных оправданий*. Ситуация основана на желании объекта оправдаться перед необоснованными обвинениями. В такой ситуации защитный барьер психики у объекта ослабевает, и субъект, управляя развитием ситуации, может сформировать у объекта необходимую ему линию поведения или спровоцировать его на выдачу необходимой информации.
– *Мнимое признание выгоды оппонента.* Ситуация основана на предварительном обвинении объекта в неких преимуществах, якобы отсут-

ствующих у субъекта. После этого субъект навязывает объекту определенный способ действий, как вариант доказательства отсутствия такого мнимого преимущества.

- *Имитация предвзятости*. Субъект намеренно ставит объект воздействия в некие заданные условия, когда последний, стремясь отвести от себя подозрение в излишней предвзятости по отношению к субъекту, позволяет проводить над собой манипуляции за счет бессознательного убеждения в искренности действий субъекта.
- *Слова оппонента в качестве доказательства.* В данном случае манипулятивное воздействие достигается и оказывается весьма существенным за счет приведения субъектом в качестве доказательств своей позиции информации, ранее сформированной объектом. Подобное действие, как правило, навязывает строго «согласительную» позицию объекта по отношению к позиции субъекта воздействия.
- *Навязывание выбора.* В этом случае субъект формирует выбор у объекта воздействия таким образом, что не фактически оставляет объекту возможности принятия иного выбора, нежели чем тот, который ему озвучен манипулятором (разница лишь в моделях осуществления).
- *Мнимое отсутствие практики.* В этом случае субъект в качестве контраргумента по отношению к позиции объекта выдвигает суждение, согласно которому действия или позиция объекта имеют исключительно теоретическое обоснование, тогда как на практике ситуация якобы будет совсем иной.

3) Сценарии навязывания поведения.

- *Мнимая слабость.* Данная ситуация направлена на формирование необходимого поведения объекта путем демонстрации субъектом своей уязвимости или слабости.
- *Боль души или помощь ближнему.* Данная ситуация основана на бессознательном желании объекта оказать поддержку больным, попавшим в беду, находящимся в сложной ситуации и т. д.
- *Преодоление внутреннего сопротивления.* Ситуация основана на предварительном формировании некого противоречия в психике объекта воздействия, преодоление которого требует от объекта действий, выгодных субъекту. После этого субъект рекомендует объекту этот способ действий как вариант разрешения возникшего противоречия.
- *Мнимая услуга.* Ситуация основана на предварительном оказании субъектом некоторой незначительной услуги объекту воздействия. В дальнейшем субъект в качестве ответной услуги требует от объекта определенного способа действий.
- *Сценарий «дверь в лицо»*. Объект склонен идти на уступку и соглашаться с малопривлекательным предложением субъекта в том случае, если это предложение предлагается объекту сразу после его отказа от другой более обременительной просьбы.

– *Сценарий «нога в двери»*. После выполнения изначально незначительной просьбы субъекта, объект будет склонен согласиться исполнять другие более обременительные требования субъекта.

4.5. Лингвистические воздействия

Лингвистические средства (языковые единицы, «специальная» терминология, обороты речи, имеющие семантическую неоднозначность при переводе на другие языки, и др.) предназначены главным образом для использования высококвалифицированными специалистами при составлении стандартов, международных документов, текста организационно-нормативных мер и политики обеспечения ИБ. Данные способы воздействия, распространяемые через систему международных стандартов, могут обеспечить долговременный высокоэффективный результат посредством формирования уязвимостей информационных систем на документальном уровне [1].

4.6. Психотронные воздействия

Психотронное воздействие – воздействие технических средств на физическое состояние и сознание человека. По мнению, ряда специалистов, такое воздействие полностью решает проблему дистанционного управления физическим состоянием человека, его психикой и сознанием. При этом необходимо отметить, что профессиональные психологи указывают на необходимость осторожного отношения, как к выявлению эффектов, так и к общей результативности данного типа ИПВ, из-за неоднозначности результатов отдельных частных экспериментов, а также в связи с отсутствием в настоящее время масштабных системных исследований по данному вопросу [80].

К средствам психотронного воздействия относятся [56-58]:

- генераторы электромагнитных излучений;
- генераторы инфразвука и ультразвука;
- лазерные и световые излучатели;
- генераторы специальных излучений;
- компьютерные технологии и др.

Рассмотрим особенности воздействия этих типов психотронного оружия на человека.

4.6.1. Генераторы электромагнитных излучений

В настоящее время СВЧ- и КВЧ-излучение широко используется в физиотерапии. Обобщение опыта физиотерапевтического лечения свидетельствует, что длительное неинтенсивное или кратковременное интенсивное (при уровнях более 10^{-4} Вт/см^2) воздействие коротковолновым ЭМИ может вызывать тревогу, а затем – компенсацию и адаптацию, сопровождающиеся структурными изменениями организма. При длительном интенсивном воздействии наблюдаются стадия тревоги, стадия истощения и возникновение патологии организма. Также следует отметить, что при длительном неинтенсивном воздействии возмож-

ны генетические изменения организма, которые могут вызвать нежелательные последствия в будущих поколениях. Кроме того, необходимо добавить, что длительное (в течение многих лет) воздействие низкоэнергетических СВЧ- и КВЧ-излучений способно вызвать существенное снижение и даже полное подавление иммунитета. Это может привести к распространению различных болезней, эпидемий и вымиранию больших масс населения [56].

Кроме того, СВЧ-излучение может быть использовано для биорезонансной стимуляции работы головного мозга. Как известно, основную роль в психической деятельности человека, саморегуляции его поведения играет головной мозг. Поэтому большими потенциальными возможностями психологического воздействия обладают биорезонансные системы, способные обеспечить манипуляцию тонкими механизмами работы мозга и нервной системы [56].

Биорезонансная стимуляция работы головного мозга человека основывается на том, что в зависимости от психического состояния человека интегральное функционирование головного мозга характеризуется электрической активностью в определенных диапазонах частот (биоритмом). При том или ином состоянии организма (умственная или физическая нагрузка, эмоциональное напряжение, сон и т.п.) регистрируются биоритмы определенной частоты и характера. Воздействуя определенным образом на волны какого-либо биоритма головного мозга с помощью резонансного эффекта, можно переводить его в доминирующее состояние и тем самым влиять на сознание человека. Очевидно, что такое ИПВ может носить не только положительный, но и скрытый деструктивный характер [56].

4.6.2. Генераторы инфразвука и ультразвука

Генераторы инфразвука и ультразвука используют эффекты деструктивного воздействия на психику и организм человека инфразвука (частота колебаний ниже 16 Гц) и ультразвуковых колебаний (свыше 20 кГц) [56].

Отдельные исследования показали, что при уровне интенсивности от 95 до 150 дБ и более инфразвук может вызывать у людей неприятные субъективные ощущения и многочисленные реактивные изменения, к числу которых следует отнести изменения в центральной нервной, сердечно-сосудистой и дыхательной системах, а также в вестибулярном анализаторе. Эти изменения способны также возбуждать у людей состояние ужаса и паники, вызывать потерю самоконтроля. Частота же между 6 и 9 Гц вообще чрезвычайно опасна. Теоретически такой инфразвук достаточной мощности может разорвать внутренние органы [56].

Ультразвуковые колебания не ощущаются человеком, но даже малая интенсивность ультразвуковых колебаний низкочастотного диапазона (20-30 кГц) значительно влияет на психику человека: вызывает головную боль, головокружение, быструю утомляемость, расстройства зрения и дыхания. Ультразвук низкочастотного диапазона может использоваться для угнетения иммунной системы и подавления воли, оказания вредного воздействия на сердечно-сосудистую, нервную и эндокринную системы, нарушения обмена веществ. Под длительным действием интенсивного ультразвука температура тела чело-

века повышается, пульс становится реже, замедляются рефлекторные реакции на внешние раздражения [56].

4.6.3. Лазерные излучатели

Сравнительно новым средством ИПВ, которое может найти широкое применение на практике, являются генераторы голографических изображений в атмосфере, которые создаются лазерным излучением. По данным зарубежных СМИ, в ряде стран разрабатываются проекты установки на действующих космических аппаратах лазерно-световых комплексов, способных проецировать на облака различные изображения. Так в США имеются проекты по созданию на небе голографические изображения. Таким образом, неожиданное созерцание образов святых, чудовищ (драконов, ящеров, мутантов и др.) или иных незнакомых явлений может оказать сильное психологическое воздействие на людей, причем как мобилизующего, так и деморализующего порядка [58, 59].

4.6.4. Световые излучатели

Для деморализации психики людей может использоваться источник мелькающего света с частотой 10-20 Гц. Установлено, что наиболее сильное воздействие оказывает излучение с частотой следования импульсов 15 Гц, лежащее в красной области спектра и имеющее весьма малую интенсивность (почти невидимый свет) с крутым передним фронтом импульсов. Под влиянием такого облучения у 5% облучаемых людей возникли эпилептические припадки, а 25% облученных чувствовали недомогание, тошноту, головокружение, затруднения при быстрых движениях и даже теряли сознание. Установлено, что при воздействии мелькающего света клетки мозга перестраивают частоты своих колебаний в соответствии с частотой вспышек света. Такое навязывание ритма может влиять на состояние психики, умственную деятельность и самочувствие человека [56, 58].

4.6.5. Компьютерные технологии

Высшим достижением компьютерных технологий в области психологического воздействия на сегодня является виртуальная реальность, которая позволяет прорываться в глубинные пласты человеческой психики, подменять отдельные элементы самообраза в нужном направлении и, в конечном итоге, – эффективно манипулировать сознанием виртуального пользователя. Быстрое развитие компьютерных технологий виртуальной реальности создает угрозу появления техногенного наркотика – более сильного и «гибкого» для управления сознанием человека, чем любые известные фармакологические наркотические препараты. С помощью компьютерных игр можно трансформировать психику играющего человека в заданном программно-поддерживаемом направлении. При этом в мозгу играющего возникают следы-фантомы: сновидения, страхи, эпилептические припадки, кошмары. Многие дети после подобных игр попали в больницы и получили серьезные психологические травмы [58].

4.7. Психофизические воздействия

Психофизическое воздействие – скрытое насильственное воздействие на подсознание человека с целью модификации его сознания, поведения и физиологического состояния в нужном для воздействующей стороны направлении [58].

При этом необходимо отметить, что профессиональные психологи указывают на необходимость осторожного отношения, как к выявлению эффектов, так и к общей результативности данного типа ИПВ, из-за неоднозначности результатов отдельных частных экспериментов, а также в связи с отсутствием в настоящее время масштабных системных исследований по данному вопросу [80-82].

Психофизические ИПВ, производимые без ведома самого человека, лишают его права самостоятельного выбора логически обоснованных решений, свободы выбора своего поведения, исполнения желаний, выражения эмоций. Психофизические средства основаны на суггестии [58].

Суггестия (*внушение*) – это целенаправленное воздействие на личность или группу (массовое внушение), воспринимаемое на уровне подсознания и приводящее либо к появлению определенного состояния духа, чувства, отношения, либо к совершению определенных поступков [58].

В результате суггестивного воздействия у объекта внушения возникает склонность подчиняться и изменять поведение не на основании разумных, логических доводов или мотивов, а по одному лишь требованию или предложению, исходящему от другого внушаемого лица. При этом сам человек не отдает себе отчета в такой подчиняемости, продолжая считать свой образ действия как бы следствием собственной инициативы или собственного выбора.

Наиболее распространенными являются следующие типы психофизического воздействия, основанные на различных видах суггестии [56, 58]:

- средства и способы предъявления неосознаваемой акустической информации;
- средства предъявления неосознаваемой визуальной информации;
- средства предъявления неосознаваемой комбинированной информации.

Рассмотрим эти средства более подробно.

4.7.1. Средства и способы предъявления неосознаваемой акустической информации

При предъявлении неосознаваемой акустической информации основным приемом является предъявление акустических сигналов ниже порога слышимости на фоне более громкой маскирующей информации. В этом случае очень слабые нижнепороговые стимулы не воспринимаются сознанием, глубоко внедряясь в подсознание. Неосознаваемая акустическая информация предъявляется на очень тихом уровне звучания (уровень громкости составляет 9-30% от фонового звука и более), путем спектральной маскировки речевого сигнала музыкой или шумом [56].

4.7.2. Средства предъявления неосознаваемой зрительной информации

Визуальные средства, в отличие от акустических, позволяют человеку практически мгновенно воспринимать запрограммированное ИПВ (хотя сработать оно может значительно позднее), причем это воздействие может являться более глубоким и долговечным, поскольку визуальные системы влияют не только на интеллект, но и на эмоционально-чувственный базис человека. Основными параметрами зрительного восприятия являются положение, форма и движение объекта, их цвет и яркость визуальных объектов. При предъявлении неосознаваемой информации используются методы различной маскировки – прямой, обратной, метаконтраста и др. [56].

Более совершенные методы неосознаваемого предъявления зрительной информации основываются на «диспаратном» предъявлении, т. е. каждый кадр видеоинформации содержит только часть суггестивного образа, недостаточную для его осознания. При последовательном предъявлении ряда таких кадров происходит суммирование частей образной суггестии на неосознаваемом уровне. Данный подход укладывается в принципы нейросемантического гипертекста, которые используются в методах нейролингвистического программирования [56].

4.7.3. Средства предъявления неосознаваемой комбинированной информации

Эффект психологического воздействия может существенно усилиться при комбинированном использовании различных типов суггестии. Наиболее известным и простым примером такой кооперации воздействия является комплексное использование акустической и визуальной суггестии. Наиболее сложной формой предъявления неосознаваемой комбинированной информации является нейролингвистическое программирование, достигаемое путем долгого и кропотливого подбора «ключа» к подсознанию человека. В качестве такого «ключа» может использоваться специально подобранный текст (так называемый нейросемантический гипертекст), содержащий наиболее значимые слова и фразы для внушаемого лица, значительной группы лиц, подразделения, региона. При этом память, сознание и подсознание любого человека рассматриваются как личностная модель мира, которая может быть «перепрограммирована» после ввода человека в специальные психологически-интерфейсные режимы [58].

4.8. Психотропные воздействия

Психотропное воздействие базируется на использовании механизма изменения биохимических характеристик процессов нервной системы человека посредством введения в его организм фармакологических препаратов, наркотических веществ, ядов в концентрациях, вызывающих необходимые психические реакции, состояния и поведение. Многие психотропные средства могут скрыто вводиться в организм людей через предметы личной гигиены, как через кожу,

так и при вдыхании аэрозолей. Исходя из свойств психотропных средств, возможно представить следующие возможности при использовании их для ИПВ на человека [54].

Во-первых, психотропные средства модифицируют психику человека, который в большинстве случаев остается работоспособным и продолжает принимать решения, неотражающие адекватно окружающую обстановку и несоответствующие реальности. Окружающим человека с модифицированной психикой неизвестно, что его решения и поступки неадекватны ситуации. Если такой человек является ЛПР, то его решения остаются обязательными для членов руководимого им коллектива, и их ошибочность становится понятной для большинства или слишком поздно, или не осознаётся коллективом вообще. В этом случае коллектив не связывает свои неудачи и поражения с неправильным принятием решений и считает, что всё это произошло в силу каких-то иных причин [54].

Во-вторых, психотропные средства могут применяться как против конкретного человека, так и против большого количества людей. В случае применения против конкретного человека учитываются его личностные особенности и его положение в социальном коллективе. Ожидаемое изменение психики в случае применения психотропных средств может быть связано с ожидаемым изменением в поведении, поступках, действиях малых групп людей и в поведении больших социальных групп [54].

В-третьих, люди, на которых было произведено воздействие психотропными средствами, сохраняют свое соматическое (телесное) здоровье. Более того, модификация психики со временем, исчисляемым в неделях или месяцах, прекращается или автоматически, или с помощью направленного психотерапевтического воздействия [54].

Таким образом, использование психотропных средств вышло далеко за рамки психиатрической клиники. Они могут широко применяться для достижения определенных политических, экономических, военных и других целей.

4.9. Сомато-психологические воздействия

Основные средства сомато-психологического оружия представлены в таблице 3 по данным из работы [54].

В основе сомато-психологического воздействия лежит принцип психофизического параллелизма, определяющий взаимосвязь внутренних (психических) процессов и внешних (физических) проявлений по виду: «внутреннее проявляется во внешнем, внешнее отражается во внутреннем». Другими словами, речь идет о том, что конкретное состояние организма, тела человека во многом обусловливают его психические состояния, эмоции, мотивы и модели поведения. Следовательно, целенаправленно изменяя соматическое состояние человека, можно в известной степени корректировать его психологические характеристики.

Таблица 3 – Основные средства сомато-психологического воздействия [54]

Наименование оружия	**Краткая характеристика оружия**
Лазерные средства	Лазерные генераторы и устройства, применяемые для временного ослепления
Средства обездвижения людей	Быстро затвердевающие суперклеевые составы, распыляемые и приклеивающие людей к технике, почве, друг к другу. Суспензии, многократно снижающие коэффициенты трения и делающие невозможными передвижения людей и техники, что порождает чувства бессилия, страха, отчаяния
Средства постановки «психологических заграждений»	Генераторы трудно переносимого шума, составы с непереносимым запахом, перцовые, слабительные, рвотные и др. аэрозоли, распыляемые над определенной территорией и создающие условия, невозможные для пребывания на ней других людей
Биологические средства нелетального действия	Микроорганизмы, искусственно выведенные насекомые, вызывающие недомогания (плохое самочувствие, чесотку, нестерпимый зуд, обширные язвы и др.) и заболевания, препятствующие ведению активных действий и способствующие деморализации людей
Экологические средства нелетального действия	Средства создания и поддержания в течение длительного времени погодно-климатических условий, крайне неблагоприятных для жизнедеятельности

Выводы по четвертой главе

Подводя итог материалу четвертой главы можно сделать следующие краткие обобщенные выводы.

1) Для аудита уровня защищенности объектов КИИ в организационной и психологической сферах может использоваться тестирование отдельных лиц и персонала КИИ путем воздействия на них специальными средствами и способами ИПВ. Причем данные средства и способы ИПВ, а также сценарий их применения должны соответствовать тем средствам, способам и сценариям, которые предполагаются к применению против персонала КИИ со стороны потенциального противника.

2) Средства и способы специальных ИПВ, предназначенные для тестирования объектов КИИ, целесообразно классифицировать на: информационные; лингвистические; психотронные; психофизические; психотропные; сомато-психологические. В рамках тестирования объектов КИИ должны реализовываться сценарии поэтапного интегрального применения указанных типов ИПВ для всеобъемлющего анализа информационно-организационной подсистемы объектов КИИ, вскрытия ее уязвимостей в организационной и психологических сферах, а также для формирования предложений по повышению уровня информационно-психологической безопасности в интересах обеспечения устойчивости объектов КИИ в условиях ведения информационного противоборства.

3) Человек (ЛПР, оператор технической системы, единица персонала КИИ) в структуре КИИ является, с одной стороны, «ключевым звеном» системы, т.к. именно к нему стекаются все информационные потоки, и именно за ним остается приоритет в интерпретации информации, а также в принятии окончательных решений, но, с другой стороны, человек является наиболее «слабым» звеном системы, подвержен воздействию ИПВ, которые могут принудить его к сознательному или бессознательному нарушению политики ИБ. В связи с этим, актуальным и важным направлением аудита ИБ объектов КИИ, является проверка психологической устойчивости персонала путем его тестирования специальными средствами и способами ИПВ, которые планируются к использованию силами информационных и психологических операций потенциального противника.

4) Дальнейшим развитием исследований в области влияния информационно-психологической безопасности личности, как единицы персонала КИИ, на уровень ИБ является формирование специальных средств и способов теоретического и практического тестирования защищенности КИИ в организационной и психологической сферах. Интеграция этих средств и способов в состав единого комплекса тестирования защищенности КИИ позволит обеспечить имитацию передовых возможностей сил информационных и психологических операций потенциального противника. Кроме того, по итогам анализа результатов тестирования станет возможным совершенствование оборонительных средств ИТВ с учетом выявленных уязвимостей объектов КИИ в организационной и психологической сферах.

Заключение

На протяжении 80–90-х гг. прошлого века информационные технологии за счет своего революционного развития проникали во все сферы жизнедеятельности человека. Это в конечном итоге привело к тому, что новые информационные технологии, а также высокоразвитые информационные системы и сети сформировали информационное ядро государства – критическую информационную инфраструктуру. Одновременно с этим, в условиях развития теории и практики информационного противоборства возникают новые, специфичные именно для информационной эпохи угрозы средства и способы информационных воздействия, а также профессиональные силы информационных операций. Следствием этого является насущная потребность в аудите ИБ в форме проверки устойчивости КИИ государства в условиях целенаправленных ИТВ и ИПВ со стороны потенциального противника.

Данная работа направлена на систематизацию основных сведений об этапах, теоретических и практических подходах к аудиту ИБ объектов КИИ, и на их основе сформировать оригинальный подход к тестированию информационных систем, как одного из основных типов аудита КИИ, в том числе с учетом возможности использования специальных способов и средств на основе ИТВ и ИПВ. Именно этот авторский подход и отличает данную работу от других работ по тематике аудита ИБ.

Автор выражает надежду на то, что результат его работы вызовет интерес у широкого круга специалистов. Он надеется на то, что материал, обобщенный им в монографии, вызовет благосклонное внимание соискателей ученых степеней, военных и технических специалистов, которые выбрали сложные и увлекательные проблемы информационной безопасности и информационного противоборства в качестве области своих научных интересов. Кроме того, материал работы должен помочь специалистам, которые занимаются вопросами разработки средств и способов информационных воздействий, методически правильно скорректировать полученные ими научные и практические результаты с целью приведения их в соответствие с научными специальностями 05.13.19 «Методы и системы защиты информации, информационная безопасность» и 19.00.03 «Психология труда, инженерная психология, эргономика».

Список используемых сокращений

CMM – Capability Maturity Model – модели зрелости.

COBIT – Control Objectives for Information and related Technology – стандарт по формализации задач управления для информационных и смежных технологий.

IDEF – Integrated DEFinition) – представление любой изучаемой системы в виде набора взаимодействующих и взаимосвязанных блоков.

MBT – Model Based Testing – тестирование на основе моделей.

URSIT – Uniform Interagency Rating System for Information Technology – стандарт для единой оценки информационных технологий.

БД – база данных.

ИБ – информационная безопасность.

ИПб – информационное противоборство.

ИПВ – информационно-психологическое воздействие.

ИС – информационная системы.

ИТВ – информационно-техническое воздействие.

КВЧ – крайне высокая частота.

КИИ – критическая информационная инфраструктура.

НСД – несанкционированный доступ.

ОТС – организационно-техническая система.

ПО – программное обеспечение.

ПЭМИН – побочные электромагнитные излучения и наводки.

РЭП – радиоэлектронное подавление.

РЭС – радиоэлектронное средство.

СВЧ – сверхвысокая частота.

СМИ – средства массовой информации.

СУБД – система управления базами данных.

ЭМИ – электромагнитное излучение.

Глоссарий терминов и определений

Активное информационно-техническое воздействие – см. воздействие информационно-техническое активное.

Активное тестирование – см. тестирование активное.

Активный аудит – см. аудит активный.

Алгоритмическая компьютерная разведка – см. разведка компьютерная алгоритмическая.

Анализ риска – систематическое использование информации для идентификации источников угроз и оценки величины риска.

Аппаратная закладка – см. закладка аппаратная.

Аппаратная компьютерная разведка – см. разведка компьютерная аппаратная.

Атака сетевая удаленная – это атакующее информационно-техническое воздействие, осуществляемое по каналам связи удаленным относительно атакуемой системы субъектом и характерное для структурно- и пространственно-распределенных информационных систем.

Атакующее информационно-техническое воздействие – см. воздействие информационно-техническое атакующее.

Аттестация – комплексная проверка 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.

Аудит активный – аудит, при котором проводимые мероприятия аудита связаны 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.

Аудит внешний – аудит, который проводится внешними независимыми экспертами или с использованием технических средств и способов тестирования, находящихся вне исследуемой системы.

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

Аудит детектирующий – аудит, направленный на обнаружение новых или уточнение особенностей уже имеющихся угроз и уязвимостей системы защиты во время или после инцидентов ИБ.

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.

Аудит комбинированный – аудит, который проводится с использованием способов аудита, как на основе анализа рисков, так и на основе анализа стандартов информационной безопасности.

Аудит корректирующий – аудит, направленный на формирование комплекса мер повышения эффективности существующей системы защиты после инцидентов ИБ с учетом вновь выявленных угроз и уязвимостей.

Аудит на основе «белого ящика» – аудит, при котором аудитор имеет доступ к полной информации о структуре и функционировании исследуемой системы.

Аудит на основе «серого ящика» – аудит, при котором аудитору частично известно о параметрах исследуемой системы, но информация обо всех принципах ее функционирования и структуры являются скрытыми от него.

Аудит на основе «черного ящика» – аудит, при котором информация о параметрах, структуре и принципах функционирования исследуемой системы является изначально недоступной для аудитора.

Аудит на основе анализа рисков – аудит, который проводится с использованием формальных методов анализа рисков, когда аудитор определяет для исследуемой системы индивидуальный набор требований ИБ, в наибольшей степени учитывающий особенности данной системы, среды ее функционирования и характерные угрозы безопасности.

Аудит на основе анализа стандартов информационной безопасности – аудит, который проводится путем сравнения определенных параметров системы с требованиями стандартов ИБ.

Аудит на основе экспериментальных исследований – аудит, который проводится с применением против исследуемой системы средств и способов ИТВ или ИПВ с целью практической проверки эффективности технических или организационных мер защиты, а также выявления новых уязвимостей системы.

Аудит организационно-нормативный – аудит, при котором анализируется организационные мероприятия обеспечения ИБ и нормативные акты в данной сфере.

Аудит пассивный – аудит, при котором проводимые мероприятия аудита не вносят изменений в реальный объект аудита и не переводят его в другое состояние.

Аудит превентивный – аудит, направленный на превентивное выявление угроз и уязвимостей и предотвращение инцидентов ИБ.

Аудит технический – аудит, при котором анализируются технические средства и способы обеспечения ИБ.

Аудит экспертный – аудит, при котором процесс выявления недостатков и уязвимостей системы производится на основе имеющегося опыта экспертов, участвующих в нем.

Блокирующее информационно-техническое воздействие – см. воздействие информационно-техническое блокирующее.

Вирус – программа, несанкционированно внедренная в информационную систему и способная осуществлять создание собственных дубликатов (не всегда совпадающих с оригиналом), несанкционированное самораспространение, несанкционированный доступ к информационным ресурсам, изменение логики функционирования зараженной программы, снижение качества или эффективности информационной системы.

Вирус компьютерный – см. вирус.

Вирусная компьютерная разведка – см. разведка компьютерная вирусная.

Внешнее тестирование – см. тестирование внешнее.

Внешний аудит – см. аудит внешний.

Внутреннее тестирование – см. тестирование внутреннее.

Внутренний аудит – см. аудит внутренний.

Внушение – см. суггестия.

Воздействие информационное – воздействие на психику человека или группы людей за счет манипуляцией информацией и способом ее доведения.

Воздействие информационно-психологическое – информационное, психотронное или психофизическое воздействие на психику человека или группы людей, оказывающее влияние на восприятие ими реальной действительности, в том числе на их поведенческие функции, а, в некоторых случаях, и на функционирование органов и систем человеческого организма [56].

Воздействие информационно-техническое – 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 вызвать заданные структурные или функциональные изменения.

Воздействие информационно-техническое активное – информационно-техническое воздействие, которое оказывает непосредственное влияние на функционирование информационной системы и проявляется в активном изменении ее параметров, среды функционирования, нарушении принятой в ней политики безопасности.

Воздействие информационно-техническое атакующее – информационно-техническое воздействие, которое ориентировано на непосредственное воздействие на информацию, системы ее сбора, передачи, хранения, обработки и представления, а также на используемые в этих системах информационные технологии, как правило, с целью снижения уровня информационной безопасности или эффективности функционирования.

Воздействие информационно-техническое блокирующее – информационно-техническое воздействие, которое ориентировано на блокировку атакующих информационно-технических воздействий со стороны нарушителя/противника.

Воздействие информационно-техническое высокоточное – информационно-техническое воздействие, которое ориентировано на определенный информационный ресурс, процесс, технический объект или систему;

Воздействие информационно-техническое выявляющее – информационно-техническое воздействие, которое ориентировано на выявление, как самого факта, так и последовательности действий атакующих и обеспечивающих информационно-технических воздействий со стороны нарушителя/противника.

Воздействие информационно-техническое комплексное – информационно-техническое воздействие, которое ориентировано на несколько информационных ресурсов, процессов, технических объектов или систем.

Воздействие информационно-техническое контратакующее – информационно-техническое воздействие, которое ориентировано на блокировку ата-

кующих информационно-технических воздействий со стороны нарушителя/ противника.

Воздействие информационно-техническое обеспечивающее – информационно-техническое воздействие, которое ориентировано на сбор данных, обеспечивающих эффективное применение оборонительных или атакующих информационно-технических воздействий, а также на преодоление средств защиты атакуемой системы.

Воздействие информационно-техническое оборонительное – информационно-техническое воздействие, которое ориентировано на противодействие обеспечивающим и атакующим информационно-техническим воздействиям нарушителя/противника.

Воздействие информационно-техническое отвлекающее – информационно-техническое воздействие, которое ориентировано на дезинформацию нарушителя/противника, отвлечение его атакующих или обеспечивающих информационно-технических воздействий на незначащие или ложные объекты.

Воздействие информационно-техническое пассивное – информационно-техническое воздействие, которое не оказывает непосредственного влияния на функционирование информационной системы, но может нарушать ее политику безопасности.

Воздействие психотронное – воздействие технических средств на физическое состояние и сознание человека.

Воздействие психофизическое – скрытое насильственное воздействие на подсознание человека с целью модификации его сознания, поведения и физиологического состояния в нужном для воздействующей стороны направлении [58].

Высокоточное информационно-техническое воздействие – см. воздействие информационно-техническое высокоточное.

Выявляющее информационно-техническое воздействие – см. воздействие информационно-техническое выявляющее.

Детектирующий аудит информационной безопасности – см. аудит детектирующий.

Детерминированное тестирование – см. тестирование детерминированное.

Динамическое тестирование – см. тестирование динамическое.

Закладка аппаратная – электронное устройство, скрытно внедряемое к остальным элементам и способное вмешиваться в работу аппаратных или технических средств информационной системы.

Закладка программная – скрытно внедренная в защищенную информационную систему программа либо намеренно измененный фрагмент программы, которая позволяет осуществлять несанкционированный доступ к ресурсам системы на основе изменения свойств системы защиты [45].

Интеграционное тестирование – см. тестирование интеграционное.

Информационное воздействие – см. воздействие информационное.

Информационной процесс – процесс получения, создания, сбора, обработки, накопления, хранения, поиска, распространения, представления и использования информации.

Информационно-психологическое воздействие – см воздействие информационно-психологическое.

Информационно-техническое воздействие – см. воздействие информационно-техническое.

Информационный ресурс – отдельный массив информации, который представлен в форме документов, массивов сведений, баз данных, баз знаний или других форм организованного представления информации.

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

Комбинированный аудит – см. аудит комбинированный.

Комплексное информационно-техническое воздействие – см. воздействие информационно-техническое комплексное.

Компонентное тестирование – см. тестирование модульное.

Компьютерная разведка – см. разведка компьютерная.

Компьютерная сеть – см. сеть компьютерная.

Компьютерный вирус – см. вирус.

Контратакующее информационно-техническое воздействие – см. воздействие информационно-техническое контратакующее.

Корректирующий аудит информационной безопасности – см. аудит корректирующий.

Критическая информационная инфраструктура – совокупность информационные систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, функционирующих в интересах государственных органов и государственных учреждений, организаций здравоохранения, науки, транспорта, связи, энергетики, банковской и финансовой сферы, топливно-энергетического комплекса, атомной энергетики, оборонной, горнодобывающей, металлургической, химической, ракетно-космической промышленности, а также сети связи, используемые для организации взаимодействия между ними.

Легальное тестирование – см. тестирование легальное.

Легальный аудит – аудит, который проводится в рамках существующего законодательства, как правило, на основании договора аудитора с заказчиком, имеющим прямое отношение к обеспечению безопасности объекта аудита.

Манипуляция психологическая – процесс целенаправленного использования различных способов и средств изменения поведения, целей, желаний, намерений, отношений, установок, психических состояний и других психологических характеристик человека в интересах субъекта воздействия [68].

Модель аудита – формализованное описание: объекта аудита; цели аудита; предъявляемых требований к защищенности объекта аудита; используемых при аудите практических и теоретических подходов; масштаба и глубины аудита; исполнителей; порядка проведения аудита.

Модель нарушителя – формализованное описание нарушителя: категорирование нарушителей; формальные количественные предположения о квалификации, возможностях, располагаемых средствах и способах информационного воздействия для каждой категории нарушителей; сценарии действий каждой категории нарушителей; уровень полномочий и способы получения доступа к системе для каждой категории нарушителей; критерии нарушения ИБ.

Модель противника – формализованное описание противника: категорирование противников; формальные количественные предположения о ресурсах, возможностях, располагаемых средствах и способах информационного воздействия для каждой категории противников; сценарии ИТВ и ИПВ для каждой категории противников; уровень полномочий и способы получения доступа к системе для каждой категории противника; критерии нарушения ИБ; показатели и критерии достижения информационного превосходства.

Модульное тестирование – см. тестирование модульное

Нарушитель – субъект, преднамеренно использующий уязвимости технических и нетехнических мер и средств контроля и управления безопасностью информационной системы с целью снижения их эффективности или снижения уровня конфиденциальности, доступности и целостности информационных ресурсов.

Нелегальное тестирование – см. тестирование нелегальное.

Нелегальный аудит – аудит, который основан на получении информации об уязвимостях исследуемой системы нелегальными противозаконными способами.

Несанкционированный доступ – доступ к информации, нарушающий установленные правила разграничения доступа [69].

Обеспечивающее информационно-техническое воздействие – см. воздействие информационно-техническое обеспечивающее.

Оборонительное информационно-техническое воздействие – см. воздействие информационно-техническое оборонительное.

Объект воздействия – человек, группа лиц, организационно-техническая система или техническое средство, которое подвергается воздействию со стороны субъекта воздействия.

Оптикоэлектронная разведка – процесс добывания информации с помощью средств, включающих входную оптическую систему с фотоприемником и электронные схемы обработки электрического сигнала, которые обеспечивают прием и анализ электромагнитных волн видимого и ИК-диапазонов, излученных или отраженных объектами и местностью [39].

Организационно-нормативный аудит – см. аудит организационно-нормативный.

Отвлекающее информационно-техническое воздействие – см. воздействие информационно-техническое контратакующее.

Оценка соответствия – доказательство того, что заданные требования к продукции, процессу, системе, лицу или органу выполнены.

Пассивное информационно-техническое воздействие – см. воздействие информационно-техническое пассивное.

Пассивное тестирование – см. тестирование пассивное.

Пассивный аудит – см. аудит пассивный.

Пользовательская компьютерная разведка – см. разведка компьютерная *пользовательская.*

Потоковая компьютерная разведка – см. разведка компьютерная потоковая.

Превентивный аудит информационной безопасности – см. аудит превентивный.

Программная закладка – см. закладка программная.

Противник – субъект, с которым ведется противоборство, соперничество или соревнование в военной, информационной, спортивной или в другой сфере с целью достижения выигрыша.

Психологическая манипуляция – см. манипуляция психологическая.

Психотронное воздействие – см. воздействие психотронное.

Психофизическое воздействие – см. воздействие психофизическое.

Радиоразведка – составная часть радиоэлектронной разведки, ориентированная на добывание сведений в системах радиосвязи, основным содержанием которой является: обнаружение и перехват открытых, засекреченных, кодированных передач; пеленгование их источников; анализ и обработка добываемой информации; снижение нагрузки или подрыв криптографических систем [39].

Радиоэлектронная разведка – см. разведка радиоэлектронная.

Разведка компьютерная – добывание информации из компьютерных систем и сетей, характеристик их программно-аппаратных средств и пользователей [1].

Разведка компьютерная алгоритмическая – разведка, обеспечивающая добывание информации путем использования заранее внедренных изготовителем программных или аппаратных закладок, ошибок и недекларированных возможностей компьютерных систем и сетей [40].

Разведка компьютерная аппаратная – разведка, обеспечивающая добывание информации путем обработки сведений, получения аппаратуры, оборудования, технических модулей и их анализа, испытания для выявления их технических характеристик и возможностей, полученных другими видами компьютерной разведки [40].

Разведка компьютерная вирусная – разведка, обеспечивающая добывание данных путем внедрения и применения вирусных программ в уже эксплуатируемые программные комплексы и в системы для перехвата управления компьютерными системами [40].

Разведка компьютерная пользовательская – разведка, обеспечивающая добывание информации о пользователях, их деятельности и интересах на основе определения их сетевых адресов, местоположения, организационной принадлежности, анализа их сообщений и информационных ресурсов, а также пу-

тем обеспечения им доступа к информации, циркулирующей в специально созданной ложной информационной инфраструктуре [40].

Разведка компьютерная потоковая – разведка, обеспечивающая добывание информации путем перехвата, обработки и анализа сетевого трафика, выявления структур компьютерных сетей, а также их технических параметров [40].

Разведка компьютерная разграничительная – разведка, обеспечивающая добывание информации из отдельных (локальных) компьютерных систем, которые могут не входить в состав сети и осуществляемая на основе преодоления средств разграничения доступа путем несанкционированного доступа к информации, физического доступа к компьютерной системе или к носителям информации [40].

Разведка компьютерная семантическая – разведка, обеспечивающая добывание фактографической и индексно-ссылочной информации путем поиска, сбора и анализа структурируемой и неструктурируемой информации из общедоступных информационных ресурсов или конфиденциальных источников компьютерных систем и сетей, а также путем семантической (аналитической) обработки полученных и накопленных массивов сведений и документов [40].

Разведка компьютерная сетевая – разведка, обеспечивающая добывание информации из компьютерных сетей путем мониторинга сети, инвентаризации и анализа уязвимостей сетевых ресурсов и объектов пользователей, а также последующего удаленного доступа к информации путем использования выявленных уязвимостей систем и средств сетевой (межсетевой) защиты ресурсов, а также блокирование доступа к ним, модификация, перехват управления либо маскировка своих действий [40].

Разведка компьютерная форматная – разведка, обеспечивающая добывание информации путем агрегированной обработки, фильтрации, декодирования, а также проведения других преобразований форматов (представления, передачи и хранения) добытых данных в сведения, а затем – в информацию для последующего ее наилучшего представления пользователям [40].

Разведка радиоэлектронная – процесс получения информации в результате приема и анализа электромагнитных излучений радиодиапазона, создаваемых работающими радиоэлектронными средствами.

Разведка техническая – целенаправленная деятельность по добыванию информации с помощью соответствующих технических средств.

Разграничительная компьютерная разведка – см. разведка компьютерная разграничительная.

Семантическая компьютерная разведка – см. разведка компьютерная *семантическая.*

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

Сетевая компьютерная разведка – см. разведка компьютерная сетевая.

Сеть компьютерная – объединение компьютерных систем путем включения их в сеть связи или соединения их линиями связи [40].

Системное тестирование – см. тестирование системное.

Способ информационно-технического воздействия – порядок применения сил информационных операций и средств информационно-технического воздействия, вызывающий заданные структурные и/или функциональные изменения в объекте воздействия.

Средство информационно-технического воздействия – техническое, аппаратное или программное средство, реализующее информационно-техническое воздействие или защиту от него.

Статическое тестирование – см. тестирование статическое.

Стохастическое тестирование – см. тестирование стохастическое.

Субъект воздействия – источник, реализующий воздействия на объект целью достижения своих интересов.

Суггестия – целенаправленное воздействие на личность или группу людей (массовое внушение), воспринимаемое на уровне подсознания и приводящее либо к появлению определенного состояния духа, чувства, отношения, либо к совершению определенных поступков [58].

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

Тестирование – это техническая операция, заключающаяся в определении одной или нескольких характеристик продукта, процесса или услуги соответствующей процедуре.

Тестирование активное – тестирование, которое предусматривает целенаправленное воздействие на объект исследования с целью анализа его реакций или перевода его в требуемое состояние, как правило, с более низким уровнем защищенности или эффективности функционирования.

Тестирование внешнее – тестирование, которое проводится с использованием средств и способов, находящихся вне тестируемого объекта.

Тестирование внутреннее – тестирование, которое проводится с использованием средств и способов, находящихся внутри защищаемого периметра тестируемого объекта.

Тестирование детерминированное – тестирование, при котором параметры тестирования динамически изменяются по детерминированным законам.

Тестирование динамическое – тестирование объекта на основе динамически изменяющихся наборах входных данных, условиях функционирования, структуре, и т. д.

Тестирование интеграционное – тестирование, которое ориентировано на проверку взаимодействия между элементами исследуемого объекта.

Тестирование легальное – тестирование, которое проводится в рамках существующего законодательства, как правило, на основании договора с заказчиком.

Тестирование модульное – тестирование, которое ориентировано на проверку функционирования отдельно взятого элемента, модуля или компонента исследуемого объекта.

Тестирование на основе «белого ящика» – тестирование, при котором имеется доступ к полной информации о структуре и функционировании исследуемой системы.

Тестирование на основе «серого ящика» – тестирование, при котором частично известно о параметрах исследуемой системы, но информация обо всех принципах ее функционирования и структуры являются скрытыми.

Тестирование на основе «черного ящика» – тестирование, при котором информация о параметрах, структуре и принципах функционирования исследуемой системы является изначально недоступной.

Тестирование на основе моделей – теоретический подход к тестированию, основанный на построении соответствующих моделей и их исследовании.

Тестирование нелегальное – тестирование, которое основано на получении информации об уязвимостях исследуемой системы нелегальными противозаконными способами.

Тестирование пассивное – тестирование, которое не вносит изменений в реальный объект исследования или в его модель-прототип, а также не переводит их в измененное состояние.

Тестирование системное – тестирование, которое охватывает целиком весь объект и его внешние интерфейсы, а также среду функционирования.

Тестирование специальными средствами и способами – практический подход к тестированию, в основе которого лежат эксперименты по использованию средств и способов информационных воздействий против объекта тестирования или его прототипа.

Тестирование статическое – 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.

Тестирование стохастическое – тестирование, при котором параметры тестирования динамически изменяются по вероятностным законам.

Техническая разведка – см. разведка техническая.

Технический аудит – см. аудит технический.

Троян – вирус, основной целью которого является дестабилизирующее воздействие на информационную систему путем выполнения несанкционированных действий, связанных, как правило, с нарушением работоспособности и безопасности информационной системы, снижением ее эффективности, изменением логики ее функционирования, а также несанкционированным использованием ее ресурсов.

Удаленная сетевая атака – см. атака сетевая удаленная.

Форматная компьютерная разведка – см. разведка компьютерная форматная.

Червь – вирус, распространяющийся по сетям и каналам связи и способный к самостоятельному преодолению подсистем защиты информационных систем, а также к созданию и дальнейшему распространению своих дубликатов (необязательно совпадающих с оригиналом).

Экспериментальный аудит – см. аудит на основе экспериментальных исследований.

Экспертный аудит – см. аудит экспертный.

Эксплойт – потенциально невредоносный набор данных, который некорректно обрабатывается информационной системой, работающей с такими данными, вследствие ошибок в ней. Результатом некорректной обработки такого набора данных может быть перевод информационной системы в уязвимое состояние.

Литература

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

2. 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 (дата обращения: 01.06.2018).

3. 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: 01.06.2018).

4. 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.

5. Аверичников В. И. Аудит информационной безопасности. Учебное пособие для вузов. – Брянск: БГТУ, 2012. – 268 с.

6. Иванова Н. В., Коробулина О. Ю. Аудит информационной безопасности. Учебное пособие. – СПб.: ПГУПС, 2011. – 57 с.

7. Корниенко А. А., Диасамидзе С. В. Аудит и управление информационной безопасностью. Учебное пособие. – СПб.: ПГУПС, 2011. – 82 с.

8. Петренко А. А., Петренко С. А. Аудит безопасности Internet. Монография. – М.: ДМК Пресс, 2010. – 388 с.

9. 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.

10. 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.

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

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

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

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

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

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

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

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

21. 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.

22. 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.

23. 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.

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

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

26. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». – М., 2017.

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

28. 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.

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

30. 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.

31. 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.

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

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

34. 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.

35. Петренко А. А., Петренко С. А. Кибероружения: методические рекомендации ENISA // Вопросы кибербезопасности. 2015. № 3 (11). С. 2-14.

36. Емельянов С. Л. Техническая разведка и технические каналы утечки информации // Системи обробки інформації. 2010. № 3 (84). С. 20-23.

37. Чукляев И. И., Морозов А. В., Болотин И. Б. Теоретические основы оптимального построения адаптивных систем комплексной защиты информационных ресурсов распределенных вычислительных систем: монография. – Смоленск: ВА ВПВО ВС РФ, 2011. – 227 с.

38. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. – К.: Юниор, 2003. – 504 с.

40. Меньшаков Ю. К. Теоретические основы технических разведок: учеб. пособие / Под ред. Ю.Н. Лаврухина. – М.: МГТУ им. Н.Э. Баумана, 2008. – 536 с.

41. Варламов О. О. О системном подходе к созданию модели компьютерных угроз и ее роли в обеспечении безопасности информации в ключевых системах информационной инфраструктуры // Известия ЮФУ. Технические науки. 2006. № 7 (62). С. 216-223.

42. Пахомова А. С., Пахомов А. П., Юрасов В. Г. Об использовании классификации известных компьютерных атак в интересах разработки структурной модели угрозы компьютерной разведки // Информация и безопасность. 2013. Т. 16. № 1. С. 81-86.

43. Barnum S. Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description // Cigital Inc. 2008. Vol. 3.

44. Ларина Е. С., Овчинский В. С. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. – М.: Книжный мир, 2014. – 352 с.

45. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – М.: Стандартинформ, 2007. — 11 с. – URL: http://docs.cntd.ru/document/gost-r-51275-2006 (дата обращения: 14.08.2016).

46. Куприянов А. И., Сахаров А. В., Шевцов В. А. Основы защиты информации: учебное пособие. – М.: Издательский центр «Академия», 2006. – 256 с.

47. Дождиков В. Г., Салтан М. И. Краткий энциклопедический словарь по информационной безопасности. – М.: ИАЦ Энергия, 2010. – 240 с.

48. Виноградов А. А. Функциональность, надежность, киберустойчивость в системах автоматизации критических инфраструктур [Доклад] // Конференция «Региональная информатика-2012». – СПб.: ОАО «НПО «Импульс», 2012.

49. Емелин В. И. Информационно-психологическая безопасность АСУ критических систем. – СПб.: Профессиональная литература, 2012. – 76 с.

50. Присняков В. Ф., Приснякова Л. М. Математическое моделирование переработки информации оператором человеко-машинных систем. – М.: Машиностроение, 1990. – 248 с.

51. Сергеев С. Ф. Инженерная психология и эргономика. – М.: НИИ ШТ, 2008. – 174 с.

52. Сергеев С. Ф. Эргономика объектов вооружения. Монография. – Тула, 2003. – 123 с.

53. Крысько В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт). — Мн: Харвест, 1999. – 448 с. – URL: http://www.e-reading.club/bookreader.php/1005378/Vladimir_-_Sekrety_psihologicheskoy_voyny.html (дата обращения: 30.06.2018).

54. Караяни А. Г., Зинченко Ю. П. Информационно-психологическое противоборство в войне: история, методология, практика: учебник для курсантов и студентов вузов. – М.: МГУ, 2007. – 172 с.

55. Сидорин А. Н. Прищепов В. М., Акуленко В. П. Вооруженные силы США в XXI веке: военно-теоретический труд. – М.: Кучково поле; Военная книга, 2013. – 800 с.

56. Баришполец В. А. Информационно-психологическая безопасность: основные положения // Информационные технологии. 2003. Том 3. № 2. С. 69-104.

57. Назаров Д. В., Ахмедзянов В. Р. Психотронное оружие. Воздействие скрытых команд на подсознание человека // Вестник РУДН. Серия: Экология и безопасность жизнедеятельности. 2008. № 4 С. 49-54. — URL: http://cyberleninka.ru/article/n/psihotronnoe-oruzhie-vozdeystvie-skrytyh-komand-na-podsoznanie-cheloveka (дата обращения: 23.01.2018).

58. Паршакова Е. Д. Информационные войны: учебное пособие. – Краматорск: ДГМА, 2012. – 92 с.

59. Караяни А. Г. Информационно-психологическое противоборство в современной войне // ArmyRus. Военно-информационный портал [Электронный ресурс]. 16.08.2014. – URL: http://armyrus.ru/index.php?option=com_content&task=view&id=739 (дата обращения: 30.06.2016).

60. Микрюков В. Победа в войне должна быть достигнута еще до первого выстрела // Независимое военное обозрение [Электронный ресурс]. 15.01.2016. — URL: http://nvo.ng.ru/concepts/2016-01-15/10_infowar.html (дата обращения: 30.06.2019).

61. Остапенко Г. А., Мешкова Е. А. Информационные операции и атаки в социотехнических системах: организационно-правовые аспекты

противодействия: учебное пособие / под редакцией Ю.Н. Лаврухина. – М: Горячая линия - Телеком, 2007. – 295 с.

62. Еременко В. Т. Рязанцев П. Н. Информационное противоборство в социотехнических системах: учебное пособие. – Орел: ОГУ им. И.С. Тургенева, 2016. – 209 с.

63. Зелинский С. А. Манипулирование личностью и массами. Манипулятивные технологии власти при атаке на подсознание индивида и масс. – СПб.: Издательско-торговый дом «Скифия», 2008. – 240 с.

64. Зелинский С. А. Информационно-психологическое воздействие на массовое сознание. Средства массовой коммуникации, информации и пропаганды — как проводник манипулятивных методик воздействия на подсознание и моделирования поступков индивида и масс. – СПб.: Издательско-торговый дом «Скифия», 2008. – 280 с.

65. Список когнитивных искажений // Википедия [Электронный ресурс]. 2018. – URL: https://ru.wikipedia.org/wiki/Список_когнитивных_искажений (дата обращения: 25.07.2018).

66. Шейнов В. П. Скрытое управление человеком. – М.: Издательство АСТ, 2001.

67. Чалдини Р. Психология влияния. – СПб.: Питер, 2006.

68. Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. – М.: Издательство РАГС, 1998. – 125 с.

69. ГОСТ Р 50922-96 Защита информации. Основные термины и определения. – М, 1996.

70. Расторгуев С. П. Математические модели в информационном противоборстве. Экзистенциальная математика. – М.: АНО ЦСОиП, 2014. – 260 с.

71. Губанов Д. А., Новиков Д. А., Чхартишвили А. Г. Социальные сети: модели информационного влияния, управления и противоборства / Под ред. чл.-корр. РАН Д.А. Новикова. – М.: Издательство физико-математической литературы, 2010. – 228 с.

72. Бухарин С. Н., Цыганов В. В. Методы и технологии информационных войн. – М.: Академический проект, 2007. – 382 с.

73. Абрамов М. В., Тулупьев А. Л., Сулейманов А. А. Задачи анализа защищенности пользователей от социоинженерных атак: построение социального графа по сведениям из социальных сетей // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 2. С. 313-321.

74. Абрамов М. В., Азаров А. А., Тулупьева Т. В., Тулупьев А. Л. Модель профиля компетенций злоумышленника в задаче анализа защищённости персонала информационных систем от социоинженерных атак // Информационно-управляющие системы. 2016. № 4 (83). С. 77-84.

75. Азаров А. А., Абрамов М. В., Тулупьева Т. В., Тулупьев А. Л. Анализ защищённости групп пользователей информационной системы от социоинженерных атак: принцип и программная реализация // Компьютерные инструменты в образовании. 2015. № 4. С. 52-60.

76. Тулупьев А. Л. Анализ степени защищенности от социоинженерных атак: задачи и подходы к их решению // Лавровские чтения 2014. Материалы пленарных докладов всероссийской научной конференции по проблемам информатики. 2014. С. 88-99.

77. Тулупьева Т. В., Тулупьев А. Л., Азаров А. А. Психологические аспекты оценки безопасности информации в контексте социоинженерных атак // Медико-биологические и социально-психологические проблемы безопасности в чрезвычайных ситуациях. 2013. № 1. С. 77-83.

78. Тулупьева Т. В., Азаров А. А., Тулупьев А. Л. Социоинженерные атаки как вид социального воздействия // Научные труды Северо-Западного института управления. 2013. Т. 4. № 4 (11). С. 100-110.

79. Монахов М. Ю., Полянский Д. А., Монахов Ю. М., Семенова И. И. Концепция управления процессом обеспечения достоверности информации в ИТКС в условиях информационного противодействия // Фундаментальные исследования. 2014. № 9. С. 2397-2402.

80. Джан Р. Г. Нестареющий парадокс психофизических явлений. Инженерный подход // Труды института инженеров по электротехнике и радиоэлектронике. 1982. Т. 70. № 3. С. 63-104.

81. Аллахвердов В. М., Агафонов А. Ю., Вишнякова Е. А., Волохонский В. Л., Воскресенская Е. Ю., Гершкович В. А., Иванов М. В., Иванова Е. Н., Иванова Н. А., Карпинская В. Ю., Кувалдина М. Б., Ледовая Я. А., Морошкина Н. В., Науменко О. В., Сергеев С. Ф., Филиппова М. Г. Экспериментальная психология познания: когнитивная логика сознательного и бессознательного. – СПб. СПбГУ, 2006. – 352 с.

82. Аллахвердов В. М., Воскресенская Е. Ю., Науменко О. В. Сознание и когнитивное бессознательное // Вестник Санкт-Петербургского университета. Серия 12. Психология. Социология. Педагогика. 2008. № 2. С. 10-19.

83. Климов С. М. Модель бескомпроматного аудита информационной безопасности сети спутниковой связи // Двойные технологии. 2013. №3 (64). С. 15-20.

84. 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.

85. 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.

86. Бойко А. А., Обущенко Е. Ю., Щеглов А. В. Особенности синтеза полного множества тестовых способов удаленного информационнотехнического воздействия на пространственно распределенные системы информационно-технических средств // Вестник Воронежского государственного университета. Серия: Системный анализ и информационные технологии. 2017. № 2. С. 33-45.

87. 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.

88. Петренко С. А., Курбатов В. А., Петренко А. С. Автоматизация аудита информационной безопасности на основе SAP ETD // Защита информации. Инсайд. 2018. № 2 (80). С. 12-17.

89. Максименко В. Н., Ясюк Е. В. Основные подходы к анализу и оценке рисков информационной безопасности // Экономика и качество систем связи. 2017. № 2 (4). С. 42-48.

90. Хмелюкова С. О., Ситнов А. А. Конвенция аудита информационной безопасности // Аудиторские ведомости. 2017. № 11. С. 6-12.

91. Воеводин В. А. Аудит информационной безопасности // Современные проблемы и задачи обеспечения информационной безопасности. Труды Международной научно-практической конференции «СИБ - 2016». – 2016. – С. 35-42.

92. Новикова Т. Л., Надеждин Е. Н. Информационное обеспечение внутреннего аудита информационной безопасности образовательной организации // Комплексная защита объектов информатизации – 2016. Сборник научных трудов Всероссийской научно-практической конференции с международным участием. – 2016. – С. 48-51.

93. Надеждин Е. Н., Новикова Т. Л. Интеллектуальный анализ материалов аудита информационной безопасности // Информационные технологии в науке, образовании и управлении. Материалы XLIV международной конференции и XIV международной конференции молодых учёных IT + S&E`16. – 2016. – С. 60-65.

94. Надеждин Е. Н., Новикова Т. Л. Информационно-аналитическая поддержка деятельности аудитора информационной безопасности // Фундаментальные исследования. 2016. № 10-1. С. 67-72.

95. Козьминых С. И., Козьминых П. С. Аудит информационной безопасности // Вестник Московского университета МВД России. 2016. № 1. С. 181-186.

96. Кузнецова А. П., Файман О. И. О методиках оценки информационных рисков // Информационные технологии и автоматизация управления. Материалы VI Всероссийской научно-практической конференции студентов, аспирантов, работников образования и промышленности. – 2015. – С. 136-139.

97. Баранова Е. К., Худышкин А. А. Особенности анализа безопасности информационных систем методом тестирования на проникновение // Моделирование и анализ безопасности и риска в сложных системах. Труды международной научной школы МАБР - 2015. – С. 200-205.

98. Кураленко А. И. Методика аудита информационной безопасности информационных систем // Проблемы информационной безопасности. Компьютерные системы. 2015. № 4. С. 48-51.

99. Будовских И. А., Загинайлов Ю. Н., Алферова Л. Д. Автоматизация аудита информационной безопасности кредитных организаций основанного на стандартах банка России // Ползуновский альманах. 2015. № 1. С. 122-125.

100. Баранова Е. К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. 2015. № 1 (9). С. 73-79.

101. Машкина И. В., Сенцова А. Ю. Автоматизация экспертного аудита информационной безопасности на основе использования искусственной нейронной сети // Безопасность информационных технологий. 2014. Т. 21. № 2. С. 65-70.

102. Баранова Е. К., Чернова М. В. Сравнительный анализ программного инструментария для анализа и оценки рисков информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. 2014. № 4. С. 160-168.

103. Лившиц И. И. Стандарты ISO/IEC, ITIL и COBIT в контексте требований к информационной безопасности // Менеджмент качества. 2013. № 2. С. 94-106.

104. Иванова Н. В., Коробулина О. Ю. Аудит информационной безопасности. – СПб.: ПГУПС, 2011. – 57 с.

105. Дорофеев А. Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? // Защита информации. Инсайд. 2010. № 6 (36). С. 72-73.

106. Фомин А. А. Исследование и оптимизация алгоритмов аудита информационной безопасности организации // Вопросы защиты информации. 2009. № 3 (86). С. 57-63.

107. Харжевская (Зотова) А. В., Ломако А. Г., Петренко С. А. Аудит безопасности на основе многослойных инвариантов подобия // Защита информации. Инсайд. 2018. № 2 (80). С. 22-33.

108. Умницын М. Ю. Подход к полунатурному анализу защищенности информационной системы // Известия Волгоградского государственного технического университета. 2018. № 8 (218). С. 112-116.

109. Бородин М. К., Бородина П. Ю. Тестирование на проникновение средства защиты информации VGATE R2 // Региональная информатика и информационная безопасность. – СПб., 2017. – С. 264-268.

110. 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.

112. Полтавцева М. А., Печенкин А. И. Интеллектуальный анализ данных в системах поддержки принятия решений при тестировании на проникновение // Проблемы информационной безопасности. Компьютерные системы. 2017. № 3. С. 62-69.

113. Кадан А. М., Доронин А. К. Инфраструктурные облачные решения для задач тестирования на проникновение // Ученые записки ИСГЗ. 2016. Т. 14. № 1. С. 296-302.

114. Еременко Н. Н., Кокоулин А. Н. Исследование методов тестирования на проникновение в информационных системах // Master's Journal. 2016. № 2. С. 181-186.

115. Туманов С. А. Средства тестирования информационной системы на проникновение // Доклады Томского государственного университета систем управления и радиоэлектроники. 2015. № 2 (36). С. 73-79.

116. Кравчук А. В. Модель процесса удаленного анализа защищенности информационных систем и методы повышения его результативности // Труды СПИИРАН. 2015. № 1 (38). С. 75-93.

117. Горбатов В. С., Мещеряков А. А. Сравнительный анализ средств контроля защищенности вычислительной сети // Безопасность информационных технологий. 2013. Т. 20. № 1. С. 43-48.

118. Косенко М.Ю. Сбор информации при проведении тестирования на проникновение // Вестник УрФО. Безопасность в информационной сфере. 2013. № 3 (9). С. 11-15.

119. Рытов М. Ю., Лексиков Е. В., Ковалев П. А. Использование нечеткого когнитивного моделирования для проведения аудита информационной безопасности информационных порталов региональных органов исполнительной власти // Вестник Брянского государственного технического университета. 2016. № 2 (50). С. 201-206.

120. Рытов М. Ю., Горлов А. П. Автоматизация процесса оценки уровня информационной безопасности объекта информатизации // Информация и безопасность. 2014. Т. 17. № 2. С. 280-283.

121. Юрьев В. Н., Эрман С. А. Теоретико-вероятностная модель оценки рисков информационной безопасности предприятия // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Экономические науки. 2014. № 4 (199). С. 188-194.

122. Васильчук О. И. Средства компенсации угроз и аудита безопасности корпоративной информационной системы // Вестник Поволжского государственного университета сервиса. Серия: Экономика. 2013. № 4 (30). С. 127-131.

123. Найханова И. В. Виды и методики аудита информационной безопасности: состояние и анализ // Информатизация образования и науки. 2012. № 3 (15). С. 81-94.

124. Антонов С. Г., Гордеев С. В., Климов С. М., Рыжов Б. С. Модели угроз совместных-информационно-технических и информационно-психологических воздействий в гибридных войнах // Информационные войны. 2018. № 2 (46). С. 83-87.

125. Информационно-психологическая и когнитивная безопасность. Коллективная монография / Под ред. И.Ф. Кефели, Р.М. Юсупова. – СПб.: ИД «Петрополис», 2017. – 300 с.

Макаренко Сергей Иванович

Аудит безопасности критической инфраструктуры специальными информационными воздействиями
Монография

Научное издание

Рецензенты:

Климов Сергей Михайлович, доктор технических наук, профессор (4 ЦНИИ МО РФ);

Марков Алексей Сергеевич, доктор технических наук, старший научный сотрудник (АО НПО «Эшелон»);

Михайлов Роман Леонидович, кандидат технических наук (ЧВВИУРЭ);

Саенко Игорь Борисович, доктор технических наук, профессор (СПИИРАН);

Сергеев Сергей Федорович, доктор психологических наук, профессор (СПбПУ Петра Великого).

Издательство «Наукоемкие технологии»
ООО «Корпорация «Интел групп»
197372, Санкт-Петербург, пр. Богатырский, дом 32, к. 1 лит. А, пом. 6Н.
http://publishing.intelgr.com
Тел.: +7 (812) 945-50-63
E-mail: publishing@intelgr.com

ISBN 978-5-6041427-8-3

Гарнитура «TimesNewRoman». 5,86 п.л.
Тираж 600 экз. Подписано в печать 01.11.2018.

Материалы изданы в авторской редакции

Макаренко Сергей Иванович – кандидат технических наук, доцент. Профессор Академии военных наук.

Родился в 1980 году в Ставрополе. В 2002 году окончил Военный авиационный технический университет имени проф. Н. Е. Жуковского (филиал в г. Ставрополь) по специальности «Автоматизированные системы управления и обработки информации».

В 2007 году в Ставропольском высшем военном авиационном инженером училище защитил диссертацию на соискание ученой степени кандидата технических наук по специальности «Вооружение и военная техника. Комплексы и системы военного назначения».

В период с 2007 по 2017 годы проходил службу на должностях научного и преподавательского состава в Ставропольском высшем военном авиационном инженером училище, в ВУНЦ ВВС «Военно-воздушная академия имени проф. Н.Е. Жуковского и Ю.А. Гагарина», в Военно-космической академии имени А.Ф. Можайского. С 2017 года – работает на предприятиях оборонно-промышленного комплекса России.