УДК 004.056.53 DOI 10.18522/2311-3103-2016-8-2736

С.М. Климов

ИМИТАЦИОННЫЕ МОДЕЛИ ИСПЫТАНИЙ КРИТИЧЕСКИ ВАЖНЫХ ИНФОРМАЦИОННЫХ ОБЪЕКТОВ В УСЛОВИЯХ КОМПЬЮТЕРНЫХ АТАК

Статья посвящена вопросам имитационного моделирования критически важных информационных объектов, компьютерных атак и средств защиты информации на стендовых полигонах информационной безопасности. Показана актуальность и важность априорной оценки реального уровня защищенности и устойчивости функционирования критически важных информационных объектов в условиях компьютерных атак в форме вредоносных программ. Целью имитационного моделирования критически важных информационных объектов является оценка их реального уровня защищенности и устойчивости функционирования в условиях компьютерных атак и применения различных вариантов средств защиты информации. Предложены определения для понятий компьютерные атаки и устойчивость функционирования критически важных информационных объектов. Определен комплекс имитационных моделей в виде совокупности сегментов критически важных информационных объектов, компьютерных атак, элементов системы предупреждения, обнаружения и ликвидации последствий компьютерных атак. Разработана имитационная модель сегментов критически важных информационных объектов в виде типовых технологических циклов управления, выполняемых за установленное время, а также временных задержек от действий компьютерных атак. Рассмотрен паспорт уязвимостей критически важных информационных объектов. В качестве угроз информационной безопасности предложено рассматривать комбинированные воздействия DDoS-атаками, информационной нагрузкой, средствами фаззинга и вредоносными программами. Определены параметры оценки средств имитации компьютерных атак и защиты от них, критерии оценки защищенности критически важных информационных объектов в условиях компьютерных атак. Особое внимание уделено модульной структуре стендового полигона для оценки защищенности критически важных информационных объектов. В заключении отмечено, что предварительные испытания на стендовом полигоне позволяют обеспечить вероятность защиты информации критически важных информационных объектов в условиях комбинированных компьютерных атак до значений 0,85–0,95 за счет своевременного устранения уязвимостей и настройки средств защиты информации.

Критически важные информационные объекты; компьютерные атаки; реальный уровень защищенности и устойчивости функционирования.

S.M. Klimov

IMITATING MODELS OF TESTING THE CRITICALLY IMPORTANT INFORMATION OBJECTS IN THE CONDITIONS OF COMPUTER ATTACKS

The article is dedicated to the problems of imitating modeling of the critically important information objects, computer attacks and information security facilities with utilization of the special information security testbeds. Demonstrated is the topicality and importance of prior estimation for the real level of security and operation stability of critically important information objects in conditions of computer attacks in the form of injurious programs. The aim of the critically important information objects imitating modeling is estimation for the real level of information security, critically important information objects operation stability in conditions of computer attacks and using of different variants of information security facilities. In this work we propose the definitions for conceptions of a computer attack and a critically important information object operation stability. Determined is the imitation models complex in the form of a set of critical important information object segments, computer attacks and elements of the system of warning, alert and liquidation the computer attacks consequences. Developed is the imitation model of critically important information objects segments in the form of standard technological control cycles, per-

formed in set time, and time delays as a result of computer attacks. Considered is the vulnerability passport for critically important information objects. The combined impacts of DDoS-attacks, information-load, fuzzing and injurious programs are proposed to be treated as the information security threats. Determined are the parameters of estimation for computer attacks and protection imitation facilities, criteria for estimation of critically important information objects immunity in conditions of computer attacks. Special attention is devoted to a modular structure of the testbed for estimation of critically important information objects immunity. We conclude that initial tests using the testbed allow providing the probability of critically important information objects security in conditions of combined computer attacks up to 0,85–0,95 value at the expense of timely removal of vulnerabilities and information security facilities tuning.

Critically important information objects; computer attacks; real level of information security and operation stability.

Введение. В настоящее время наблюдается тенденция интенсивного увеличения числа компьютерных инцидентов, связанных с воздействием компьютерных атак на критически важные информационные объекты (КВИО) через глобальные информационные сети, магистральное цифровое коммуникационное оборудование и несанкционированное подключение внешних электронных носителей информации.

К критически важным информационным объектам относятся современные компьютеризированные элементы и информационные ресурсы систем управления энергетики, транспорта, связи, городской инфраструктуры, промышленных предприятий.

К новым и наиболее опасным средствам реализации компьютерных атак, выявленным в современных КВИО, относятся скрытно проникающие через вычислительные сети вредоносные программы, например: Stuxnet, Reign, Wiper, Shamoon [16].

Указанные вредоносные программы реализованы на промышленной и унифицированной программной платформе, скрытно внедряют свой код в КВИО, собирают информацию об уязвимостях, развертывают атакующую сеть (до десятков тысяч компьютеров в глобальной или корпоративной сети) и по команде реализуют массированные воздействия на «зараженные» объекты.

С целью обеспечения необходимого уровня информационной безопасности КВИО целесообразно заблаговременно оценить их реальный уровень защищенности и устойчивости функционирования в условиях компьютерных атак. В связи с тем, что на реальных объектах проводить проверки в условиях компьютерных атак весьма затруднительно и трудоемко, предлагается развертывать стендовые полигоны с сегментами (имитационными моделями) КВИО для тестирования их в условиях компьютерных атак [7–10].

Применение технологий виртуальных машин и облачных вычислений на стендовых полигонах позволяет сэкономить ресурсы на развертывание имитационных моделей сегментов КВИО, средств защиты информации и имитаторов компьютерных атак.

Под компьютерной атакой будем понимать целенаправленное программное (или программно-аппаратное) воздействие на КВИО, осуществляемое в целях нарушения безопасности информации и устойчивости функционирования объекта.

Устойчивость функционирования КВИО определим, как способность объекта обеспечивать установленные регламенты выполнения технологических циклов управления (вероятностно-временные характеристики) в условиях компьютерных атак.

В последнее время в электронных публикациях появилось понятие таргетированных атак, в качестве которых и рассматриваются целевые компьютерные атаки, разработанные с учетом специфики работы КВИО и его уязвимостей [1]. Противодействие таким сложным скрытно внедряемым и удаленно управляемым компьютерным атакам возможно только путем априорного анализа их структуры, функций и кода на стендовом полигоне совместно с элементами КВИО и средствами защиты информации.

Постановка задачи. Для решения задачи оценки реального уровня защищенности и устойчивости функционирования КВИО в условиях компьютерных атак на стендовом полигоне необходим комплекс имитационных моделей: сегментов КВИО, компьютерных атак, элементов системы предупреждения, обнаружения и ликвидации последствий компьютерных атак (СОПКА).

Имитационные модели, позволяющие исследовать динамические процессы реализации массированных и целенаправленных компьютерных атак, процессы функционирования КВИО и средств СОПКА на стендовых полигонах находятся в стадии начальной разработки и развития [1–6, 11–20].

В статье предлагается совокупность имитационных моделей сегментов КВИО, компьютерных атак и элементов СОПКА для оценки реального уровня защищенности и устойчивости функционирования КВИО в условиях компьютерных атак.

Имитационные модели сегментов КВИО представляются технологическими циклами управления (ТЦУ) КВИО в виде взаимосвязанных процессов сбора, обработки, передачи и выдачи управляющей информации (рис. 1). Приведенная модель включает в свой состав типовой сценарий нарушения устойчивости функционирования КВИО. Этот сценарий показывает, что в условиях компьютерных атак параметры КВИО выходят за допустимые пределы, что приводит к нарушению устойчивости его функционирования.

Сущность нарушения устойчивости функционирования КВИО в условиях компьютерных атак заключается в том, что несвоевременно выполняется технологические циклы управления. Вводится искусственное замедление. На период времени действия компьютерных атак и восстановления КВИО срываются сроки обработки и передачи требуемых объемов информации или данные поступают в искаженном виде. Поэтому, для КВИО наиболее значимы ограничения на время и вероятность выполнения требуемого объема информационно-расчетных задач и выдачи управляющих воздействий с учетом специфики объекта.

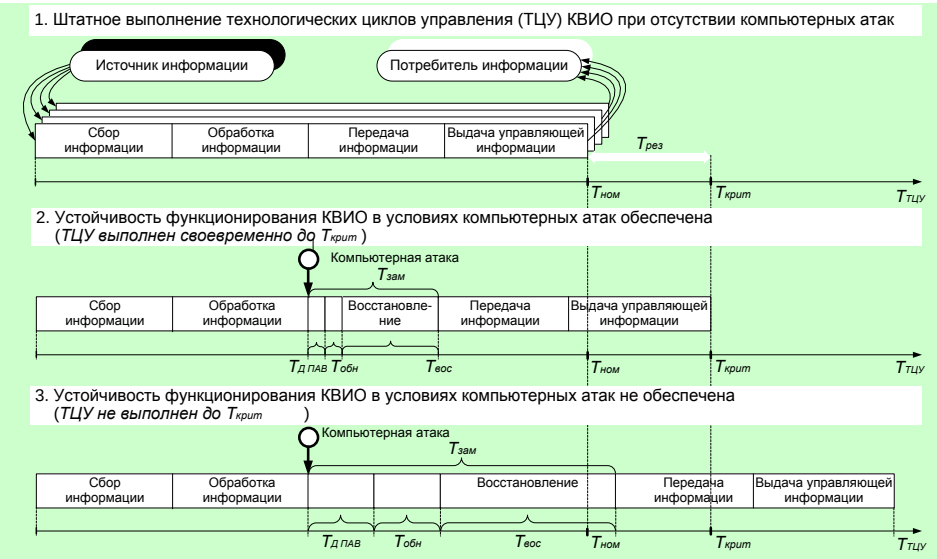

Рис. 1. Имитационная модель сегментов КВИО в виде технологического цикла управления в условиях компьютерных атак

Для исследования реального уровня защищенности и устойчивости функционирования имитационных моделей сегментов КВИО необходимо подготовить паспорта на сегмент КВИО и уязвимости программного обеспечения (ПО) объекта.

Паспорт на сегмент КВИО должен определять следующие основные исходные данные:

1. Категория важности объекта по назначению и предъявленным требованиям к решаемым задачам.

2. Степень конфиденциальности обрабатываемой информации (персональных данных, информации ограниченного доступа и других сведений).

3. Периодичность и тип проверок (тестирования) на защищенность и устойчивость функционирования.

4. Состав и характеристики технического обеспечения (характеристики компьютеров, серверов, цифрового коммуникационного оборудования и других IP-устройств).

5. Состав и характеристики общего и специального программного обеспечения (тип операционной системы, системы управления базой данными, электронной почты и других программ).

6. Параметры настройки вычислительной сети (каналообразующее оборудование проводных, беспроводных, спутниковых сетей; топология вычислительной сети; электронные параметры абонентов сети IP и MAC – адреса; доступные номера портов коммуникационного оборудования и другие параметры).

7. Состав и характеристики средств защиты информации (автоматизированных модулей доверенной загрузки (АМДЗ), межсетевых экранов (МЭ), элементов СОПКА, средств антивирусной защиты (САВЗ), виртуальных частных сетей (ВЧС), ложных сетевых информационных объектов (ЛСИО) и других средств защиты информации).

Паспорт уязвимостей программного обеспечения КВИО удобно сформировать в соответствии с ГОСТ Р 56545-2015 и ГОСТ Р 56546-2015 и определить семнадцатью основными параметрами уязвимостей. В табл. 1 представлен пример паспорта уязвимостей программного обеспечения для ОС Microsoft Windows 10.

Имитационные модели компьютерных атак на КВИО представляют собой программно-алгоритмическое обеспечение, которое воспроизводит возможный сценарий действий нарушителя по пассивному и активному сканированию уязвимостей КВИО, подготовке исходных данных и практической реализации компьютерных атак.

В моделях предлагается сымитировать четыре основных вида компьютерных атак нарушителя:

1. DDoS-атаки («отказ в обслуживании»), которые реализованы программами эксплойтами, направляемым по сети на выявленные (известные) уязвимые места и вызывающим нарушение безопасности информации и устойчивости функционирования КВИО.

2. Информационная нагрузка, заключающаяся в воздействии интенсивным потоком стандартных пакетов данных (со скоростью от 2 Мбит/с до 10 Гбит/с) на абонентов сети, приводящая к перегрузке сетевого трафика и «зависанию» сегментов КВИО.

3. Фаззинг, метод исследования уязвимостей, основанный на отправке нестандартных (искаженных) пакетов данных на электронные адреса сетевых устройств, позволяющих выявить доступные уязвимые места для компьютерных атак «нулевого дня».

4. Вредоносные программы, осуществляющие скрытое проникновение в КВИО программного кода минимального размера, самораспространение в КВИО, самомодификацию и выполнение удаленных команд по несанкционированному сбору информации или загрузке программ реализации компьютерных атак.

Таблица 1

Паспорт уязвимых мест программного обеспечения КВИО с использованием ГОСТ Р 56545-2015 и ГОСТ Р 56546-2015

№ п/п	Элементы описания уязвимости	Описание уязвимости
1	Наименование уязвимости	Уязвимость в Microsoft Windows
2	Идентификатор уязвимости	CVE-2015-2554
3	Краткое описание уязвимости	Уязвимости позволяют обойти ограничения безопасности, скомпрометировать систему и повысить привилегии
4	Класс уязвимости	Уязвимость кода
5	Наименование ПО и его версия	Microsoft Windows 10
6	Служба (порт), которая (который) используется для функционирования ПО	80
7	Язык программирования ПО	СИ++
8	Тип недостатка	Недостатки, связанные с аутентификацией
9	Место возникновения уязвимости	Уязвимость существует из-за некорректной обработки объектов в памяти
10	Идентификатор типа недостатка	Нет данных
11	Наименование ОС и тип аппаратной платформы	Microsoft Windows
12	Дата выявления уязвимости	14.10.2015
13	Автор выявленной уязвимости	Microsoft
14	Способ (правило) обнаружения уязвимости	Выполнение пошаговой инструкции
15	Критерии опасности уязвимости	В соответствии с CVSS-AV:N/AC:M/Au:N
16	Степень опасности уязвимости	Высокая
17	Возможные меры по устранению уязвимости	Установите исправление с сайта производителя

Исследования защищенности и устойчивости функционирования КВИО на стендовом полигоне позволяют провести испытания объекта в условиях пиковой нагрузки в форме комбинированных компьютерных атак, которые формируются из приведенных выше четырех типов.

Имитационные модели элементов СОПКА позволяют сформировать эталоны трафика нормального (штатного) функционирования, определить уязвимые места и классифицировать угрозы компьютерных атак по последствиям воздействия и с учетом специфики применения КВИО [7–10].

Модели обнаружения компьютерных атак основаны на комплексном применении разнородных программных и программно-аппаратных детекторов (сенсоров). Обнаружение известных компьютерных атак осуществляется методами сигнатурного анализа. Методами анализа аномалий и корреляционного анализа выявляются неизвестные компьютерные атаки, которые позволяют идентифицировать факты подготовки и реализации компьютерных атак. Модели ликвидации последствий компьютерных атак заключаются в совокупности экспертных оценок, аналитических расчетов и эвристическом анализе программного кода для расследования компьютерных инцидентов, выявления новых компьютерных атак, обновления паспортов КВИО и баз данных уязвимостей, классификаторов компьютерных атак.

По результатам испытаний КВИО в условиях компьютерных атак на стендовом полигоне формируются рекомендации и проводятся организационно-технические мероприятия по устранению уязвимостей в КВИО. Важнейшим и самостоятельным во-

просом перспективных исследований защищенности КВИО в условиях компьютерных атак является оценка отказоустойчивости и восстанавливаемости объектов для оперативной ликвидации последствий компьютерных атак [7, 19–20].

Параметры оценки средств имитации компьютерных атак и защиты от них, а также критерии оценки защищенности КВИО в условиях имитации компьютерных атак представлены соответственно в табл. 2 и 3.

Комплекс имитационных моделей КВИО, компьютерных атак и средств защиты информации, реализованных в виде аппаратно-программных комплексов целесообразно объединить в стендовый полигон для испытаний КВИО и компьютеризированных элементов промышленных производств в условиях компьютерных атак.

Структура стендового полигона оценки реального уровня защищенности и устойчивости функционирования КВИО в условиях компьютерных атак представлена на рис. 2.

Типовую структуру стендового полигона в области информационной безопасности предлагается сформировать по модульному принципу в виде совокупности базовых и специальных аппаратно-программных комплексов, взаимоувязанных по функциям и формату данных.

Первый модуль – система имитаторов компьютерных атак и сценариев действий нарушителя.

Второй модуль – сегменты КВИО, включающие в свой состав, как элементы информационно-телекоммуникационных систем, так и компьютеризированных промышленных производств.

Третий модуль – комплекс средств защиты информации.

Таблица 2

Параметры оценки средств имитации компьютерных атак и защиты от них

Средства имитации атак	Средства защиты от атак	Способы имитации атак	Способы защиты от атак
N_a – число средств реализации атак; ξ_a – число уязвимостей; $T^a_{ВУ}$ – время выявления уязвимостей; $T^a_{Д}$ – время доставки атак; $T^a_{пр}$ – время преодоления СрЗИ; $T^a_{размн}$ – время размножения; $T^a_{МД}$ – время модификации; $T^a_{возд}$ – время воздействия; $T^a_{НФ}$ – время нарушения КВИО; λ_a – интенсивность атак.	$K^a_{СрЗИ}$ – количество СрЗИ; Z_a – класс защищенности СрЗИ; $T^a_{ОБ}$ – время обнаружения; $T^a_{АН}$ – время анализа; $T^a_{ПР}$ – время противодействия; $T^a_{В}$ – время восстановления; $T^a_{ТЦУ}$ – время выполнения ТЦУ.	J – способы реализации атак; $J_{ОО}$ – одна атака – один элемент КВИО; $J_{ОМ}$ – один тип атак ко многим элементам КВИО; $J_{ММ}$ – массированные атаки на множество элементов КВИО; $J_{КС}$ – контейнер с атакой в программе саморазмножения; $J_{КМ}$ – контейнер с атакой в программе самомодификации; $W_{КВИО}$ – тип элемента КВИО; *элементы КВИО:* $W_{СВ}$ – сервер, $W_{ЦКО}$ – ЦКО, $W_{АРМ}$ – АРМ.	M – способы противодействия атакам; $\alpha_{СОПКА}$ – весовой коэффициент СОПКА; $\alpha_{МЭ}$ – весовой коэффициент МЭ; $\alpha_{АВП}$ – весовой коэффициент АВП; $\alpha_{ВЧС}$ – весовой коэффициент ВЧС; $\alpha_{ЛСИО}$ – весовой коэффициент ЛСИО.

Таблица 3

Критерии оценки защищенности КВИО в условиях имитации компьютерных атак

Критерии оценки атак	Критерии способов имитации атак	Критерии выбора оптимальных стратегий	Критерии выбора оптимальных стратегий при защите от атак	Условия невозможности успешных атак
$\max Y^{a}$ – максимальное число успешно реализованных атак; $\min \xi$ – минимум уязвимых мест КВИО; $\max X^{б}$ – максимальное количество обнаруженных атак; $K^{a}_{ИТВ} = \frac{Y^{a}_{УСП}}{Y_{общ}}$ – коэффициент реализуемости атак.	$P^{б}_{нарі} \to \max$ – вероятность нарушения максимального количества элементов КВИО; $P^{a}_{восj} \to \max$ – вероятность восстановления максимального количества элементов КВИО; $P^{a}_{рабк} \to \max$ – вероятность обеспечения максимального количества работоспособных элементов КВИО.	а) $W_1 = \min\limits_{n} \max\limits_{m} W_{ij}$ – минимальное количество атак (n) для нарушения КВИО при m СрЗИ; б) $W_2 = \max\limits_{n} \min\limits_{m} W_{ij}$ – максимальное количество для нарушения элементов КВИО; $W_1 = W_2$ – гарантированный результат.	а) $G_1 = \min\limits_{m} \max\limits_{n} G_{ij}$ – минимальное количество СрЗИ для противодействия атакам за период ТЦУ; б) $G_2 = \max\limits_{m} \min\limits_{n} G_{ij}$ – максимальное количество СрЗИ для противодействия атакам за период ТЦУ.	$T^{a}_{ТЦУ} = 0$ – ТЦУ в КВИО не выполняется; $\mu = 0$ – отсутствуют уязвимости КВИО; $P^{Б}_{дост} = 0$ – вероятность доступа к КВИО равна 0.

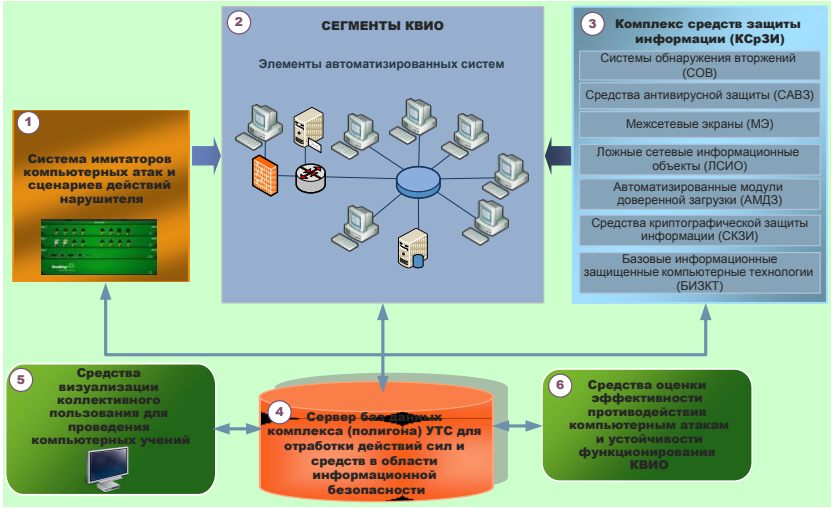

Рис. 2. Структура стендового полигона оценки реального уровня защищенности и устойчивости функционирования КВИО в условиях компьютерных атак

Четвертый модуль – сервер баз данных стендового полигона для отработки действий специалистов и средств в области информационной безопасности.

Пятый модуль – средства визуализации коллективного пользования для проведения испытаний КВИО и компьютерных учений по противодействию компьютерным атакам.

Шестой модуль – средства оценки эффективности противодействия компьютерным атакам и устойчивости функционирования КВИО.Проведение оценки защищенности и устойчивости функционирования КВИО включает четыре этапа:

1. Подключение к элементам исследуемого КВИО (анализ интенсивности трафика, предварительная настройка сетевых интерфейсов и параметров имитационных моделей компьютерных атак и средств защиты информации).

2. Анализ сети (определение доступных электронных адресов абонентов и топологии сети, определение используемых операционных систем, состояние портов, активных сетевых служб и сервисов).

3. Подготовка сценария и проведение испытаний КВИО (одновременная или раздельная имитация компьютерных атак и информационной нагрузки на сеть, сбор данных о количестве успешных и не успешных компьютерных атак).

4. Формирование отчета по результатам проведенных испытаний (проведение статистических расчетов, экспертная оценка результатов испытаний, выдача заключения об уровне защищенности и устойчивости функционирования).

Следует отметить, что точность и достоверность результатов испытаний (тестирования) на реальный уровень защищённости и устойчивости функционирования КВИО в условиях известных и неизвестных компьютерных атак будет зависеть от адекватности разработанных имитационных моделей нарушителя по обеспечению комплекса воздействий DDoS-атаками, информационной нагрузкой, методом фаззинга и скрытно проникающими в КВИО вредоносными программами.

Заключение. В статье на основе анализа современных угроз компьютерных атак обоснована совокупность необходимых имитационных моделей для испытаний КВИО в условиях компьютерных атак и структура стендового полигона оценки реального уровня защищенности и устойчивости функционирования КВИО в условиях компьютерных атак.

Научная новизна предложенных имитационных моделей испытаний КВИО в условиях компьютерных атак заключается в том, что в отличие от существующих моделей, в них предложено следующее:

- имитационное моделирование процессов функционирования КВИО в условиях атак технологическими циклами управления и временными задержками, искусственно вносимыми компьютерными атаками;
- количественные параметры оценки средств имитации компьютерных атак и защиты от них;
- минимаксные критерии оценки защищенности КВИО в условиях имитации компьютерных атак;
- унифицированные модули стендового полигона оценки реального уровня защищенности и устойчивости функционирования КВИО в условиях компьютерных атак.

Преимущество разработанных имитационных моделей и стендового полигона состоит в том, что они позволяют априорно провести исследование защищенности КВИО в условиях комбинированных воздействий DDoS-атаками, информационной нагрузкой, средствами фаззинга и вредоносными программами. Кроме того, рассмотренные предварительные испытания на стендовом полигоне позволяют обеспечить вероятность защиты информации КВИО в условиях комбинированных компьютерных атак в интервале 0,85–0,95 за счет своевременного устранения уязвимостей и настройки средств защиты информации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Левцов В., Демидов Н.* Анатомия таргетированной атаки // Информационная безопасность. – 2016. – № 2. – С. 36-39.
2. *Васильев В.И.* Интеллектуальные системы защиты информации: учеб. пособие. – 2-е изд., испр. и доп. – М.: Машиностроение, 2013. – 172 с.
3. ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
4. ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.
5. *Давыдов А.Е., Максимов Р.В., Савицкий О.К.* Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. – М.: ОАО «Воентелеком», 2015. – 520 с.
6. *Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В.* Информационная безопасность открытых систем: учебник для вузов. В 2-х т. Т. 2. Средства защиты в сетях. – М.: Горячая линия-Телеком, 2008. – 558 с.
7. *Климов С.М.* Методы и модели противодействия компьютерным атакам. – Люберцы. Изд-во: Каталит, 2008. – 316 с.
8. *Климов С.М., Астрахов А.В., Сычев М.П.* Технологические основы противодействия компьютерным атакам. Электронное учебное издание. – М.: МГТУ им. Н.Э. Баумана, 2013. – 71 с.
9. *Климов С.М., Астрахов А.В., Сычев М.П.* Методические основы противодействия компьютерным атакам. Электронное учебное издание. – М.: МГТУ им. Н.Э. Баумана, 2013. – 110 с.
10. *Климов С.М., Астрахов А.В., Сычев М.П.* Экспериментальная оценка противодействия компьютерным атакам. Электронное учебное издание. – М.: МГТУ им. Н.Э. Баумана, 2013. – 116 с.
11. *Лукацкий А.В*. Обнаружение атак. – СПб.: БХВ-Петербург, 2001. – 624 с.
12. *Лукацкий А.В.* Мир атак многообразен. – URL: http://www.infosec.ru//press/pub_luka.html.
13. *Мельников Д.А.* Организация и обеспечение безопасности информационно-технологических сетей и систем: учебник. – М.: ИД КДУ, 2015. – 598 с.
14. *Сердюк В.А.* Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. – М.: Изд. дом Гос. ун-та – Высшей школы экономики, 2011. – 572 с.
15. *Скудис Эд.* Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите: пер. с англ. – М.: ДМК Пресс, 2003. – 512 с.
16. Угрозы информационной безопасности в кризисах и конфликтах XXI века / под ред. А.В. Загорского, Н.П. Ромашкиной. - М.: ИМЭМО РАН, 2015. - 151 с.
17. *Устинов Г.Н.* Основы информационной безопасности систем и сетей передачи данных. учебное пособие. Серия «Безопасность». – М.: СИНТЕГ, 2000. – 248 с.
18. *Хогланд, Грег, Мак-Гроу, Гари*. Взлом программного обеспечения: анализ и использование кода: пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 400 с.
19. *Шубинский И.Б.* Функциональная надежность информационных систем. Методы анализа. – Ульяновск: Областная типография «Печатный двор», 2012. – 296 с.
20. *Язов Ю.К.* Основы методологии количественной оценки эффективности защиты информации в компьютерных системах. – Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006. – 274 с.

REFERENCES

1. *Levtsov V., Demidov N.* Anatomiya targetirovannoy ataki [Anatomy of a targeted attack], *Informatsionnaya bezopasnost'* [Information security], 2016, No. 2, pp. 36-39.
2. *Vasil'ev V.I.* Intellektual'nye sistemy zashchity informatsii: ucheb. posobie [Intellectual systems of information security: a training manual]. 2nd ed. Moscow: Mashinostroenie, 2013, 172 p.
3. GOST R 51583-2000. Zashchita informatsii. Poryadok sozdaniya avtomatizirovannykh sistem v zashchishchennom ispolnenii. Obshchie polozheniya [State Standard RF 51583-2000. The order of creation of the automated systems in the protected execution. General provisions].
4. GOST R 56546-2015. Zashchita informatsii. Uyazvimosti informatsionnykh sistem. Klassifikatsiya uyazvimostey informatsionnykh system [State Standard RF 56546-2015. Vulnerability of information systems. Classification of vulnerabilities of information systems].
5. *Davydov A.E., Maksimov R.V., Savitskiy O.K.* Zashchita i bezopasnost' vedomstvennykh integrirovannykh infokommunikatsionnykh system [The protection and security of departmental integrated information and communication systems]. Moscow: OAO «Voentelekom», 2015, 520 p.

6. *Zapechnikov S.V., Miloslavskaya N.G., Tolstoy A.I., Ushakov D.V.* Informatsionnaya bezopasnost' otkrytykh sistem: uchebnik dlya vuzov [Information security of open systems: textbook for universities]. In 2 vol. Vol. 2. Sredstva zashchity v setyakh [Protection in networks]. Moscow: Goryachaya liniya-Telekom, 2008, 558 p.
7. *Klimov S.M.* Metody i modeli protivodeystviya komp'yuternym atakam [Methods and models of counteracting computer attacks]. Lyubertsy. Izd-vo: Katalit, 2008, 316 p.
8. *Klimov S.M., Astrakhov A.V., Sychev M.P.* Tekhnologicheskie osnovy protivodeystviya komp'yuternym atakam. Elektronnoe uchebnoe izdanie [Technological bases of counteraction against computer attacks. Electronic educational edition]. Moscow: MGTU im. N.E. Baumana, 2013, 71 p.
9. *Klimov S.M., Astrakhov A.V., Sychev M.P.* Metodicheskie osnovy protivodeystviya kom-p'yuternym atakam. Elektronnoe uchebnoe izdanie [Methodological bases of counteraction against computer attacks. Electronic educational edition]. Moscow: MGTU im. N.E. Baumana, 2013, 110 p.
10. *Klimov S.M., Astrakhov A.V., Sychev M.P.* Eksperimental'naya otsenka protivodeystviya komp'yuternym atakam. Elektronnoe uchebnoe izdanie [Experimental evaluation of counteraction to computer attacks. Electronic educational edition]. Moscow: MGTU im. N.E. Baumana, 2013, 116 p.
11. *Lukatskiy A.V.* Obnaruzhenie atak [The attack detection]. St. Petersburg: BKhV-Peterburg, 2001, 624 p.
12. *Lukatskiy A.V.* Mir atak mnogoobrazen [The world of the attacks are diverse]. Available at: http://www.infosec.ru//press/pub_luka.html.
13. *Mel'nikov D.A.* Organizatsiya i obespechenie bezopasnosti informatsionno-tekhnologicheskikh setey i sistem: uchebnik [Organization and security of information technology networks and systems: textbook]. Moscow: ID KDU, 2015, 598 p.
14. *Serdyuk V.A.* Organizatsiya i tekhnologii zashchity informatsii. Obnaruzhenie i predotvrashchenie informatsionnykh atak v avtomatizirovannykh sistemakh predpriyatiy: uchebnoe posobie [Organization and technology of information protection. The detection and prevention of informational attacks of automated systems of enterprises: textbook]. Moscow: Izd. dom Gos. un-ta – Vysshey shkoly ekonomiki, 2011, 572 p.
15. *Skudis Ed.* Protivostoyanie khakeram. Poshagovoe rukovodstvo po komp'yuternym atakam i effektivnoy zashchite [Opposition to hackers. Step-by-step guide to computer attacks and effective protection]: translation from English. Moscow: DMK Press, 2003, 512 p.
16. Ugrozy informatsionnoy bezopasnosti v krizisakh i konfliktakh XXI veka [Threats to information security in crises and conflicts of the XXI century], ed. by A.V. Zagorskogo, N.P. Romashkinoy. Moscow: IMEMO RAN, 2015, 151 p.
17. *Ustinov G.N.* Osnovy informatsionnoy bezopasnosti sistem i setey peredachi dannykh. uchebnoe posobie. Seriya «Bezopasnost'» [Foundations of information security systems and data networks. textbook. A Series Of "Security"]. Moscow: SINTEG, 2000, 248 p.
18. *Khogland, Greg, Mak-Grou, Gari.* Vzlom programmnogo obespecheniya: analiz i ispol'zovanie koda [Hacking software: analysis and use code]: translation from English. Moscow: Izdatel'skiy dom «Vil'yams», 2005, 400 p.
19. *Shubinskiy I.B.* Funktsional'naya nadezhnost' informatsionnykh sistem. Metody analiza [Functional reliability of information systems. Methods of analysis]. Ul'yanovsk: Oblastnaya tipografiya «Pechatnyy dvor», 2012, 296 p.
20. *Yazov Yu.K.* Osnovy metodologii kolichestvennoy otsenki effektivnosti zashchity informatsii v komp'yuternykh sistemakh [The basics of methodology of quantitative assessment of the effectiveness of the protection of information in computer systems]. Rostov-on-Don: Izd-vo SKNTs VSh, 2006, 274 p.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Климов Сергей Михайлович – МГТУ им. Н.Э. Баумана; e-mail: klimov.serg2012@yandex.ru; 141090 г. Королев, мкр. Юбилейный Московской обл., ул. Б. Комитетская, 12, кв. 105; тел.: 89859281355; д.т.н.; профессор.

Klimov Sergey Mikhailovich – Bauman Moscow State Technical University; e-mail: klimov.serg2012@yandex.ru; 12, B. Komitetskay street, apt. 105, Korolev, community Ubileynuy, Moscow distr., 141090, Russia; phone: +79859281355; dr. of eng. sc.; professor.