ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2023-50-3-57-65 Оригинальная статья /Original article

Рекомендации по применению методики оценки защищённости автоматизированной системы управления критической информационной инфраструктуры от DDoS-атак на основе имитационного моделирования методом Монте-Карло

В.А. Воеводин, В.С. Черняев, И.В. Виноградов
Национальный исследовательский университет
«Московский институт электронной техники»,
124498, г. Москва, г. Зеленоград, пл. Шокина, 1, Россия

Резюме. **Цель**. Целью исследования является разработка методики оценки защищённости автоматизированной системы управления критической информационной инфраструктуры от DDoS-атак. Данная методика позволяет лицу, принимающему решение (ЛПР), получить оценку риска подверженности вычислительной сети (ВС) DDoS-атакам и принять необходимые меры для снижения уровня риска реализации угрозы воздействия DDoS-атак. **Метод**. Для достижения заявленной цели исследования использовалось имитационное моделирование на основе метода Монте-Карло, реализованное в рамках специализированного программного средства, а также метод расчёта интегрального риска. **Результат.** Была предложена методика оценки защищённости автоматизированной системы управления критической информационной инфраструктуры от DDoS-атак с учётом значимости отдельных узлов её ВС. **Вывод.** Разработанная методика полезна при проведении аудита информационной безопасности (АИБ) для оценки интегрального риска реализации угрозы воздействия DDoS-атаки на ВС. Методика призвана помочь организации в достижении глобальных целей информационной безопасности (ИБ), а также для обоснования размера выплачиваемой страховой премии при страховании киберрисков.

Ключевые слова: имитационное моделирование, метод Монте-Карло, DDoS-атака, аудит информационной безопасности, оценка риска информационной безопасности.

Для цитирования: В.А. Воеводин, В.С. Черняев, И.В. Виноградов. Рекомендации по применению методики оценки защищённости автоматизированной системы управления критической информационной инфраструктуры от DDoS-атак на основе имитационного моделирования методом Монте-Карло. Вестник Дагестанского государственного технического университета. Технические науки. 2023; 50(3):57-65. DOI:10.21822/2073-6185-2023-50-3-57-65

Recommendations for using a methodology for assessing the security of an automated control system for critical information infrastructure from DDoS attacks based on Monte Carlo simulation

V.A. Voevodin, V.S. Chernyaev, I.V. Vinogradov
National Research University of Electronic Technology,
1 Shokin Square, Moscow, Zelenograd 124498, Russia

Abstract. Objective. The objective of the research is to develop a methodology for the security of an automated control system of critical information infrastructure from DDoS attacks. The methodology allows the decision-maker to obtain an assessment of the risk of exposure of the computer network (CN) to DDoS attacks and take necessary actions to reduce the risk of this threat. **Method.** To achieve the stated objective of the research, simulation modeling based on the Monte Carlo method was used, implemented within the framework of a specialized software environment, as well as a method for calculating integral risk. **Result.** A methodology was proposed for assessing the security of an automated control system for critical information infrastructure

from DDoS attacks, taking into account the importance of individual nodes of its CN. **Conclusion.** Thus, the developed methodology is useful when conducting an information security audit to assess the integral risk of impact implementation of a DDoS attack on a CN and is designed to help an organization achieve global information security goals, as well as to justify the amount of the insurance premium paid when insuring cyber risks.

Keywords: simulation modeling, Monte Carlo method, DDoS attack, information security audit, information security risk assessment.

For citation: V.A. Voevodin, V.S. Chernyaev, I.V. Vinogradov. Recommendations for using a methodology for assessing the security of an automated control system for critical information infrastructure from DDoS attacks based on Monte Carlo simulation. Herald of Daghestan State Technical University. Technical Science. 2023; 50 (3): 57-65. DOI: 10.21822 /2073-6185-2023-50-3-57-65

Введение. В статье, размещенной ранее в данном журнале, была предложена методика оценки вероятности отказа элементов информационной инфраструктуры ВС, функционирующей в условиях воздействия DDoS-атак. В настоящей статье предложена методика оценки интегрального риска реализации угрозы воздействия DDoS-атак на ВС в целом, основой которой служит применение методов, представленных в предыдущей публикации. На сегодняшний день проблема защиты сетевой инфраструктуры от DDoS-атак является актуальной. Организациям промышленного сектора требуется защита от подобного вида атак, так как в случае её успешной реализации нанесённый ущерб может иметь не только материальный характер, но и последствия для здоровья и жизни людей.

Согласно данным открытых источников, прошедший 2022 год был насыщенным по количеству DDoS-атак на финансовые организации. В марте 2022 года Министерство цифрового развития, связи и массовых коммуникаций РФ предложило помощь российским банкам в борьбе с DDoS-атаками, которые происходят из-за рубежа. Банки имеют возможность направить Центральному банку РФ список информационных систем (ИС), подверженных угрозе воздействия DDoS-атак, чтобы получить поддержку. Минцифры России организует фильтрацию зарубежного трафика и координирует меры противодействия угрозам, чтобы предотвратить нарушения доступности ресурсов банков.

Эксперты считают такую инициативу целесообразной, поскольку она позволит снизить мощность зарубежных DDoS-атак. Отмечается, что методика фильтрации трафика по геолокации является неточной и неэффективной, так как атаки имеют распределенный характер и могут происходить из различных стран, включая Россию. К середине марта 2022 года количество DDoS-атак на банки выросло в четыре раза по сравнению с февралем 2022 года, составив около 400 атак, по сведениям специалистов по кибербезопасности. Кроме этого, ряд крупных банков сообщил о массированных кибератаках, которые были успешно отражены [1].

В терминах стандарта ИСО/МЭК 27001 успешная DDoS-атака может повлиять на достижение следующих глобальных целей ИБ организации [2, 3]:

1. Обеспечение надлежащей и безопасной эксплуатации средств обработки информации.
2. Информационная безопасность должна обеспечиваться на всём жизненном цикле ИС.
3. Обеспечение доступности к средствам обработки информации.

Таким образом, оценка интегрального риска реализации угрозы воздействия DDoS-атаки на ВС может быть актуальна при проведении аудита на соответствие международным стандартам в области ИБ, что обуславливает необходимость разработки методики оценки интегрального риска подверженности ВС DDoS-атакам.

В общем случае можно выделить следующие этапы проведения аудита информационной безопасности:

1. **Подготовительный этап.** На подготовительном этапе происходит согласование плана аудита и определяется объём аудиторских процедур. Согласование объёма аудиторских процедур происходит совместно с руководителями соответствующих

бизнес или ИТ-подразделений. На данном этапе также происходит согласование сроков, определяется информация, которую компания считает критичной и не желательной для предоставления в рамках аудита. В этом случае с представителями аудиторской группы согласовываются альтернативные способы проведения проверки без использования данной информации.

2. **Основной этап.** Основной этап включает непосредственное проведение аудиторских процедур. На данном этапе проводятся очные или дистанционные интервью, запрашиваются и анализируются необходимые отчёты по ИС, формируются выборки. В зависимости от целей аудита проверке подвергаются процедуры внесения изменений в продуктивную среду организации, управления доступом, разграничения полномочий, настройки резервного копирования и другие процедуры.

Заключительный этап. На заключительном этапе формируется аудиторское заключение, а также выдаётся ряд рекомендаций для устранения уязвимостей и недостатков в обеспечении ИБ. Программа АИБ представляет собой стратегический план, который определяет проведение одного или нескольких АИБ и других проверок в определенный период времени с целью достижения определенных результатов в области ИБ [4].

Для результативного проведения аудита в рамках установленных сроков, программа аудита должна содержать следующую информацию [5]:

1. Цели аудита.
2. Риски, возможности, связанные с программой аудита, и план действий по их управлению.
3. Объем каждого аудита в рамках программы аудита, включая глубину охвата и границы места проведения.
4. График проведения аудитов, включая число, продолжительность и частоту.
5. Типы аудитов, такие как внутренний или внешний.
6. Критерии аудита.
7. Методы аудита, которые будут применяться.
8. Критерии для выбора членов аудиторской группы.
9. Соответствующая документированная информация.

Модель аудита включает в себя следующие компоненты:

1. Объект аудита – предмет, подлежащий проверке в рамках аудита.
2. Цели аудита – задачи и цели, которые необходимо достичь в процессе аудита.
3. Предъявляемые требования – стандарты, нормы и критерии, которым должен соответствовать объект аудита.
4. Используемые практические и теоретические подходы – методы, подходы и инструменты, применяемые в процессе аудита.
5. Масштаб и глубина – уровень детализации и степень проникновения при проведении аудита.
6. Исполнители – лица или группы, ответственные за выполнение аудита.
7. Порядок проведения аудита – последовательность и этапы, которые исследуются во время проведения аудиторской проверки.

Согласно стандарту ГОСТ Р ИСО 19011–2021 аудит является систематическим, независимым и документированным процессом, который направлен на установление объективных доказательств и их последующую оценку с целью определения степени соответствия критериям аудита. Аудит ИБ можно рассматривать как исследование, которое позволяет оценить текущее состояние защиты информации и спланировать дальнейшие действия по улучшению уровня безопасности, охватывая все аспекты ИБ [6].

Для проведения аудита необходимо следовать формальной процедуре проверки объекта аудита, которая основывается на заранее сформированных формальных описаниях объекта и процесса аудита, а также учитывает современные угрозы. Схема процесса аудита представлена на рис. 1.

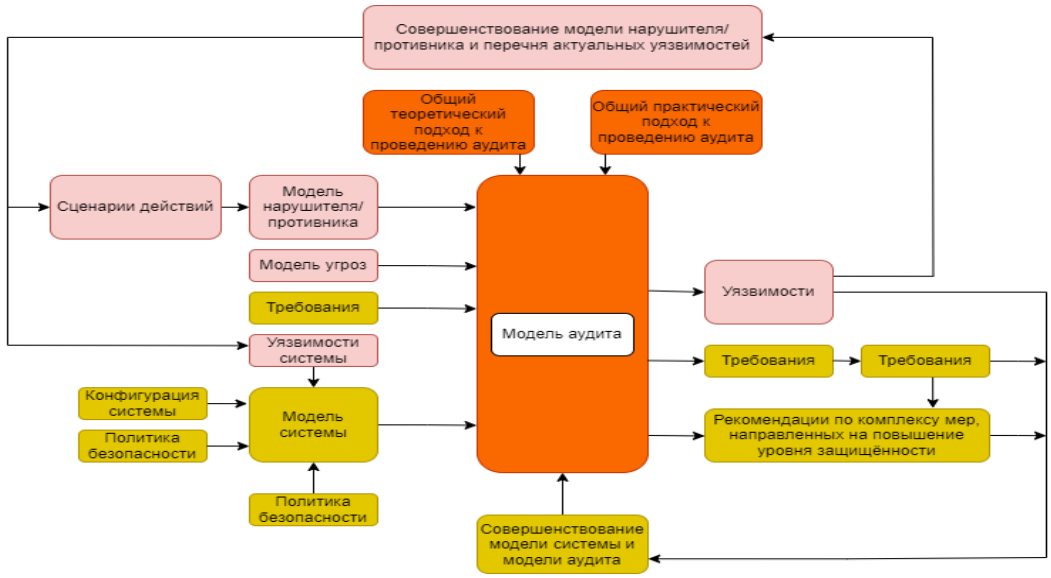

Рис.1. Схема процесса аудита
Fig.1. Audit process diagram

В общем случае для формализации процесса АИБ необходимо определить следующие аспекты: источники угроз, защищаемые элементы системы, связи между ними и структуру с функционированием подсистемы защиты.

Можно выделить четыре подхода к проведению АИБ [7]:

1. Риск-ориентированный аудит.
2. Аудит, основанный на директивном подходе.
3. Комбинированный аудит, сочетающий риск-ориентированный подход и директивный аудит.
4. Экспериментальный аудит.

При риск-ориентированном подходе проводится анализ рисков, свойственных проверяемой системе. Цель подобного подхода – обнаружение и снижение рисков путём внедрения контрольных процедур. Достоинство такого подхода заключается в возможности учёта особенностей проверяемой системы. Недостатком может стать субъективность в оценке, когда какой-то риск или аспект ИБ не был учтён [8].

Директивный подход к АИБ основан на проверке соответствия требованиям различных Регуляторов, нормативных правовых актов, международных и отраслевых стандартов. От организации требуется формальное соответствие требованиям, без учёта конкретной специфики. В случае аудита государственной организации также проверяется соответствие национальным нормативным актам. Плюсом данного подхода является достаточная прозрачность при проведении аудита, когда набор формальных требований однозначно определён. Минус директивного подхода заключается в том, что на итоговую оценку ИБ системы может оказать влияние критерий, который, в действительности, не является важным. При комбинированном аудите объединяются лучшие подходы двух предыдущих видов аудита: за основу берётся набор требований, представленный в стандарте, либо в нормативном правовом документе, но также учитываются особенности исследуемой системы. Подобный подход позволяет, с одной стороны, использовать лучшие практики, описанные в стандартах, а с другой – учесть особенности конкретной системы.

Экспериментальный аудит подразумевает проведение некоторых испытаний системы или ее прототипа, что позволяет оценить текущее реальное состояние различных аспектов ИБ системы. Этот подход может включать тестирование на проникновение, моделирование атак злоумышленника и активный анализ системы с позиции потенциального атакующего. Достоинством экспериментального аудита является наглядность получаемых результатов, однако существенным недостатком будет возможное нарушение операционной деятельности организации, либо невозможность применения данного вида аудита для некоторых критичных ИС, например, АСУ ТП.

Постановка задачи. Рассмотрим произвольную ВС, которая состоит из соединенных друг с другом устройств (серверов, маршрутизаторов, коммутаторов и т.д.) с уникальными IP-адресами [9, 10]. Каждое устройство будет называться узлом ВС, а доступ к ним будет осуществляться только авторизованными администраторами с целью их настройки. Каждому узлу присваивается номер в нумерации ВС: $i = 1, 2, \dots, N$, где N – общее число узлов. Для узлов ВС следует ввести вектор вероятностей поражения узлов ВС:

$$P = \{p_1, p_2, \dots, p_N\}.$$

Для оценки риска реализации угрозы воздействия DDoS-атак на ВС необходимо учитывать, что в сети присутствуют как критичные, так и менее критичные устройства [11]. Например, выход из строя коммутатора уровня доступа в одном подразделении не повлияет на работу всей сети в целом, но в случае сетевой атаки это может быть не так. Целесообразность учета весового коэффициента в рамках АИБ была показана в работах [12,13].

Методы исследования. В общем случае сетевая инфраструктура может включать следующие компоненты:

1. Сервер базы данных, обеспечивающий обслуживание и управление базой данных. Особый интерес для аудитора представляют продуктивные сервера, на которых обрабатывается информация, непосредственно влияющая на операционную деятельность организации. Информация, хранящаяся на таких серверах способна оказать влияние на финансовую отчётность.
2. Сервер приложений, предназначенный для обеспечения работы приложений, использующихся на предприятии сотрудниками, относящимся к бизнес-подразделениям. Такими приложениями выступают различные бухгалтерские программы и комплексы для ведения учёта в организации, например, продукты компаний 1С и SAP.
3. Транспортный сервер, обеспечивающий перенаправление информационных потоков.
4. Proxy-сервер, обеспечивающий подключение сотрудников к защищённому сетевому периметру организации.
5. Веб-сервер, предназначенный для получения доступа к внутренним информационным ресурсам организации.
6. Сервер обработки данных.
7. Маршрутизатор, обеспечивающий объединение внутренней сети организации с внешней.
8. Администраторский АРМ, предназначенный для управления системой.
9. АРМ операторов, которые используются для взаимодействия пользователей с системой.

Для корректной оценки риска подверженности ВС DDoS-атакам предлагается оценить критичность каждого узла и отранжировать по важности для функционирования ВС. Для этого предлагается ввести вектор критической значимости узлов:

$$w = \{w_1, w_2, \dots, w_N\}, \quad (1)$$

где w_i — вес (значимость) i-го узла для всей ВС в целом. Весовые коэффициенты определяются экспертом (аудитором) из анализа структурной схемы ВС при соблюдении нормирующего условия, то есть:

$$\sum_{i=1}^{N} w_i = 1. \quad (2)$$

Интегральный уровень риска K реализации угрозы воздействия DDoS-атаки на ВС в таком случае определяется линейной комбинацией следующего вида:

$$K = w_1 p_1 + w_2 p_2 + \cdots + w_N p_N = \sum_{i=1}^{N} w_i p_i. \quad (3)$$

Таким образом, общую методику определения интегрального уровня риска ИБ можно описать следующим алгоритмом:

1. Анализ структурной схемы ВС и определение вектора критичности узлов ВС: $w = \{w_1, w_2, \dots, w_N\}$.

В общем случае предлагается трёхуровневая оценка значимости. Основанием для присвоения оценки могут служить параметры, важные для той или иной сети, например, количество пользователей, на которых скажется выход из строя того или иного узла, время остановки деятельности организации, финансовые потери, издержки, налагаемые штрафными санкциями Регулятора и т.д. Следует отметить возможность исключения из рассмотрения отдельных узлов путём присвоения им нулевого приоритета.

2. Определение вектора вероятностей отказа узлов ВС такого, что: $i_1, i_2, i_3, \dots, i_N;\ U_i = \{p_1, p_2, \dots, p_N\}$.
3. Определение интегрального уровня риска ИБ всей ВС с учётом уровня значимости отдельного узла, определяемой при условии (2).
4. Присвоение качественной оценки риска на основании полученной численной интегральной оценки риска.

В общем случае предлагается использование пятиуровневой шкалы риска в соответствии с табл. 1.

Таблица 1. Качественная шкала риска
Table 1. Qualitative risk scale

Значение интегрального уровня риска K The value of the integral risk level K	**Оценка/ Grade**
0 - 0,2	1 «Незначительный риск»/ Little risk
0,2 - 0,4	2 «Небольшой риск»/ Slight Risk
0,4 - 0,6	3 «Средний риск»/ Medium risk
0,6 - 0,8	4 «Крупный риск»/ Large risk
0,8 - 1,0	5 «Катастрофический риск»/ Catastrophic risk

5. Предложение ЛПР мер, снижающих интегральный уровень риска реализации угрозы воздействия DDoS-атаки. Принятие ЛПР текущего уровня риска либо принятие ЛПР мер по его снижению путём внедрения предложенных рекомендаций.
6. Проведение повторной оценки интегрального риска ВС после внедрения мер по снижению уровня риска при необходимости.

Таким образом, для реализации приведенного выше алгоритма на втором шаге необходимо определение вероятностей выхода из строя узлов сети p_i.

Для решения данной задачи предлагается применение разработанного программного средства имитационного моделирования по методу Монте-Карло [14, 15].

Обсуждение результатов. Пусть после исследования топологии сети значимость узла N_1 оценена в 0,4; N_2 – в 0,6; остальные узлы ВС признаны незначительными, и узел N_1 имеет меньшие вычислительные мощности, чем узел N_2.

Последнее утверждение в терминах теории систем массового обслуживания описывается меньшим количеством каналов обслуживания. После проведения испытаний были получены соответствующие вероятности отказа для названных компонент ВС (рис. 2-3).

Интегральный уровень риска реализации угрозы воздействия DDoS-атаки для рассмотренного примера по формуле (3):

$$K = \sum_{i=1}^{N} w_i p_i = w_1 p_1 + w_2 p_2 = 0{,}50 \cdot 0{,}40 + 0{,}60 \cdot 0{,}47 = 0{,}482. \quad (4)$$

Таким образом, полученный интегральный уровень риска K исследуемой ВС равен 0,482, что соответствует оценке «Средний риск» согласно шкале (табл.1).

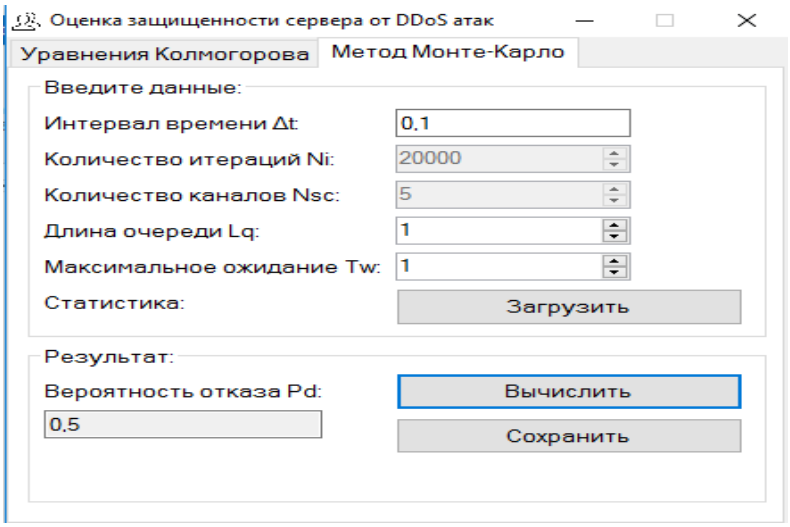

Рис.2. Вероятность отказа узла N_1
Fig.2. Node N_1 failure probability

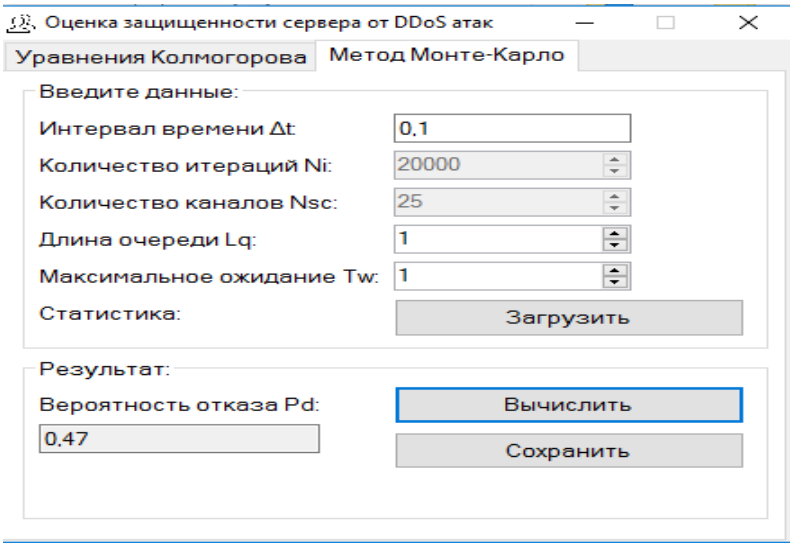

Рис.3. Вероятность отказа узла N_2
Fig.3. Node N_2 failure probability

В качестве рекомендаций по снижению риска реализации угрозы воздействия DDoS-атак предлагаются следующие меры, разработанные на основе рекомендаций компании АО «Лаборатория Касперского» [16]:

1. Замена модели сервера на более производительную модель, что позволит сохранить работоспособность при большом количестве вредоносных запросов.
2. Резервирование сервера, что позволит снизить критичность узла для ВС.
3. Создание защиты периметра от несанкционированного доступа посредством внедрения средств межсетевого экранирования, что позволит отделять поток вредоносных запросов.
4. Принятия ряда организационных мер, включающих усовершенствование политики ИБ и повышение квалификации персонала. Данный шаг повысит общую подготовленность персонала к отражению DDoS-атак, а также снизит возможность использования потенциальных уязвимостей сети для проведения DDoS-атаки.
5. Размещение средств анализа трафика. Подобная мера позволит своевременно детектировать подозрительную активность в сетевом контуре.

Вывод. Представлена методика оценки защищенности автоматизированной системы управления критической информационной инфраструктуры от DDoS-атак. Для оценки вероятности отказа узла ВС предлагается использовать специализированное программное средство имитационного моделирования DDoS-атак по методу Монте-Карло. Кроме того, в рамках методики вводится весовой коэффициент критичности узлов ВС для более точной оценки защищенности.

Разработанная методика позволяет оценить общий риск, связанный с возможной реализацией угрозы воздействия DDoS-атаки на ВС, и принять соответствующие организационные и технические меры для повышения уровня ИБ. Предложенная методика может быть использована при проведении АИБ в организации для обоснования размера страховой премии в рамках страхования киберрисков.

Библиографический список:

1. DDoS-атаки на банки в России. [Электронный ресурс]: https://www.tadviser.ru/index.php/Статья:DDoS-атаки_на_банки_в_России
2. ГОСТ Р ИСО/МЭК 27001— 2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2021 г. № 1653-ст. Москва Российский институт стандартизации 2021, - 24 с.
3. Implementing capacity management according to ISO 27001:2013 control A.12.1.3 [Электронный ресурс]: https://advisera.com/27001academy/blog/2016/02/22/implementing-capacity-management-according-to-iso-270012013-control-a-12-1-3/
4. Стандарт Банка России СТО БР ИББС-1.1-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности». Введен в действие распоряжением ЦБР от 28 апреля 2007 г. N Р-345.
5. ГОСТ Р ИСО 19011–2021 Руководящие указания по проведению аудита систем менеджмента. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 21 апреля 2021 г. N261-ст. М.: Стандартинформ, 2021. – 42 с.
6. Информационная безопасность автоматизированных систем / А.В. Солодянников - СПб. : Изд-во СПбГЭУ, 2020 - 108 с.
7. Макаренко С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. № 1. С. 1–29. Электронный ресурс: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf
8. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. N 632-ст. М.: Стандартинформ, 2012, - 91 с.
9. Вычислительные системы, сети и телекоммуникации: учебник. В 2 ч. Ч. 2. Сети и телекоммуникации / В. П. Галас ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир: Изд-во ВлГУ, 2017. − 284 с.
10. Вычислительные системы, сети и телекоммуникации: учебник для студ. учреждений высш. проф. образования / А. И. Гусева, В.С. Киреев – М.: Издательский центр «Академия», 2014 – М. : Издательский центр «Академия», 2014. – 288с. – (Сер. Бакалавриат).
11. Губарева О. Ю. Разработка методики оценки рисков информационной безопасности корпоративных телекоммуникационных сетей специальность 05.12.13 «Сети, системы и устройства телекоммуникаций» : автореферат диссертации на соискание учёной степени кандидата технических наук. Федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет телекоммуникаций и информатики» – Самара, 2018. – 176 с.
12. Воеводин В.А., Буренок Д.С., Черняев В.С. 2021, Программа для оценки защищенности сервера от DDoS-атак свидетельство официальной регистрации компьютерной программы номер 2021615403.
13. Воеводин В.А., Черняев В.С., Буренок Д.С., Виноградов И.В. Методика оценки защищённости автоматизированной системы управления критической информационной инфраструктуры от DDoS-атак на основе имитационного моделирования методом Монте-Карло. Вестник Дагестанского государственного технического университета. Технические науки. 2023;50(1):62-74.
14. Воеводин В. А., Маркин П. В., Маркина М. С., Буренок Д. С. Методика разработки программы аудита информационной безопасности с учетом весовых коэффициентов значимости свидетельств аудита на основе метода анализа иерархий // Системы управления, связи и безопасности. 2021. № 2. С. 96–129. DOI: 10.24412/2410-9916-2021-2-96-129.
15. Воеводин В. А., Карманьян А. И., Суханов Е. Э., Штанг К. С. О методике оценки значимости аудиторских свидетельств информационной безопасности // Интеллектуальные системы в информационном противоборстве: сборник научных трудов Российской научной конференции. 2019. С. 40-44.
16. Кибербезопасность АСУ ТП: вести с передовой / [Электронный ресурс]. Режим доступа: https://www.kaspersky.ru/blog/ics-report-2017/17812/

References:

1. DDoS attacks on banks in Russia. Available at: https://www.tadviser.ru/index.php/Статья:DDoS-атаки_на_банки_в_России (In Russ).

2. GOST R ISO/IEC 27001—2021 Information technology. Methods and means of ensuring safety. Information security management systems. Requirements. Approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated November 30, 2021 No. 1653-st. Moscow Russian Institute of Standardization 2021; 24. (In Russ).
3. Implementing capacity management according to ISO 27001:2013 control A.12.1.3 [Electronic resource]: https://advisera.com/27001academy/blog/2016/02/22/implementing-capacity-management-according-to- iso-270012013-control-a-12-1-3/(In Russ).
4. Standard of the Bank of Russia STO BR IBBS-1.1-2007 "Ensuring information security of organizations of the banking system of the Russian Federation. Information security audit." Put into effect by order of the Central Bank of Russia dated April 28, 2007;345. (In Russ).
5. GOST R ISO 19011–2021 Guidelines for conducting audits of management systems. Approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated April 21, 2021 N261-Art. M.: Standartinform, 2021; 42. (In Russ).
6. Information security of automated systems / A.V. Solodyannikov - St. Petersburg. : Publishing house of St. Petersburg State Economic University, 2020;108. (In Russ).
7. Makarenko S.I. Information security audit: main stages, conceptual foundations, classification of activities. *Management, communication and security systems*. 2018;1:1–29. Electronic resource: http://sccs.intelgr.com/archive/2018-01/01-Makarenko.pdf(In Russ).
8. GOST R ISO/IEC 27005-2010 Information technology. Methods and means of ensuring safety. Information security risk management. Approved and put into effect by Order of the Federal Agency for Technical Regulation and Metrology dated November 30, 2010 N 632-st. M.: Standartinform, 2012; 91.
9. Computing systems, networks and telecommunications: textbook. In 2 hours. Part 2. Networks and telecommunications. V. P. Galas; Vladim. state University named after A. G. and N. G. Stoletov. Vladimir: VlSU Publishing House, 2017; 284. (In Russ).
10. Computing systems, networks and telecommunications: a textbook for students. institutions of higher education prof. education. A.I. Guseva, V.S. Kireev. M.: Publishing center "Academy", 2014 - M.: Publishing center "Academy", 2014; 288 (Ser. Bachelor's degree). (In Russ).
11. Gubareva O. Yu. Development of a methodology for assessing the risks of information security of corporate telecommunication networks, specialty 05.12.13 "Networks, systems and devices of telecommunications": abstract of the dissertation for the degree of candidate of technical sciences. Federal State Budgetary Educational Institution of Higher Education "Volga Region State University of Telecommunications and Informatics". Samara, 2018; 176. (In Russ).
12. Voevodin V.A., Burenok D.S., Chernyaev V.S. 2021, Program for assessing server security against DDoS attacks, certificate of official registration of the computer program number 2021615403. (In Russ).
13. Voevodin V.A., Chernyaev V.S., Burenok D.S., Vinogradov I.V. Methodology for assessing the security of an automated control system for critical information infrastructure from DDoS attacks based on Monte Carlo simulation. *Herald of Daghestan State Technical University. Technical Science*. 2023; 50(1):62-74. DOI: 10.21822/2073-6185-2023-50-1-62-74 (In Russ).
14. Voevodin V. A., Markin P. V., Markina M. S., Burenok D. S. Methodology for developing an information security audit program taking into account the weighting coefficients of the significance of audit evidence based on the hierarchy analysis method. *Management Systems, Communications and security*. 2021; 2. 96–129. DOI: 10.24412/2410-9916-2021-2-96-129. (In Russ).
15. Voevodin V. A., Karmanyan A. I., Sukhanov E. E., Shtang K. S. On the methodology for assessing the significance of audit certificates of information security. *Intelligent systems in information warfare: collection of scientific papers of the Russian scientific conference.* 2019; 40-44. (In Russ).
16. Cybersecurity of automated process control systems: news from the front lines / [Electronic resource]. Access mode: https://www.kaspersky.ru/blog/ics-report-2017/17812/(In Russ).

Сведения об авторах:

Воеводин Владислав Александрович, кандидат технических наук, доцент, доцент кафедры «Информационная безопасность»; vva541@mail.ru

Черняев Валентин Сергеевич, магистрант; sergeich1997@yandex.ru

Виноградов Иван Вадимович, студент; ivanvinogradov1111@gmail.com

Information about authors:

Vladislav A. Voevodin, Cand. Sci.(Eng.), Assoc. Prof., Department of Information Security; vva541@mail.ru

Valentin S. Chernyaev, Master's student; sergeich1997@yandex.ru

Ivan V. Vinogradov, Student; ivanvinogradov1111@gmail.com

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 22.06.2023.

Одобрена после рецензирования/ Reviced 10.07.2023.

Принята в печать/Accepted for publication 10.07.2023.