УДК: 004 DOI: 10.53816/23061456_2022_1–2_80

МЕТОДИКА ОЦЕНКИ ИНФОРМИРОВАННОСТИ ИСТОЧНИКА ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ О СТРУКТУРЕ КОРПОРАТИВНОЙ СИСТЕМЫ УПРАВЛЕНИЯ

METHODOLOGY FOR ASSESSING THE INFORMATION OF THE SOURCE OF DESTRUCTIVE EFFECTS ABOUT THE STRUCTURE OF THE CORPORATE GOVERNANCE SYSTEM

Канд. техн. наук С.А. Иванов

Ph.D. S.A. Ivanov

Военная академия связи им. С.М. Буденного

Реализация управляющих воздействий и взаимодействия корпоративных систем управления осуществляется посредством ресурсов систем связи. Формируемые при этом информационные направления являются прямым отображением структуры корпоративной системы управления. Корпоративные системы управления используют ресурсы сетей связи общего пользования, являющихся элементами международного киберпространства, посредством которого может осуществляться вскрытие структуры сети связи и соответствующей структуры корпоративной системы управления. Чем выше информированность источника деструктивных воздействий о структуре целевой системы управления, тем выше эффективность реализации деструктивных воздействий (физических, радиоэлектронных, информационно-технических), поэтому для своевременного принятия мер по снижению эффективности или недопущению реализации деструктивных воздействий необходимо иметь данные о информированности их источников о структуре целевой корпоративной системы управления.
Ключевые слова: корпоративная система управления, сеть связи, деструктивные воздействия.

Implementation of control actions and interaction of corporate management systems is carried out through the resources of communication systems. The information directions formed in this case are a direct reflection of the structure of the corporate management system. Corporate management systems use the resources of public communication networks, which are elements of international cyberspace, through which the structure of the communication network and the corresponding structure of the corporate management system can be opened. The higher the awareness of the source of destructive influences on the structure of the target control system, the higher the efficiency of the implementation of destructive influences (physical, electronic, information technology), therefore, in order to take timely measures to reduce efficiency, or to prevent the implementation of destructive influences, it is necessary to have data on their awareness. sources on the structure of the target corporate management system.
Keywords: corporate management system, communication network, destructive influences.

Введение

Развитие информационных и телекоммуникационных технологий привело к формированию из национальных сетей связи общего пользования международного киберпространства, являющегося неотъемлемым пространством жизнедеятельности человека [1]. Сети связи общего пользования (ССОП) предоставляют услуги связи множеству корпоративных систем управления, что, с одной стороны, позволяет им пользоваться достижениями информационного общества, а, с другой стороны, создает дополнительные уязвимости штатному функционированию и безопасности систем управления [2].

Становление и развитие киберпространства способствует развитию в нем угроз для пользователей — киберугроз, реализующихся посредством деструктивных программных воздействий. Статистика указывает на постоянный рост деструктивных информационно-технических воздействий наряду с количественным и качественным ростом характеристик образующих киберпространство сетей связи общего пользования [3].

Объекты воздействий источников деструктивных воздействий целевые, а их ресурсы ограничены. Поэтому знание структуры объекта воздействия позволят источнику воздействия нанести максимальный ущерб первому. Противодействие деструктивным воздействиям (физическим, радиоэлектронным, информационно-техническим) актуально для любой корпоративной системы управления (КСУ), особенно относящийся к критической инфраструктуре государства. Системы управления, в зависимости от их состава и структуры, занимаемых пространственных, физических и логических фрагментов и элементов ССОП, используемых информационных услуг и т.д., представляют объекты различной сложности для источников деструктивных воздействий в части определения структуры системы управления, что требует от источников деструктивных воздействий постоянного повышения информированности о структуре целевой КСУ для эффективного нанесения урона.

Таким образом, со стороны источника деструктивных воздействий существует задача, связанная с затруднением или срывом штатного функционирования корпоративной системы управления за счет нанесения эффективных дестабилизирующих воздействий опираясь на данные о структуре атакуемой системы управления, которую необходимо вскрыть.

Своевременное получение данных об информированности источника деструктивных воздействий о структуре защищаемой КСУ позволит заблаговременно принять меры к снижению последствий или недопущению проведения источником деструктивных воздействий целенаправленной сосредоточенной атаки, направленной на нанесение критического (ощутимого) урона корпоративной системе управления. Поэтому необходима разработка методов и методик, направленных на оценку информированности источников деструктивных воздействий о структуре корпоративных систем управления. Вариант решения этой задачи описан в статье.

Описание способа защиты

Существуют различные методики, описанные в публикациях и патентах на изобретения, в той или иной степени направленные на искомую оценку [4–6]. Однако в них имеются недостатки, относящиеся к отсутствию учета важности элементов сети для корпоративной системы управления, функционирование которой она обеспечивает, и связанной с этим снижением достоверности оценки, а также к распределению доступного ресурса сети между абонентами без оценки целенаправленности деструктивных воздействий — только на основе оценки их последствий.

Разработанная методика направлена на оценку информированности источника деструктивных воздействий о структуре корпоративной системы управления.

Реализация предлагаемой методики оценки поясняется обобщенной структурно-логической последовательностью (рис. 1), где на начальном этапе задают исходные данные:

– площадь реального географического фрагмента территории, на котором планируется размещение КСУ, (что можно реализовать различными способами, например, с помощью программного обеспечения «SAS. Планета» [7];

– количество и состав органов КСУ;

– структура информационных направлений (ИН) корпоративной системы управления, определяемая потребностями ее информаци-

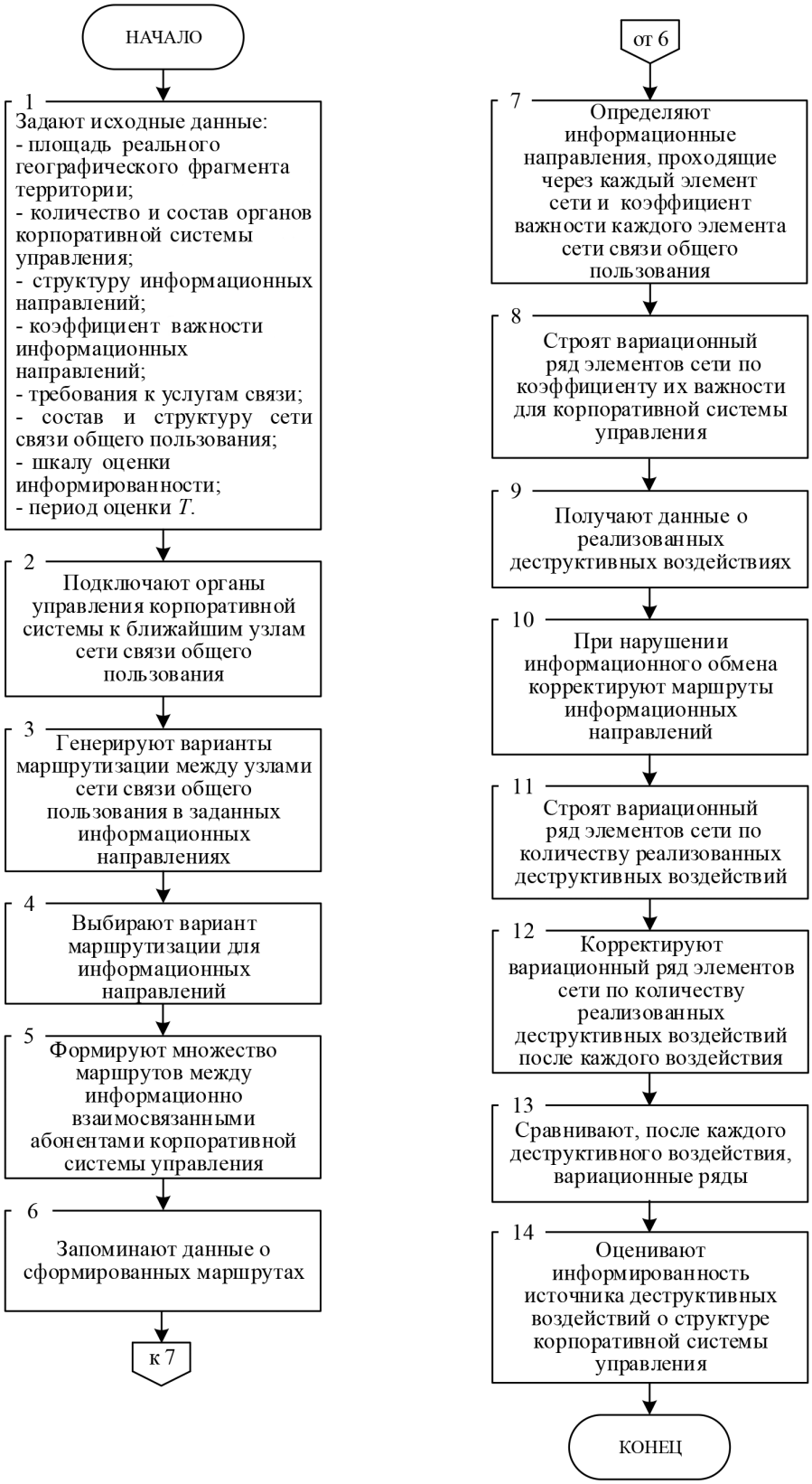

Рис. 1. Обобщенная структурно-логическая последовательность методики оценки информированности источника деструктивных воздействий о структуре корпоративной системы управления

онно взаимосвязанных абонентов, например, в виде матрицы из M информационных направлений. Матрица является квадратной размером $n \times n$, где n — количество абонентов системы управления;

– коэффициент важности $k_{\text{ИН}m}$ информационных направлений, который устанавливается исходя из приоритетов информационно взаимосвязанных абонентов ($k_{\text{ИН}m} \in \{1, 2 \ldots K_{\text{ИН}M}\}$, где $K_{\text{ИН}M}$ — количество коэффициентов важности M информационных направлений КСУ, $K_{\text{ИН}M} = M$);

– требования корпоративной системы управления к услугам связи;

– состав из I элементов и структуру ССОП (в данном случае, к элементам сети относятся узлы и линии связи), при этом топологию и структуру сети связи принимают в соответствии с текущей телекоммуникационной оснащенностью заданного реального географического фрагмента территории, либо моделируют при помощи известных способов моделирования фрагментов сетей связи [8, 9];

– шкалу оценки информированности источника деструктивных воздействий о структуре корпоративной системы управления, для которой устанавливаются деления и шаг между ними, определяющий точность (погрешность) оценки [10] (устанавливаемая градация оценки — делений заданной шкалы оценки информированности источника деструктивных воздействий о структуре корпоративной системы управления может определяться требованиями нормативных документов по безопасности информационного обмена КСУ, опытным путем, исходя из погрешности практических результатов и т.д.);

– период функционирования КСУ T, о котором необходимо иметь оценку информированности источника деструктивных воздействий о ее структуре.

На следующем этапе (блоки 2–6, рис. 1), формируют множество маршрутов между информационно взаимосвязанными абонентами корпоративной системы управления с учетом ее структуры и запоминают данные о маршрутах, для чего предварительно:

– подключают органы управления КСУ к ближайшим узлам сети связи общего пользования;

– генерируют варианты маршрутизации между узлами ССОП в заданных ИН. Маршрутизация может осуществляться по известным алгоритмам, например: алгоритм Дейкстры; алгоритм Беллмана – Форда; алгоритм поиска A*; алгоритм Флойда – Уоршелла; алгоритм Джонсона; алгоритм Ли; алгоритм Килдала;

– выбирают вариант маршрутизации в каждом информационном направлении.

Далее строят вариационный ряд элементов сети связи общего пользования по коэффициенту важности ее элементов (блоки 7–8, рис. 1), для чего определяют m_i-ые информационные направления корпоративной системы управления, проходящие через каждый i-й элемент сети, и коэффициент важности $k_{\text{ЭС}i}$ каждого элемента сети связи общего пользования для корпоративной системы управления

$$k_{\text{ЭС}i} = \sum_{m_i=1}^{M_i} m_i k_{\text{ИН}m},$$

где $k_{\text{ЭС}i}$ — коэффициент важности i-го элемента сети связи общего пользования, $i \in \{1, 2 \ldots I\}$; m_i — информационные направления корпоративной системы управления, проходящие i-й элемент сети связи общего пользования, $m_i \in \{1, 2 \ldots M_i\}$, M_i — количество ИН, проходящих через i-й элемент ССОП. Формируется множество коэффициентов важности элементов сети связи общего пользования из $k_{\text{ЭС}i} \in \{1, 2 \ldots K_{\text{ЭС}I}\}$, где $K_{\text{ЭС}I}$ — количество коэффициентов важности элементов сети, $K_{\text{ЭС}I} = I$.

В процессе мониторинга получают данные о реализованных деструктивных воздействиях (блоки 9, рис. 1) на ССОП с указанием элемента сети и времени воздействия. Под деструктивным воздействием (дестабилизирующим фактором) для сети связи будем понимать физический или технологический процесс внутреннего или внешнего, по отношению к сети электросвязи, характера, приводящий к выходу из строя элементов сети или ограничению их функционирования.

Далее необходимо построить вариационный ряд элементов ССОП по количеству реализованных деструктивных воздействий и сравнить его с вариационным рядом элементов сети связи общего пользования по коэффициенту важности ее элементов. Данное сравнение и позволит получить оценку информированности источника деструктивных воздействий о структуре КСУ на текущий временной этап.

При этом второй вариационный ряд необходимо корректировать с учетом изменения маршрутов информационных направлений под влиянием деструктивных воздействий и других факторов.

Для выполнения этих действий корректируют маршруты (блок 10, рис. 1) с нарушенным информационным обменом между информационно взаимосвязанными абонентами корпоративной системы управления после каждого реализованного воздействия, для чего выполняют действия в соответствии со структурно-логической последовательностью, представленной на рис. 2, где:

– после получения данных о реализованных деструктивных воздействиях в блоке 1, проверяют целостность информационного обмена в направлениях (блок 2), которые обслуживают элементы ССОП, подвергшиеся деструктивным воздействиям, в случае отсутствия нарушения целостности информационного обмена в данных направлениях, переходят к блоку 1;

– при нарушении информационного обмена в данных направлениях корректируют маршруты между информационно взаимосвязанными абонентами КСУ (блок 3) с учетом заданной структуры информационных направлений и выбранного варианта маршрутизации для каждого ИН, в котором нарушен информационный обмен, и запоминают данные о изменениях (блок 4);

– далее определяют m_i-ые информационные направления КСУ, проходящие через каждый i-й элемент сети, и коэффициент важности $k_{\text{ЭС}i}$ каждого элемента ССОП для корпоративной системы управления (блок 5), что обеспечивает корректировку коэффициентов важности элементов сети после каждого деструк-

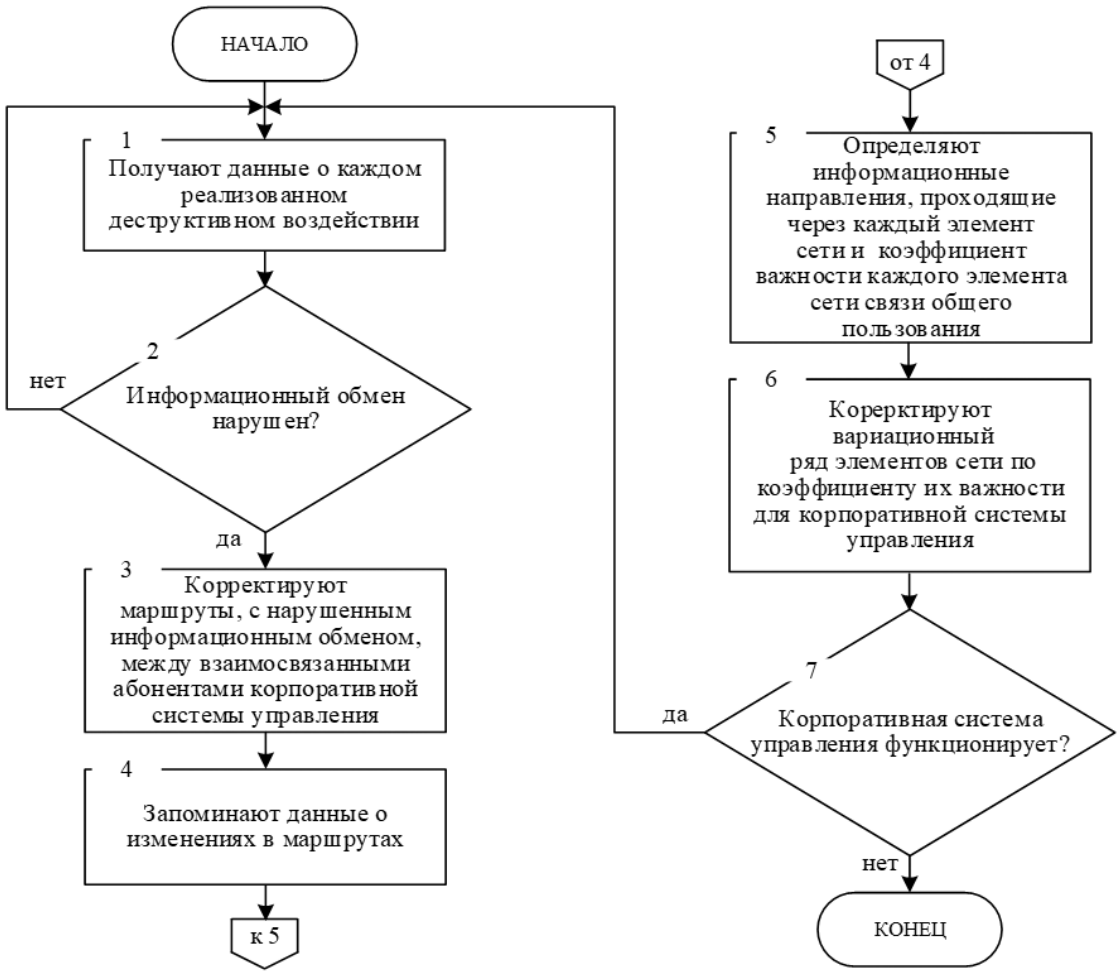

Рис. 2. Обобщенная структурно-логическая последовательность коррекции маршрутов с нарушенным информационным обменом между информационно взаимосвязанными абонентами корпоративной системы управления после каждого реализованного деструктивного воздействия

тивного воздействия (блок 6), приведшего к нарушению информационного обмена между абонентами КСУ;

– в блоке 7 проверяют функционирование корпоративной системы управления. Если КСУ функционирует, то переходят к блоку 1, если КСУ не функционирует, то заканчивают корректировку маршрутов с нарушенным информационным обменом ввиду отсутствия необходимости КСУ в них.

На следующем этапе определяют характеристики вариационного ряда элементов ССОП по количеству реализованных деструктивных воздействий, для чего:

– строят вариационный ряд элементов сети связи из $d_{\text{ЭС}i}$, с учетом времени воздействия и T, где $d_{\text{ЭС}i}$ – количество деструктивных воздействий на i-ый элемент сети связи общего пользования, $d_{\text{ЭС}i} \in \{1,2...D_{\text{ЭС}I}\}$, $D_{\text{ЭС}I} = I$. Для удобства дальнейшего использования данного вариационного ряда, при его сравнении с вариационным элементов ССОП по коэффициенту важности ее элементов, можно нормировать все его члены относительно старшего члена (максимального $d_{\text{ЭС}i}$);

– корректируют вариационный ряд после каждого реализованного воздействия с учетом времени воздействия, текущего (астрономического, модельного, оперативного) времени и T.

Итого имеем два вариационных ряда, корректируемых во времени в зависимости от реализующихся воздействий и результирующего состояния сети связи.

Полученные для сравнения вариационные ряды относятся к случайным дискретным, поэтому подходы их сравнения должны соответствовать данному типу, например:

– сравнение по коэффициенту вариации. Результат сравнения можно представить в виде отношения или разности коэффициентов вариации сравниваемых рядов. Коэффициент вариации используется при сравнении вариационных рядов, имеющих различную размерность, или одной размерности, но обладающими резкими различиями в своих значениях, затрудняющими их сопоставление;

– коэффициент корреляции вариационных рядов, устанавливающий корреляционную связь, направленную на выявление причинно-следственной связи между факторными (деструктивные воздействия) и результативными (маршрутизация — коэффициент важности элементов сети связи) признаками. Коэффициент корреляции может определяться, например, методом квадратов (метод Пирсона):

$$r_{k_{\text{ЭС}}d_{\text{ЭС}}} = \frac{\sum_{i=1}^{I}\left(k_{\text{ЭС}} \times d_{\text{ЭС}}\right)}{\sqrt{\sum_{i=1}^{I} k_{\text{ЭС}}^2 \times \sum_{i=1}^{I} d_{\text{ЭС}}^2}}.$$

Данный метод удобен в отношении простоты вычисления ошибки и достоверности коэффициента корреляции.

Оценивают информированность источника деструктивных воздействий о структуре корпоративной системы управления (блок 14, рис. 1), путем сопоставления результата сравнения вариационных рядов с заданной шкалой оценки.

Примером крайних значений оценки — «0» и «1» (при шкале от 0 до 1) являются:

«0» — равновероятное распределение деструктивных воздействий по всем элементам ССОП. Источник деструктивных воздействий не имеет данных о маршрутах информационных направлений и соответствующей структуре КСУ;

«1» — полное совпадение за время T последовательности и значений членов вариационного ряда элементов сети связи общего пользования по коэффициенту важности ее элементов и вариационного ряда элементов ССОП по количеству реализованных деструктивных воздействий. Источник деструктивных воздействий имеет полные данные о маршрутах ИН и соответствующей структуре корпоративной системы управления.

Вывод

Разработанная методика повышает достоверность оценки информированности источника деструктивных воздействий о структуре корпоративной системы управления за счет последовательного и обоснованного учета, при оценке, важности, маршрутизируемых в сети связи общего пользования, информационных направлений корпоративной системы управления и распределения деструктивных воздействий по элементам этой сети. Научная новизна методики, в отличии от известных, заключается в нахождении корреляционной связи между структурой корпоративной системы управления и оказывае-

мых на нее деструктивных воздействий. При этом учтены: динамика процессов маршрутизации информационных потоков КСУ и динамика осуществления деструктивных воздействий.

Литература

1. Стародубцев Ю.И., Давлятова М.А. Экономика цифровых информационных ресурсов. — СПб: Санкт-Петербургский политехнический университет Петра Великого. 2019. 452 с.

2. Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Техносферная война как основной способ разрешения конфликтов в условиях глобализации // Военная мысль. 2020. № 10. С. 16–21.

3. Positive Technologies. Аналитические отчеты по информационной безопасности. Официальный сайт Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1 (дата обращения: 13.07.2021).

4. Бухарин В.В., Карайчев С.Ю., Бречко А.А. и др. Метод защиты сервера услуг от DDoS атак за счет использования списков IP-адресов // Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2019. № 11–12 (137–138). С. 29–35.

5. Стародубцев Ю.И., Гречишников Е.В., Комолов Д.В. Способ обеспечения устойчивости сетей связи в условиях внешних деструктивных воздействий. Патент на изобретение RU 2379753 C1, опубл. 20.01.2010 бюл. № 2. Заявка 2008115815/09 от 21.04.2008.

6. Климов С.М., Сычев М.П., Астрахов А.В. Экспериментальная оценка противодействия компьютерным атакам на стендовом полигоне: Электронное учебное издание. — М.: МГТУ им. Н.Э. Баумана. 2013. 108 с.

7. Программное обеспечение «SAS. Планета» // [Электронный ресурс], URL: http://www.sasgis.org/sasplaneta/, дата обращения 03.07.2020.

8. Белов К.Г., Вершенник Е.В., Иванов С.А., Смирнов И.Ю. и др. Способ моделирования динамически взаимодействующих стационарных сетей и мобильных узлов связи с различными элементами сопряжения. Патент на изобретение RU 2723296 C1, опубл. 09.06.2020 бюл. № 16. Заявка № 2019137888 от 25.11.2019.

9. Беликова И.С., Закалкин П.В., Сухорукова Е.В. и др. Моделирование сетей связи с учетом топологических и структурных неоднородностей // Информационные системы и технологии. 2017. № 2 (100). С. 93–101.

References

1. Starodubtsev Yu.I., Davlyatova M.A. The economics of digital information resources. St. Petersburg. Polytechnic University Publ. 2019. 452 p. (in Russian).

2. Starodubtsev Yu.I., Zakalkin P.V., Ivanov S.A. Technosphere warfare as the chief method of conflict settlement in conditions of globalization. Military Thought. 2020. № 10. P. 16–21. (in Russian).

3. Analytical reports on information security. Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1 (date of the application: 13.07.2021).

4. Bukharin V.V., Karaychev S.Y., Brechko A.A. and others. Service server protecting method from DDoS attacks through the using IP-addresses lists. Voprosy oboronnoi tekhniki. Seriia 16. Tekhnicheskie sredstva protivodestviia terrorizmu. 2019. № 11–12. P. 29–35. (in Russian).

5. Starodubtsev Yu.I, Grechishnikov E.V., Komolov D.V. Method of stabilising communication networks in conditions of disruptive external effects. Invention patent RU 2371764 C1. Publ. 20.01.2010.

6. Klimov S.M., Sychov M.P., Astrakhov A.V. Experimental assessment of countering computer attacks at the test site. — Moscow: Bauman University. Electronic educational publ. 2013. 108 p. (in Russian).

7. Software «SAS.Planeta». URL: http://www.sasgis.org/sasplaneta/. (date of the application: 23.07.2021).

8. Belov K.G., Vershennik E.V., Ivanov S.A., Zakalkin P.V., Smirnov I.Iu. and others. Method for simulating dynamically interacting fixed-line networks and mobile communication nodes with different interface elements. Invention patent RU 2723296 C1. Publ. 09.06.2020.

9. Belikova I.S., Zakalkin P.V., Suxorukova E.V. and others. Modeling of network connection with regard typological and structural heterogeneity. Information systems and technologies. 2017. № 2 (100). P. 93–101. (in Russian).