Сергей В. Скрыль[1], Виктор В. Гайфулин[2], Дмитрий В. Домрачев[3],
Владимир М. Сычев[4], Юлия В. Грачёва[5]

[1,4,5]Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» (МГТУ им. Н.Э. Баумана), ул. 2-я Бауманская, 5, Москва, 105005, Россия

[2,3]Федеральное государственное казенное военное образовательное учреждение высшего образования «Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко» Министерства обороны, ул. Красина, 4, Краснодар, 350063, Россия

[1]e-mail: skryl@bmstu.ru, https://orcid.org/0000-0002-4309-6255

[2]e-mail: Gayfulin2007@yandex.ru, https://orcid.org/0000-0001-6026-5885

[3]e-mail: dobryi01@list.ru, https://orcid.org/0000-0002-0443-8304

[4]e-mail: dviu@mail.ru, https://orcid.org/0000-0002-2372-8980

[5]y.v.gracheva@yandex.ru, https://orcid.org/0000-0003-0884-5617

АКТУАЛЬНЫЕ ВОПРОСЫ ПРОБЛЕМАТИКИ ОЦЕНКИ УГРОЗ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org/10.26583/bit.2021.1.07

Аннотация. Статья посвящена анализу возможностей существующего методического аппарата определения актуальных угроз безопасности информации по оценке киберустойчивости значимых объектов критической информационной инфраструктуры (ЗО КИИ). В статье обосновывается актуальность вопросов повышения эффективности механизмов защиты информационных ресурсов этих объектов от компьютерных атак как предпосылки обеспечения их киберустойчивости. Даются определения данного понятия. Подробно анализируются существующие методики вероятностной оценки актуальных угроз безопасности информации на примере оценки уровня угрозы компьютерной атаки на информационные ресурсы ЗО КИИ. Приводятся принципиальные недостатки этих методик – эмпирический характер оценки, отсутствие учета тех случайных состояний угроз безопасности информации, которые характеризуют их динамику, а также ограниченное число случайных событий, в тех моделях, которые учитывают динамику возникновения и реализации угроз безопасности информации. Анализируются обстоятельства, не позволяющие характеризовать существующий уровень проработки методов оценки эффективности защиты информации от несанкционированного доступа (НСД), как достаточный для адекватной характеристики киберустойчивости. Приводятся основания, указывающие на необходимость адекватной оценки эффективности защиты информационных ресурсов ЗО КИИ от компьютерных атак как предпосылки обоснованности требований к мерам обеспечения киберустойчивости этих объектов. Обосновываются направления преодоления недостатков существующих методик оценки эффективности защиты информации от НСД.

Ключевые слова: компьютерная атака, значимые объекты критической информационной инфраструктуры, киберустойчивость, оценки угроз компьютерных атак.

Для цитирования: СКРЫЛЬ, Сергей В. и др. АКТУАЛЬНЫЕ ВОПРОСЫ ПРОБЛЕМАТИКИ ОЦЕНКИ УГРОЗ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. Безопасность информационных технологий, [S.l.], v. 28, n. 1, p. 84–94, jan. 2021. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1323>. Дата доступа: 05 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.07.

Sergey V. Skryl'[1], Victor V. Gaifulin[2], Dmitry V. Domrachev[3],
Vladimir M. Sychev[4], Yulia V. Gracheva[5]
[1,4,5]Federal State Educational Institution of Higher Education
«Bauman Moscow State Technical University»,
2nd Bauman str., 5, Moscow, 105005, Russia
[2,3]Federal State Government Military Educational Establishment education
«Krasnodar Higher Military awarded by the Order of Zhukov and by the Orders of October Revolution and the Red Banner School named after the general of the Army S.M. Shtemenko» of the Department of Defense of Russian Federation,
Krasina str., 4, Krasnodar, 350063, Russia
[1]e-mail: skryl@bmstu.ru, https://orcid.org/0000-0002-4309-6255
[2]e-mail: Gayfulin2007@yandex.ru, https://orcid.org/0000-0001-6026-5885
[3]e-mail: dobryi01@list.ru, https://orcid.org/0000-0002-0443-8304
[4]e-mail: dviu@mail.ru, https://orcid.org/0000-0002-2372-8980
[5]y.v.gracheva@yandex.ru, https://orcid.org/0000-0003-0884-5617

Topical issues of the problem of assessment of threats of cyber attacks on information resources of significant facilities of critical information infrastructure

DOI: http://dx.doi.org/10.26583/bit.2021.1.07

Annotation: This paper opens a series of studies devoted to the problems of assessing the characteristics of measures to ensure the cyber resilience of information resources of critical information infrastructure objects. The paper substantiates the relevance of issues of increasing the efficiency of mechanisms for detecting, preventing and eliminating the consequences of computer attacks on the information resources of critical information infrastructure objects as a prerequisite for ensuring the cyber stability of these objects. A detailed analysis of the methodological apparatus of probabilistic assessment of the relevance of threats to information security is provided, the provisions of which are reflected in the regulatory and methodological documents of the FSTEC of Russia. The circumstances that do not allow characterizing the existing level of development of mathematical methods in the field of information protection against unauthorized access as high are analyzed. The necessity of solving the problems of adequate assessment of the effectiveness of mechanisms for detecting, preventing and eliminating the consequences of computer attacks on the information resources of critical information infrastructure objects is substantiated as a prerequisite for substantiating the requirements for measures to ensure the cyber stability of these segments.
Keywords: computer attack, critical information infrastructure objects, cyber stability of critical information infrastructure objects, the effectiveness of mechanisms for detecting, preventing and eliminating the consequences of computer attacks on information resources of critical information infrastructure objects, assessment of current threats to information security.
For citation: SKRYL', Sergey V. et al. Topical issues of the problem of assessment of threats of cyber attacks on information resources of significant facilities of critical information infrastructure. IT Security (Russia), [S.l.], v. 28, n. 1, p. 84–94, jan. 2021. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1323>. Date accessed: 05 feb. 2021. DOI: http://dx.doi.org/10.26583/bit.2021.1.07.

Введение

Анализ перспектив развития теории и практики построения инфокоммуникационной среды [1] позволяет выявить устойчивую тенденцию расширения возможностей распределенной обработки данных [2] за счет совершенствования механизма теледоступа в информационной инфраструктуре.

Вместе с тем подобная тенденция, как позитивная, влечет за собой и ряд негативных факторов, наиболее серьезным из которых выступают объективно существующие уязвимости объектов информационной инфраструктуры для информационно-технического воздействия (ИТВ) [3]. Реализация нарушителем такого рода воздействия приводит к снижению эффективности информационных технологий, реализуемых этими объектами,

что, в свою очередь, приводит к ущербу в тех областях, в интересах которых они функционируют. Если такой ущерб существенный, то соответствующую информационную инфраструктуру относят к критической[1] [4].

Исходя из анализа состояния информационной безопасности и национальных приоритетов Российской Федерации в Доктрине информационной безопасности одним из основных направлений обеспечения информационной безопасности определено «повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры»[2].

1. Киберустойчивость значимых объектов критической информационной инфраструктуры как объект исследования

Характерным для значимых объектов критической информационной инфраструктуры (ЗО КИИ) типом ИТВ являются компьютерные атаки, которые представляют собой целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств[3]. Следует отметить, что для объектов ЗО КИИ наряду с термином «компьютерная атака» часто применяется эквивалентный по смыслу термин «кибератака» [5]. Это послужило основанием для использования термина «киберустойчивость» для характеристики устойчивости функционирования этих систем в условиях кибератак. Несмотря на усиленную в последнее время эксплуатацию данного термина, включая использование его в официальных документах, официальной трактовки данного понятия не существует. Среди многочисленных авторских определений наиболее обоснованным можно считать определение, приводимое в [6]: «под киберустойчивостью понимается способность информационно-телекоммуникационной сети поддерживать управление в условиях воздействия компьютерных атак» и приводимое в [7]: «киберустойчивость – это свойство информационной системы, позволяющее ей существовать в условиях постоянных атак»

Среди зарубежных трактовок данного понятия следует выделить определение киберустойчивости, используемое IBM: «киберустойчивость – это выравнивание возможностей по предотвращению, обнаружению и реагированию для управления, смягчения и ухода от кибератак».

Понимание свойства киберустойчивости позволяет поменять отношение к компьютерным атакам и усвоить крайне важное обстоятельство, что защититься от всех атак нельзя. Необходимо проектировать информационную систему как киберустойчивую. От этого и строится стратегия обеспечения киберустойчивости.

Указанное требование позиционирует механизмы обеспечения киберустойчивости ЗО КИИ в качестве базовых для государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

[1]Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
[2]Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. Российская газета, 2016.
[3]ГОСТ Р 51275-2006: Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

Касаясь направлений совершенствования данной системы, обозначенных в Указе Президента РФ «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»[4], одной из важнейших задач является «осуществление контроля степени защищенности информационных ресурсов Российской Федерации от компьютерных атак».

Решение данной задачи напрямую связано с решением проблемы адекватной оценки механизмов обеспечения киберустойчивости ЗО КИИ. Вместе с тем высокая технологическая сложность этих механизмов относит вопросы их исследования, с целью обоснования направлений совершенствования, к числу сложных как в научном, так и в практическом плане. В свою очередь всесторонний и системный характер [8] подобных исследований достигается адекватностью оценки [9] возможностей механизмов обеспечения киберустойчивости ЗО КИИ по реализации функций обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы этих объектов.

В соответствии с системным подходом, исследование механизмов обеспечения киберустойчивости в рамках такой довольно специфичной области, как информационная среда ЗО КИИ, связано с решением проблемы оценки их возможностей по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные ресурсы с достаточной степенью адекватности для обоснованности решений о направлениях совершенствования этих механизмов. В соответствии с положениями статьи 12 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»[5] выработка мер по повышению устойчивости функционирования ЗО КИИ осуществляется на основе оценки ее безопасности.

Поэтому крайне актуальной проблемой является повышение адекватности существующих методик оценки эффективности мер защиты информации для обоснованности решений о направлениях совершенствования процессов обнаружения, предупреждения и ликвидации последствий компьютерных атак на их информационные ресурсы объектов ЗО КИИ.

Касаясь принципиальных вопросов выбора методов исследования, следует учитывать характерную особенность ЗО КИИ, относящихся к системам, для исследования которых, вследствие существенного ущерба от риска нарушения безопасности исследуемых информационных процессов, не могут быть применены натурные эксперименты. Это обусловливает необходимость использования математического моделирования в качестве методологического аппарата для исследования вопросов обеспечения киберустойчивости таких объектов [10].

[4]Указ Президента РФ от 22 декабря 2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

[5]Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Возможности существующего методического аппарата определения актуальных угроз безопасности информации по оценке уровня угрозы компьютерной атаки

Официальными методиками, регламентирующими процедуру оценки защищенности информации, являются методики вероятностной оценки актуальных угроз безопасности информации, приводимые в ряде нормативно-методических документов ФСТЭК России. В основу этих методик положена экспертиза факторов, способствующих возникновению угроз безопасности информации.

Проанализируем возможность использования этих методик для оценки уровня угрозы компьютерной атаки на информационные ресурсы значимого объекта КИИ.

В соответствии с положениями рассматриваемых методик отнесение факторов, способствующих возникновению угроз компьютерных атак, осуществляется путем установления, на основе эмпирического опыта, соответствия между такого рода источниками и их признаками. В результате формируется множество $\{a_k\}$, $k = 1, 2, \ldots, |\{a_k\}|$, элементы которого являются признаками источников угроз, а индексы – их номерами.

Для ЗО КИИ источниками угроз компьютерных атак являются:

$k = 1$ – иностранные спецслужбы;

$k = 2$ – криминальные структуры;

$k = 3$ – конкурирующие организации;

$k = 4$ – персонал объекта;

$k = 5$ – производители оборудования и организации, осуществляющие ремонт и обслуживание средств вычислительной техники (СВТ) и периферийного оборудования объекта;

a_1 – наличие интереса у иностранных спецслужб к информационным ресурсам объекта;

a_2 – наличие интереса у криминальных структур к информационным ресурсам объекта;

a_3 – наличие интереса представителей промышленно-деловой и финансово-кредитной среды, конкурирующих с промышленными и финансовыми организациями, использующих информационные ресурсы объекта;

a_4 – самостоятельное проведение должностными лицами объекта обслуживания СВТ и периферийного оборудования;

a_5 – использование несертифицированного программного обеспечения (ПО) при техническом обслуживании и ремонтно-восстановительных работах на объекте.

Особенностью выявления уязвимостей информационных ресурсов значимого объекта КИИ, через которые возможна реализация угроз компьютерных атак, является использование расчетных методик, позволяющих установить факт потенциальной возможности угрозы.

При определении уязвимостей информационных ресурсов объекта к реализации угроз компьютерных атак проводится экспертный анализ информационной среды объекта. В результате формируется множество $\{b_l\}$, $l = 1, 2, \ldots, L$, элементы которого определяют уязвимости. При этом индексы соответствуют номерам уязвимостей из их перечня.

В случае оценки уровня угрозы компьютерной атаки на информационные ресурсы объекта уязвимыми для такого рода угроз являются:

b_1 – драйверы средств ввода информации;

b_2 – драйверы средств отображения информации;

b_3 – драйверы средств обработки информации;

b_4 – драйверы микросхем BIOS;

b_5 – ПО серверов с открытым физическим доступом;
b_6 – ПО коммуникационного оборудования объекта;
b_7 – стек протоколов TCP/IP;
b_8 – шлюз выхода в Internet;
b_9 – протоколы межсетевого взаимодействия прикладного уровня;
b_{10} – недокументированные точки межсетевого взаимодействия;
b_{11} – открытые общие сетевые ресурсы;
b_{12} – несертифицированные компоненты ПО;
b_{13} – электронная почта;
b_{14} – Web-браузер;
b_{15} – кабели оборудования объекта на участках, где к ним имеется физический доступ.

Для количественной оценки уязвимости, через которую возможна реализация компьютерной атаки на информационные ресурсы значимого объекта КИИ, определяется вероятностью наличия соответствующих благоприятных условий. Данная вероятность оценивается экспертно специалистами в области кибербезопасности. Результаты оценки представляются лингвистическими значениями: «да», «вероятно», «возможно», «маловероятно» и «нет», характеризующими возможности использования k-м источником угрозы компьютерной атаки l-ой уязвимости. Каждому из пяти лингвистических значений ставится в соответствие вероятность p_{kl} использования k-м источником l-ой уязвимости. На основании данной вероятности определяется вероятность P_l использования l-й уязвимости (l = 1, 2, …, 15) возможными пятью источниками угроз:

$$P_l = 1 - (\gamma_{1}\cdot(1 - p_{l1})\cdot\gamma_{2}\cdot(1 - p_{l2})\cdot\gamma_{3}\cdot(1 - p_{l3})\cdot\gamma_{4}\cdot(1 - p_{l4})\cdot\gamma_{5}\cdot(1 - p_{l5})), \quad (1)$$

где γ_{lk} – коэффициент соответствия, равный 1, если l-я уязвимость соответствует k-му источнику и 0, если не соответствует.

Это позволяет сформировать множество $\{u_m\}$, m = 1, 2, …, M, угроз компьютерных атак [11]:

u_1 – загрузка вредоносного ПО с функциями альтернативной ОС с расширенными полномочиями;
u_2 – несанкционированное копирование информации;
u_3 – несанкционированная модификация информации;
u_4 – внедрение ложного доверенного объекта;
u_5 – подмена системного ПО;
u_6 – перенаправление сетевого трафика;
u_7 – манипулирование данными в удаленном режиме;
u_8 – вскрытие электронного почтового ящика;
u_9 – блокирование электронного почтового ящика;
u_{10} – подмена Web-браузеров;
u_{11} – использование ошибок в алгоритмах прикладного ПО;
u_{12} – блокирование хоста пользователя;
u_{13} – блокирования маршрутизатора;
u_{14} – обход межсетевого экрана.

Количественной характеристикой уровня m-ой угрозы компьютерной атаки, где m = 1, 2, …, 14, на информационные ресурсы ЗО КИИ является вероятность:

$$P_m^{(Y)} = 1 - \prod(1 - \alpha_{lm} \cdot P_l), \quad (2)$$

где P_l – соответствует выражению (1);

α_{lm} – коэффициент актуальности уязвимостей информации объекта для инициализации угроз компьютерных атак, равный 1, если *l*-я уязвимость актуальна для инициализации *m*-ой угрозы и 0, если не актуальна.

Значения коэффициента актуальности уязвимостей информации ЗО КИИ для инициализации угроз компьютерных атак приводятся в табл. 1.

Количественной характеристикой деструктивного воздействия компьютерных атак на информационные ресурсы ЗО КИИ является вероятность:

$$P_m^{(Д)} = 1 - \prod(1 - \delta_{mn} \cdot P_m^{(У)}), \quad (3)$$

где $P_m^{(У)}$ – соответствует выражению (2);

n – номер деструкции (1 – несанкционированное копирование информации, 2 – ее несанкционированная модификация, 3 – блокирование доступа к информационным ресурсам объекта);

δ_{mn} – коэффициент деструкции, равный 1, если *m*-я угроза реализует *n*-ю деструкцию и 0, если не реализует.

Значения коэффициента деструкции угроз компьютерных атак на информационные ресурсы ЗО КИИ приводятся в табл. 2. В таблице использованы следующие условные обозначения деструкций: *НК* – несанкционированное копирование информации, *НМ* – несанкционированная модификация информации, *БД* – блокирование доступа к информационным ресурсам.

Таблица 1. Значения коэффициента актуальности уязвимостей информации ЗО КИИ для инициализации угроз компьютерных атак

Угрозы компьютерных атак	**Уязвимости информационных ресурсов ЗО КИИ к реализации угроз компьютерных атак**														
	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}	b_{13}	b_{14}	b_{15}
u_1	1	0	0	0	1	1	0	0	0	0	0	1	1	1	1
u_2	0	0	0	0	1	0	0	1	1	1	1	1	1	1	1
u_3	1	1	1	0	1	0	0	1	1	1	1	1	1	1	1
u_4	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1
u_5	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1
u_6	1	1	1	0	1	1	1	1	1	1	0	0	1	1	1
u_7	1	1	1	0	0	0	1	0	0	0	0	0	1	0	0
u_8	1	1	1	0	0	1	0	0	1	0	0	0	1	1	0
u_9	1	1	1	0	0	1	0	0	1	0	0	0	1	1	0
u_{10}	1	1	1	0	0	1	0	0	1	0	0	0	1	0	1
u_{11}	1	1	0	0	0	0	0	0	0	0	1	0	1	0	0
u_{12}	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0
u_{13}	1	0	0	0	0	1	0	1	0	1	1	1	0	0	0
u_{14}	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0

Таблица 2. Значения коэффициента деструкции угроз компьютерных атак на информационные ресурсы ЗО КИИ

Деструкции	**Угрозы компьютерных атак**													
	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8	u_9	u_{10}	u_{11}	u_{12}	u_{13}	u_{14}
НК	1	1	0	1	0	0	1	1	0	1	1	0	0	1
НМ	1	0	1	1	1	1	1	0	0	1	1	0	0	1
БД	1	0	0	1	0	0	1	0	1	1	1	1	1	1

Из изложенного следует, что достоинством существующих методик оценки актуальных угроз безопасности информации является простота процедур оценки. К

недостаткам же, принципиально ограничивающих их использование для адекватной оценки мер обеспечения киберустойчивости ЗО КИИ, следует отнести отсутствие возможности учета динамики воздействия такого рода угроз, и низкая статистическая достоверность, характерная для экспертных оценок.

3. Обстоятельства, обусловливающие необходимость совершенствования методик оценки

Анализируя в целом существующий уровень проработки вопросов использования методов математического моделирования в проблематике защиты информации от компьютерных атак, можно выявить ряд обстоятельств, не позволяющих рассматривать применяемый аппарат математического моделирования как адекватный.

Первое обстоятельство связано с применением процедур оценки возможностей нарушителя, основанных на эмпирике. Характерным примером здесь является рассмотренная выше методика ФСТЭК России, регламентирующая порядок оценки актуальных угроз безопасности информации. Как показано в [12] и лингвистический характер оценки субъектно-объектных отношений между угрозами и порождающими их уязвимостями информации, и последующий переход к количественному представлению их вероятностных характеристик, основанные на экспертном подходе, привносят большую долю субъективизма в результаты оценки и, как следствие, являются причиной низкой адекватности используемых процедур оценки.

Второе обстоятельство связано с отсутствием учета тех случайных состояний угроз безопасности информации, которые характеризуют их динамику. В п. 5 «Определение вероятностей реализации угроз» нормативно методического документа ФСТЭК России, регламентирующего порядок оценки актуальных угроз безопасности информации, прямо указывается, что модели для определения вероятности угрозы в динамике ее возникновения и реализации в настоящее время отсутствуют.

Третье обстоятельство связано с ограниченным числом случайных событий, в тех моделях, которые учитывают динамику возникновения и реализации угроз безопасности информации. К таким моделям относятся модели, учитывающие лишь продолжительность угрозы, но не учитывающие случайные состояния, связанные с динамикой их возникновения [13, 14].

Преодоление указанных недостатков в проблематике оценки киберустойчивости ЗО КИИ возможно лишь в том случае, когда формальное описание угроз компьютерных атак на информационные ресурсы этих объектов позволяет математически представить все условия, характерные для динамики такого рода угроз.

Характеризуя в целом потенциал методологии компьютерной безопасности, следует отметить, что исследования в данной области позволили дать всестороннюю характеристику угроз НСД к компьютерной информации [6, 11, 15, 16]. Вместе с тем, применяемые в исследованиях методики не обладают той степенью системности, которая позволила бы в формализованном представлении исследуемых процессов учесть особенности динамики компьютерных атак.

Реализованные в рамках данных методик подходы к систематизации проявлений такого рода угроз носят субъективный характер и в крайне ограниченном виде отражают системные проявления субъектно-объектных отношений в процессах, характерных для данной предметной области, включая формальную интерпретацию динамики компьютерных атак. Исключение составляют приведенные в [17, 18] математические модели своевременности реагирования на компьютерные атаки, учитывающие не только длительность угрозы и реагирования на нее средствами защиты, но и моменты начала атаки

и ее обнаружения. Вместе с тем, наличие в этих моделях целого ряда ограничений, связанных с использованием стандартных математических абстракций, не позволило обеспечить ожидаемую степень адекватности.

Заключение

Возрастающие требования к обеспечению киберустойчивости ЗО КИИ в целом и требования к обоснованности характеристик процессов обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы этих объектов, в частности, ставят вопросы оценки угроз компьютерных атак в разряд актуальных и нуждающихся в проработке как в методическом, так и в прикладном плане.

СПИСОК ЛИТЕРАТУРЫ:

1. Величко В.В., Катунин Г.П., Шувалов В.П.; под ред. профессора Шувалова В.П. Основы инфокоммуникационных технологий: учебное пособие для вузов. М.: Горячая линия–Телеком, 2009. – 712 с.
2. Пятибратов А.П., Гудыно Л.П., Кириченко А.А. Вычислительные системы, сети и телекоммуникации: учебник. М.: Финансы и статистика, 2004. – 512 с.
3. Гриняев С.Н. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны. М.: Харвест, 2004. – 426 с.
4. Гавдан, Григорий П., Иваненко, Виталий Г., Салкуцан, Алексей А. Обеспечение безопасности значимых объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.]. Т. 26, № 4. С. 69–82, дек. 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1232 (дата обращения: 14.10.2020). DOI: http://dx.doi.org/10.26583/bit.2019.4.05.
5. Электронный словарь: сайт. URL: https://ru.wiktionary.org/wiki/кибератака (дата обращения: 14.10.2020).
6. Коцыняк М.А., Кулешов И.А., Кудрявцев А.М., Лаута О.С. Киберустойчивость информационно-телекоммуникационной сети / СПб.: Бостон-спектр, 2015. – 150 с.
7. Лукацкий А.В. Киберустойчивость, киберживучесть, кибернадежность, кибернепрерывность. URL: http://www.iksmedia.ru/blogs/post/5445277-Kiberustojchivost-kiberzhivuchest.html#ixzz6QU4Yn2yY (дата обращения: 14.10.2020).
8. Скрыль С.В., Шелупанов А.А. Основы системного анализа в защите информации: учебное пособие для студентов высших учебных заведений. М.: Машиностроение, 2008. – 138 с.
9. Скрыль С.В., Никулин С.С., Сычев А.М., Пономарёв М.В., Ле Ву Хыонг Занг. Показатели адекватности структурированных систем оценки характеристик информационных процессов. / Промышленные АСУ и контроллеры. М: Научтехлитиздат, 2017. № 10. С. 31–37. URL: https://www.elibrary.ru/item.asp?id=30710941 (дата обращения: 14.10.2020).
10. Скрыль С.В., Сычев В.М., Астрахов А.В., Гайфулин В.В., Никитина Ю.С. Формальные аспекты представления математической модели характеристики киберустойчивости информационной среды. Промышленные АСУ и контроллеры, 2020. № 3. С. 40–46. DOI: http://dx.doi.org/10.25791/asu.3.2020.1169.
11. Сычев А.М., Коробец Б.Н., Смирнов С.Н. и др. Безопасность операционных систем: учеб. пособие для студ. учреждений высш. образования; под ред. С.В. Скрыля. М.: Издательский центр «Академия», 2021. – 256 с.
12. Скрыль С.В., Мещерякова Т.В., Голубков Д.А., Арутюнова В.И. Оценка защищенности информации от вирусных атак: существующий и перспективный методический аппарат. Промышленные АСУ и контроллеры. М: Научтехлитиздат, 2018. №9. С. 51–62. URL: https://www.elibrary.ru/item.asp?id=35648304 (дата обращения: 14.10.2020).
13. Багаев, Д.А.; Лаврухин, Ю.Н.; Скрыль, С.В. Показатели эффективности информационных процессов и их защищенности в системах реального времени. Безопасность информационных технологий, [S.l.]. Т. 16, № 3. С. 104–106, сен. 2009. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/858 (дата обращения: 14.10.2020).
14. Курило А.П. [и др.]. Оценка защищенности компьютерной информации: пути решения проблемы. // Интеллектуальные системы (INTELS’ 2010): труды девятого международного симпозиума. М.: МГТУ им. Н.Э. Баумана, 2010. С. 564–566.

15. Информационная безопасность открытых систем: учебник для вузов. В 2-х томах. Т. 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников [и др.]. М.: Горячая линия–Телеком, 2006. – 536 с.
16. Макаренко С.И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. № 3. С. 292–376. URL: https://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf (дата обращения: 14.10.2020).
17. Кондаков С.Е., Мещерякова Т.В., Скрыль С.В., Стадник А.Н., Суворов А.А. Вероятностное представление условий своевременного реагирования на угрозы компьютерных атак // Вопросы кибербезопасности. М.: АО «НПО «Эшелон», 2019. № 6. С. 59–68. DOI: http://dx.doi.org/10.21681/2311-3456-2019-6-59-68.
18. Skryl’ S. et al. Assessing the Response Timeliness to Threats as an Important Element of Cybersecurity: Theoretical Foundations and Research Model. In: Kravets A., Groumpos P., Shcherbakov M., Kultsova M. (eds) Creativity in Intelligent Technologies and Data Science. CIT&DS 2019. Communications in Computer and Information Science, vol. 1084. Springer, Cham. 2019. P. 258–269. DOI: http://dx.doi.org/10.1007/978-3-030-29750-3_20.

REFERENCES:

[1] Velichko V.V., Katunin G.P., Shuvalov V.P.; edited by professor Shuvalov V.P. Basics of infocommunication technologies: textbook for universities. M.: Gorjachaja linija –Telekom, 2009. – 712 p. (in Russian).
[2] Pjatibratov A.P., Gudyno L.P., Kirichenko A.A. Computing systems, networks and telecommunications: textbook. M.: Finansy i statistika, 2004. 512 p. (in Russian).
[3] Grinjaev S.N. The battlefield is cyberspace. Theory, techniques, means, methods and systems of information warfare. M.: Harvest, 2004. – 426 p. (in Russian).
[4] Gavdan, Grigory P., Ivanenko, Vitaliy G., Salkutsan, Alexei A. Security of significant objects of critical information infrastructure. IT Security (Russia), [S.l.]. V. 26, no. 4. P. 69–82, dec. 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1232 (accessed: 14.10.2020). DOI: http://dx.doi.org/10.26583/bit.2019.4.05.
[5] Electronic dictionary: site. URL: https://ru.wiktionary.org/wiki/кибератака. (accessed: 14.10.2020) (in Russian).
[6] Kotsynyak M.A., Kuleshov I.A., Kudryavtsev A.M., Lauta O.S. Cyber resilience of the information and telecommunications network. SPb.: Boston-spectr, 2015. – 150 p.
[7] Lukackij A.V. Cyber resilience, cyber survivability, cyber reliability, cyber continuity. URL: http://www.iksmedia.ru/blogs/post/5445277-Kiberustojchivost-kiberzhivuchest.html#ixzz6QU4Yn2yY (accessed: 18.10.2017) (in Russian).
[8] Skryl’ S.V., Shelupanov A.A. Fundamentals of systems analysis in information security: a textbook for students of higher educational institutions. M.: Mashinostroenie, 2008. – 138 p. (in Russian).
[9] Skryl’ S.V., Nikulin S.S., Sychev A.M., Ponomarev M.V., Le Vu Huong Zang. Indicators of the adequacy of structured systems for assessing the characteristics of information processes. Promyshlennye ASU i kontrollery. M.: Nauchtekhlitizdat, 2017. no. 10. P. 31–37. URL: https://www.elibrary.ru/item.asp?id=30710941 (accessed: 14.10.2020) (in Russian).
[10] Skryl’ S.V., Sychev V.M., Astrakhov A.V., Gaifulin V.V., Nikitina Yu.S. Formal aspects of the representation of the mathematical model of the characteristics of the cyber stability of the information environment. Promyshlennye ASU i kontrollery. 2020. no. 3. P. 40–46. DOI: http://dx.doi.org/10.25791/asu.3.2020.1169 (in Russian).
[11] Sychev A.M., Korobets B.N., Smirnov S.N., edited by Skryl’ S.V. Operating system security: a textbook for students of higher educational institutions. M.: Akademija [publishing house academia], 2021. – 256 p. (in Russian).
[12] Skryl’ S.V., Meshcheryakova T.V., Golubkov D.A., Arutyunova V.I. Assessment of information security against virus attacks: existing and promising methodological apparatus. Promyshlennye ASU i kontrollery. M.: Nauchtekhlitizdat, 2018. no. 9. P. 51–62. URL: https://www.elibrary.ru/item.asp?id=35648304 (accessed: 14.10.2020) (in Russian).
[13] Bagaev, D.F., Lavruhin, Ju.N., Skril’ S.V. Indicators of the effectiveness of information processes and their security in real-time systems. IT Security (Russia), [S.l.]. V. 16, no. 3. P. 104–106, sep. 2009. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/858 (accessed: 14.10.2020) (in Russian).
[14] Kurilo A.P. Assessment of the security of computer information: ways to solve the problem. Intellektual'nye sistemy (INTELS’ 2010): trudy devjatogo mezhdunarodnogo simpoziuma. M.: MGTU im. N.Je. Baumana, 2010. P. 564–566 (in Russian).

[15] Zapechnikov S.V. Information security of open systems: a textbook for universities. In 2 volumes. V. 1. Threats, vulnerabilities, attacks and approaches to defense. M.: Gorjachaja linija–Telekom, 2006. – 536 p. (in Russian).

[16] Makarenko S.I. Information weapons in the technical sphere: terminology, classification, examples. Sistemy upravlenija, svjazi i bezopasnosti [Systems of Control, Communication and Security]. 2016. no. 3. P. 292–376 (in Russian).

[17] Kondakov S.E., Meshcheryakova T.V., Skryl' S.V., Stadnik A.N., Suvorov A.A. Probabilistic representation of conditions for timely response to threats of computer attacks. Voprosy kiberbezopasnosti. M.: AO "NPO "Eshelon", 2019. no. 6. P. 59–68. DOI: http://dx.doi.org/10.21681/2311-3456-2019-6-59-68.

[18] Skryl' S. et al. Assessing the Response Timeliness to Threats as an Important Element of Cybersecurity: Theoretical Foundations and Research Model. In: Kravets A., Groumpos P., Shcherbakov M., Kultsova M. (eds) Creativity in Intelligent Technologies and Data Science. CIT&DS 2019. Communications in Computer and Information Science, vol. 1084. Springer, Cham. 2019. P. 258–269. DOI: http://dx.doi.org/10.1007/978-3-030-29750-3_20.

Поступила в редакцию – 30 ноября 2020 г. Окончательный вариант – 01 февраля 2021 г.
Received – November 30, 2020. The final version – February 01, 2021.