Григорий П. Гавдан[1], Виталий Г. Иваненко[2], Алексей А. Салкуцан[3]
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
[1]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[2]e-mail: VGIvanenko@mephi.ru, https://orcid.org/0000-0003-0823-5501
[3]e-mail: asalcutan@bk.ru, https://orcid.org/0000-0001-8282-3403

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org/10.26583/bit.2019.4.05

Аннотация. Целью статьи является рассмотрение вопросов обеспечения безопасности значимых объектов критической информационной инфраструктуры (КИИ). Актуальность соответствующих проблем обусловлена в первую очередь тем, что с каждым годом растет число кибератак на различные сферы экономики Российской Федерации и, в том числе, на значимые объекты КИИ (государственные, оборонные, нефтегазовой промышленности и др.). Ограниченность доступа в каждой сфере к общедоступной информации не позволяет сегодня аналитикам в области информационной безопасности проводить должный анализ, опираясь на имеющиеся материалы, а ресурс средств массовой информации и интернета является неполным и недоверенным. Задачи обеспечения безопасности значимых объектов КИИ в целях их устойчивого функционирования при деструктивном воздействии компьютерных атак регламентированы рядом основополагающих нормативных правовых актов. Предметом исследования являются значимые объекты КИИ, как основа стабильности и существования государства. В работе уделяется значительное внимание требованиям к структурным подразделениям обеспечения безопасности значимых объектов КИИ. Риск ущерба для субъектов КИИ от компьютерных атак на критические процессы имеет тяжелые последствия, начиная от потери репутации и до парализации работы предприятия. Приводятся требования к структурным подразделениям обеспечения безопасности значимых объектов КИИ, а также к их кадровому обеспечению.

Ключевые слова: критическая информационная инфраструктура, значимые объекты критической информационной инфраструктуры, информационные ресурсы, кибератака, киберпространство, структурные подразделения, кадровое обеспечение.

Для цитирования: ГАВДАН, Григорий П.; ИВАНЕНКО, Виталий Г.; САЛКУЦАН, Алексей А. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ. Безопасность информационных технологий, [S.l.], v. 26, n. 4, p. 69–82, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1232>. Дата доступа: 01 dec. 2019. doi:http://dx.doi.org/10.26583/bit.2019.4.05.

Grigory P. Gavdan[1], Vitaliy G. Ivanenko[2], Alexei A. Salkutsan[3]
National Nuclear Research University MEPHI,
Kashirskoe shosse, 31, Moscow, 115409, Russia
[1]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[2]e-mail: VGIvanenko@mephi.ru, https://orcid.org/0000-0003-0823-5501
[3]e-mail: asalcutan@bk.ru, https://orcid.org/0000-0001-8282-3403

Security of significant objects of critical information infrastructure

DOI: http://dx.doi.org/10.26583/bit.2019.4.05

Abstract. The issues related to the security of significant objects of critical information infrastructure are considered. The relevance of these problems is primarily due to the fact that the number of cyberattacks on various sectors of the Russian economy and primarily on significant objects of critical information infrastructure (state, defense, oil and gas industry, etc.) is increasing. Unfortunately, the limited access to the available information in this area does not allow today the researchers in the field of information security to conduct a proper analysis. In addition the corresponding media and Internet resources are incomplete.

The tasks of ensuring the security of significant objects of critical information infrastructure in order to ensure their sustainable functioning under the destructive impact of computer attacks are regulated by a number of fundamental normative legal acts, primarily the Federal law No. 187-FZ "on security of critical information infrastructure of the Russian Federation" (2017) and the Doctrine of information security of the Russian Federation (2016). Currently at the stage of formation of the digital economy the creation of national information resources and the protection of significant objects of critical information infrastructure is one of the major sources of economic, political, social and military power of the state, the basis of socio-economic and socio-political development of the Russian Federation. The subject of the study is significant objects of critical information infrastructure as the basis of stability and existence of the state, the Russian Federation. The work pays considerable attention to the requirements for structural units to ensure the security of significant objects of critical information infrastructure. Thus, the risk of computer attacks for the subjects of critical information infrastructure has serious consequences, ranging from damage to the reputation and to the paralyzation of enterprise with the subsequent disruption of defense orders for the army and Navy. The requirements to structural units of security of significant objects of critical information infrastructure as well as to their staffing are considered.
Keywords: critical information infrastructure, significant objects of critical information infrastructure, information resources, cyberattack, cyberspace, structural units, staffing.
For citation: GAVDAN, Grigory P.; IVANENKO, Vitaliy G.; SALKUTSAN, Alexei A. Security of significant objects of critical information infrastructure. IT Security (Russia), [S.l.], v. 26, n. 4, p. 69–82, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1232>. Date accessed: 01 dec. 2019. doi:http://dx.doi.org/10.26583/bit.2019.4.05.

Введение

Задачи обеспечения защиты значимых объектов критической информационной инфраструктуры (КИИ), в целях её устойчивого функционирования и регулирования отношений в области обеспечения безопасности КИИ регламентированы такими основополагающими документами, как Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (2017), Доктрина информационной безопасности Российской Федерации (2016 г.), Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы (2017 г.). В настоящее время на этапе формирования цифровой экономики (Программа «Цифровая экономика Российской Федерации», 2017 г.) создание национальных информационных ресурсов и защита значимых объектов критической информационной инфраструктуры является одним из главных источников экономической, политической, общественной, военной (мощи государства), основой социально-экономического и общественно-политического развития Российской Федерации.

Вступивший в силу с 1 января 2018 года Федеральный закон от №187-ФЗ еще с самого выхода в свет вызвал множество дискуссий со стороны субъектов КИИ[1], в то же время в периодической научной и технической литературе вопросы обеспечения безопасности значимых объектов КИИ пока не получили должного освещения. Настоящая статья в некоторой степени восполняет этот пробел.

1. Преступные деяния в сфере киберпространства

На сегодняшний день многие организации РФ и в первую очередь ФСТЭК России активно участвуют в разработке и внесении изменений в подзаконные акты в сфере обеспечения безопасности КИИ для того, чтобы обеспечить различными мерами

[1]ТБ Форум 2019: завершился крупнейший съезд руководителей по безопасности // BIS JOURNAL. URL: https://ib-bank.ru/bisjournal/news/10743 (дата обращения: 20.09.2019).

безопасность значимых объектов КИИ (ЗО КИИ) на территории РФ[2][3][4][5][6]. Во многих странах мира в сфере киберпространства[7] продолжает наблюдаться рост числа различного уровня и масштаба преступных деяния. Значимые объекты критической информационной инфраструктуры не являются исключением и при возникновении кого-либо рода конфликтов могут стать целью для атакующей стороны в информационном пространстве. В данных преступлениях замечены различные хакерские группы (группировки), которые получают финансовую (спонсорскую) поддержку от структур разного уровня (государственных, корпораций и сообществ разного уровня, коммерческих организаций, криминальных структур и др.) на ведение незаконной деятельности. Для совершения этих кибератак, они в своем арсенале используют специальное наступательное кибернетическое оружие, которое предоставляет им уникальные возможности по созданию деструктивного эффекта по нанесению максимального экономического ущерба субъекту атаки [1]. Как отмечают авторы Ахромеева Т.С., Малинецкий Г.Г. и Посашков С.А. статьи «Стратегии и риски цифровой реальности»: «Кибервойна уже началась. Всё чаще хакеры проникают в сети и инфраструктуру, припасают на будущее «черные ходы» и логические бомбы, и делают это уже сейчас, в мирное время» [2]. Так автор Мехтиева Н.Р. в статье «Информационные войны как «цифровой» аспект глобализации» пишет: «Субъектами противостояния в кибервойне оказываются как отдельные государства, целенаправленно стремящиеся избежать военного столкновения путем перевода противоборства в информационную плоскость, так и анонимные интернет-сообщества, проводящие хакерские атаки против различных государств, их политических, экономических или информационных институтов» [3].

В последнее время немалый шум в средствах массовой информации (СМИ) вызывают деятельность хакерских группировок, которые своими действиями наводят страх на крупные промышленные компании, финансовые организаций, государственные

[2]Приказ ФСТЭК России от 27.03.2019 №64 «О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. №235» // URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/288-prikazy/1882-prikaz-fstek-rossii-ot-27-marta-2019-g-n-64 (дата обращения: 20.09.2019).

[3]Приказ ФСТЭК России №59 от 21.03.2019 «О внесении изменений в форму направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденную приказом ФСТЭК №236 от 22.12.2017» // URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/288-prikazy/1864-prikaz-fstek-rossii-ot-21-marta-2019-g-n-59 (дата обращения: 20.09.2019).

[4]Приказ ФСТЭК России №60 от 26.03.2019 «О внесении изменений в Требования по обеспечению безопасности значимых объектов КИИ РФ, утвержденные приказом ФСТЭК №239 от 25.12.2017» // URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/288-prikazy/1865-prikaz-fstek-rossii-ot-26-marta-2019-g-n-60 (дата обращения: 20.09.2019).

[5]Федеральный закон от 26.07.2017 №193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» // URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/285-zakony/1705-federalnyj-zakon-ot-26-iyulya-2017-g-n-193-fz (дата обращения: 20.09.2019).

[6]Постановление Правительства Российской Федерации от 13 апреля 2019 г. №452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. №127» // URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/287-postanovleniya/1863-postanovlenie-pravitelstva-rossijskoj-federatsii-ot-13-aprelya-2019-g-n-452 (дата обращения: 20.09.2019).

[7]Group-IB представила отчет о киберпреступности и призвала рынок к хантингу // Group-IB. URL: https://www.group-ib.ru/media/hi-tech-crime-trends-2018/ (дата обращения: 20.09.2019).

ведомства и даже компании, которые работаю в сфере информационных технологий (ИТ) [4]. Примером может служить, группировка Cloud Atlas[8], которая занималась кибершпионскими операциями, где главными целями хакеров были компании промышленной отрасли и правительственные организации. Так, с начала 2019 года действия данной группировки были сосредоточенны на Россию, Центральную Азию и некоторые регионы Украины (использование фишинговых спам рассылок и др.).

Особое место в арсенале таких хакеров занимают различного рода программы вирусы, которые попадая в информационную систему (ИС), автоматизированную систему управления технологическими процессами (АСУ ТП), либо информационно-телекоммуникационную сеть (ИТКС) способны нанести, и наносят им значительный финансово-экономический ущерб.

В качестве примера на рис. 1 представлены АСУ ТП с различной степенью уязвимости на предприятиях Российской Федерации, которые являются субъектами критической информационной инфраструктуры [5].

В основном критические уязвимости в АСУ ТП были найдены в продуктах таких компаний как: Siemens (TIM 1531 IRCModules, SINUMERIKControllers), RockwellAutomation (RSLinxClassic), Circontrol (CirCarLife), NUUO (NVRmini2 andNVRsolo), SchneiderElectric (U.motionBuilder), Emerson (AMSDeviceManager) и Martem (TELEM-GW6/GWM) и др. [5].

Высокая степень автоматизации управления и глобализации ИС через ИТКС общего пользования способствовала созданию глобального информационного общества и нового поля битвы в виде киберплацдарма[9], что ставит в свою очередь значимые объекты критической информационной инфраструктуры под прицел не только от хакеров, но и от государственных кибервойск, обладающих огромными возможностями и ресурсами[10].

Так, например, в Соединённых Штатах Америки в 2009 году было создано кибер-командование США (USCYBERCOM), которое подчиняется стратегическому командованию США. В него включено 133 подразделений Силы Кибермисии (Cyber Mission Force) [6]. Данное командование рассматривает и использует интернет как виртуальный театр для ведения боевых действий, тем самым приобретает и выполняет оттачивание методов кибератак на ЗО КИИ для решения своих политических, экономических и даже военных задач[11].

Так авторы Шнепс-Шнеппе М.А., Сухомлин В.А., Намиот Д.Е. в статье «О сложностях киберзащиты информационных систем» пишут, что: «Основная задача Киберкомандования Пентагона состоит в обеспечении кибербезопасности Единой информационной среды (ЕИС), и в этом ключевую роль играют региональные стеки безопасности (Joint Regional Security Stacks, JRSS). Оборудование JRSS, по сути, представляют собой IP-маршрутизаторы со сложным комплексом программ киберзащиты» [7].

Укрепляя свою киберзащиту, США совместно со странами участниками Североатлантического альянса (далее НАТО) проводят киберучения по оттачиванию и приобретению навыков ведения кибервойн. Так в апреле 2019 г. в Таллине прошли киберучения Locked Shields 2019 («Сомкнутые щиты 2019»), которые стали крупнейшими

[8]Кибершпионская группа Cloud Atlas расширила свой арсенал полиморфной малварью // Хакер. URL: https://xakep.ru/2019/08/13/cloud-atlas-vbshower/ (дата обращения: 22.09.2019).

[9]Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем. – М.: Издательство «КДУ», 2012. – 489 с.

[10]Кибервойска Европы и НАТО // РСМД URL: https://russiancouncil.ru/analytics-and-comments/analytics/kibervoyska-evropy-i-nato/ (дата обращения: 20.09.2019).

[11]Пентагон тайно нанес ответный удар по иранским кибершпионам, нацеленным на американские корабли // YAHOO. URL: https://news.yahoo.com/pentagon-secretly-struck-back-against-iranian-cyber-spies-targeting-us-ships-234520824.html (дата обращения: 24.09.2019).

учениями НАТО в области киберзащиты, где участники совершенствовали навыки по отражению компьютерных атак на ЗО КИИ[12].

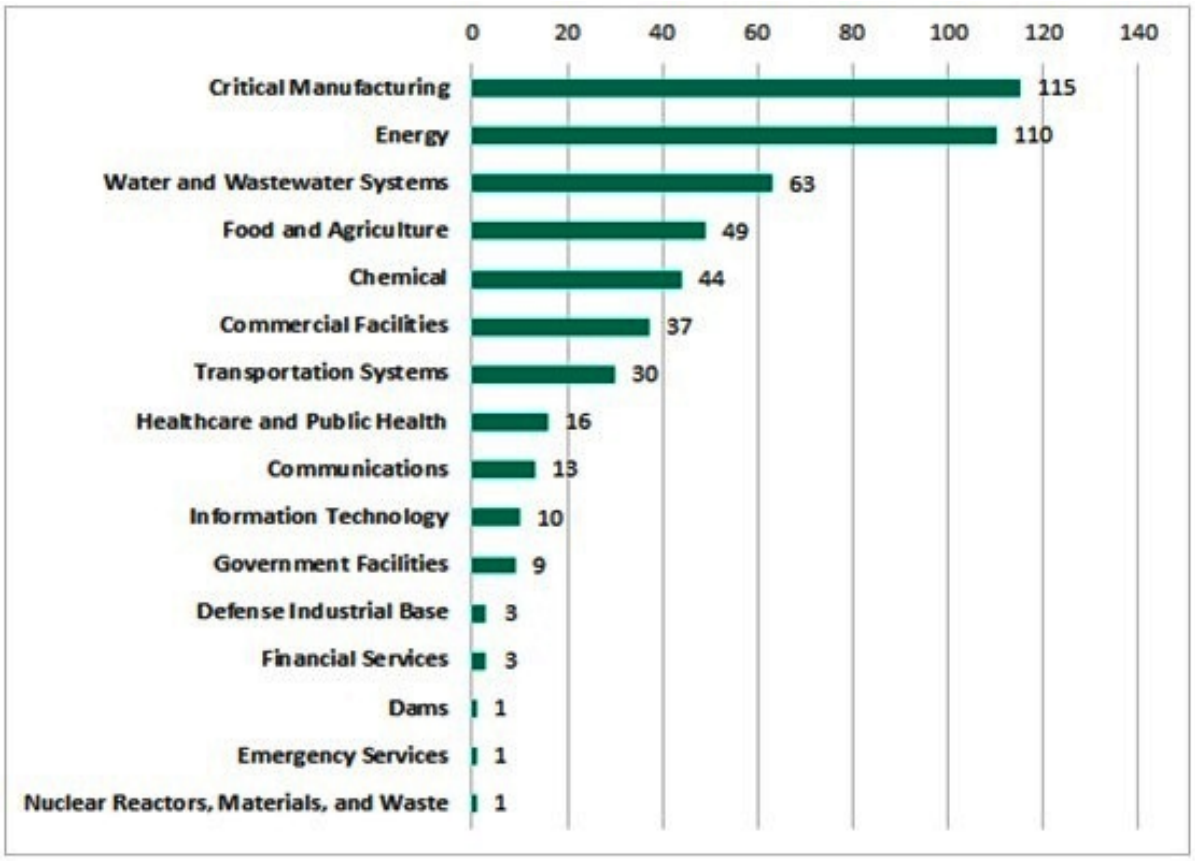

Рис. 1. Количество уязвимых АСУ ТП, используемых в различных отраслях РФ, в 2018 году [5]
(Fig. 1. Number of vulnerable automatic process control systems used in various industry branches in Russia 2018 [5]*)*

Бесспорно, стремительный подъем и развитие информационных технологий в странах запада основывается на финансировании научно-исследовательских проектов различного вида и рода направлений. Так, например, в США сосредоточены ведущие научно-технические кластеры мира. В 2017 г. финансирование научных разработок в гражданской и военной сфере достигли $152,3 млрд., что на 4,2% больше, чем в 2016 г. и на 10,1%, чем в 2015 г. [8]. На рис. 2 представлены поступления от экспорта технологий и выплаты по импорту технологий за 2017 год [9]. Благодаря развитию и внедрению научных разработок США продают значительный объем ИТ за рубеж, тем самым, оставаясь абсолютным лидером в информационной сфере [10].

2. Формирование защиты от кибероружия

В настоящее время уже не секрет что кибероружие является одним из элементов гибридной войны (свержение не угодных правительств, в сочетании с операциями спецслужб, диверсиями, поддержкой оппозиции и др.). Поэтому защита ЗО КИИ для Российской Федерации, как и для любого другого государства, является на сегодняшний

[12]Киберучение Locked Shields 2019 // ИнВоен Info. URL: https://invoen.ru/sily-obespecheniya/kiberutshenija-locked-shields-2019/ (дата обращения: 22.09.2019).

день важнейшей приоритетной задачей страны в эпоху информационного противоборства[13].

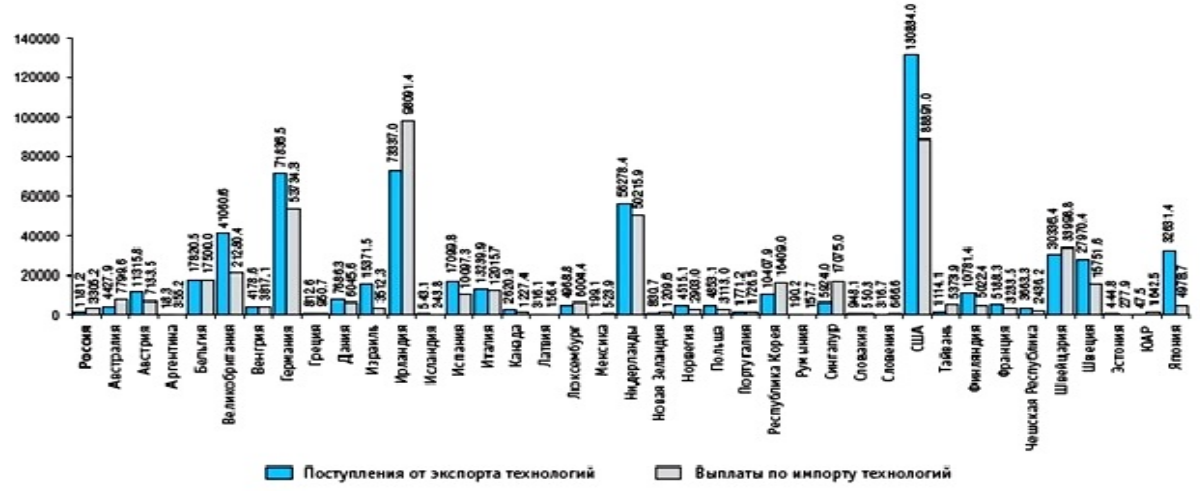

Рис. 2. Поступления от экспорта технологий и выплаты по импорту технологий за 2017 год в млн. долл. [9]
(Fig. 2. Technology export revenues and technology import payments for 2017 in millions of dollars [9]*)*

Так авторы Захарченко Р.И. и Королев И.Д. статьи «Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве» пишут: «Функционирование объектов критической информационной инфраструктуры в новой среде – киберпространстве, порождает новые уязвимости и угрозы, и требует разработки нового инструментария обеспечения устойчивости функционирование в условиях компьютерных атак» [11]. Действительно с каждым годом во всем мире количество и «качество» кибератак на ЗО КИИ постоянно растет. Многие компании, понимая наличие угроз, не могут ещё правильно организовать и адекватно противодействовать их реализации[14].

Так авторы Оюн Ч.О. и Попантонопуло Е.В. в статье «Объекты критической информационной инфраструктуры» пишут: «В настоящий момент крупные компании и государственные структуры подсчитывают потенциальные убытки, которые могут возникнуть, если они не будут готовыми к внезапному вторжению в систему» [12].

Большинство компаний сегодня действительно не уделяют должного внимания к данной проблеме и не пытаются организовывать защиту своих информационных ресурсов. Наоборот, из экономической выгоды продолжают не выделять денежные ресурсы, или снижать статьи расходов на организацию и внедрение средств защиты информации (СЗИ), тем самым, не обеспечивают защиту свои информационных ресурсов.

Понимая уровень возрастающих угроз от непринятия мер по защите ЗО КИИ, оказывающих существенное влияние на безопасность государства, по поручению Совета Безопасности, Федеральной службы безопасности с участием Федеральной службы по техническому и экспертному контролю и иных заинтересованных федеральных органов исполнительной власти разрабатываются и корректируются пакеты нормативно-правовых

[13]«Операции в киберпространстве»: в армии США заявили о стремлении к информационному доминированию // Russia Today (RT). URL: https://russian.rt.com/world/article/661526-ssha-armiya-informacionnaya-voina-komandovanie (дата обращения: 22.09.2019).
[14] Мурашов Н.Н. Компьютерные атаки на информационные ресурсы Российской Федерации: факты и цифры // Журнал "Information SecurИТ / Информационная безопасность". – 2018. – №6. – С. 6-7.

документов, призванных защитить ЗО КИИ. Между ведомствами разделены зоны ответственности для выполнения в короткие сроки поставленных специфических задач. Данные задачи определены в Федеральном законе от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Для выполнения ФЗ и подзаконных актов на постоянной основе организуются различные конференции, форумы и встречи с субъектами КИИ.

Так, например, в 2019 году были проведены следующие наиболее значимые встречи, которые были организованы крупными компаниями отраслей (в т.ч. например, антивирусными)[15]:

Инфофорум Крым – 2019 г. Ялта;

Дни кибербезопасности – 2019 г., Москва;

IT Security Day – 2019 г. Москва;

ИнфоБЕРЕГ – 2019 г. Ялта;

Информационная безопасность стратегически важных объектов регионов РФ – 2019 г. Санкт-Петербург;

Безопасность критической информационной инфраструктуры предприятий и учреждений ВПК России – 2019 г. Москва;

Саммит субъектов КИИ-1. Практикум – 2019 г. Москва;

SOC – Форум – 2019 г. Москва и др.

Формат и целевая аудитория данных встреч: межведомственная сессия представителей контролирующих органов, руководителей служб физической и информационной безопасности предприятий, представители регуляторов, федеральных и региональных органов власти, а также известные эксперты, крупные российские производители и интеграторы безопасных информационных решений и др. Так, например, на SOC – Форум 2018 ФСТЭК и ФСБ России были проведены активные дискуссии по обсуждению вопросов с субъектами КИИ, а именно [13]:

практика реализации требований законодательства о безопасности КИИ и построения центров мониторинга и управления инцидентами информационной безопасности (ФСТЭК России);

практика выполнения категорирования объектов КИИ субъектам КИИ (ФСТЭК России)[16];

задачи и функции субъекта центров Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и организации взаимодействия в сфере выявления и анализа компьютерных инцидентов (Национальный координационный центр по компьютерным инцидентам (НКЦКИ))[17];

практика применения нормативных правовых документов ФСБ России (НКЦКИ)[18];

технические аспекты взаимодействия с НКЦКИ (НКЦКИ)[19].

---

[15]Гохберг М., Дитковский К.А., Дьяченко Е.Л. и др. Поступления от экспорта технологий и выплаты по импорту технологий: 2017 // Индикатор наука. Статистический сборник 2019 // Национальный исследовательский университет «Высшая школа экономики». – 2019. – № ISBN 978-5-7598-1948-6. – 320 с. // URL: https://www.hse.ru/data/2019/05/07/1502498137/in2019.pdf (дата обращения: 25.09.2019).

[16]Торбенко Е.Б.//Практика категорирования объектов КИИ // SOC-Forum 2018. URL: https://soc-forum-2018.ib-bank.ru/files/files/SOC%202018/05_Torbenko.pdf (дата обращения: 21.09.2019).

[17]Новиков А.//О целях и задачах субъектов ГосСОПКА // SOC-Forum 2018. URL: https://soc-forum-2018.ib-bank.ru/files/files/SOC%202018/06_Novikov.pdf (дата обращения: 21.09.2019).

[18]Раевский А.//Практика применения нормативных правовых документов ФСБ России // SOC-Forum 2018. URL: https://soc-forum-2018.ib-bank.ru/files/files/SOC%202018/07_Rayevsky.pdf (дата обращения: 21.09.2019).

[19]Грачев А.//Технические аспекты взаимодействия с НКЦКИ // SOC-Forum 2018. URL: https://soc-forum-2018.ib-bank.ru/files/files/SOC%202018/08_Grachev.pdf (дата обращения: 21.09.2019).

Помимо активного участия в мероприятиях направленных на обсуждение вопросов касающейся ЗО КИИ ФСТЭК России проводит разработку подзаконных актов, методик и руководств, которые призваны, поднять задачу обеспечения безопасности ЗО КИИ на качественно новый уровень.

Рост внимания к ЗО КИИ на фоне роста киберугроз актуален, так как он влияет почти на всех субъектов КИИ, имеющих ЗО КИИ в РФ. Основным руководством, для всех стал Федеральный закон №187 «О безопасности критической информационной инфраструктуры».

В соответствии с пунктом 4 части 3 статьи 6 ФЗ №187 ФСТЭК России был утвержден приказ №235 от 21 декабря 2017 г., где субъектом КИИ создается система безопасности ЗО КИИ, которая должна быть направлена на обеспечение устойчивого функционирования всех значимых объектов, как в головных, так и в обособленных подразделениях (филиалах, представительствах и др.) с учетом внесенных изменений приказом ФСТЭК России №59 от 27 марта 2019 г.[20].

3. Требования к подразделениям, обеспечивающим безопасность значимых объектов критической информационной инфраструктуры

В данном разделе предлагаются фрагменты рекомендательной методики формирования требований к структурным подразделениям необходимой для практического использования руководителями структурных подразделений ответственных за обеспечение безопасности ЗО КИИ. Методика формирования требований к структурным подразделениям по безопасности ЗО КИИ включает основные пункты:

- решение о создании структурных подразделений ответственных за обеспечение безопасности ЗО КИИ;
- вид организационной схемы структурных подразделений ответственных за обеспечение безопасности ЗО КИИ;
- штатная численность персонала в структурных подразделениях ответственных за обеспечение безопасности ЗО КИИ;
- цели и задачи структурных подразделений, ответственных за обеспечение безопасности ЗО КИИ;
- функции структурных подразделений ответственных за обеспечение безопасности ЗО КИИ;
- функции начальников структурных подразделениях ответственных за обеспечение безопасности ЗО КИИ;
- квалификационные требования руководителей и работников структурных подразделений, ответственных за обеспечение безопасности ЗО КИИ и к организациям, выполняющим отдельные функции по обеспечению безопасности ЗО КИИ;
- механизм взаимодействия между структурными подразделениями по обеспечению безопасности ЗО КИИ, а также с уполномоченным органом ГосСОПКА и др.

За основу методики была принята образовательная инициатива NICE, которая представляет собой сотрудничество правительства, научных кругов и частного сектора экономики, возглавляемое Национальным институтом стандартов и технологий Министерства торговли США [14, 15].

[20]Приказ ФСТЭК России от 21 декабря 2017 г. №235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры российской федерации и обеспечению их функционирования» // URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/288-prikazy/1606-prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235 (дата обращения: 20.09.2019).

Использование данной методики субъектами КИИ позволяет получить достаточно большой эффект, например, в становлении структурных подразделений (с её помощью можно определить кадровый состав и смежных подразделений в составе структурных подразделений). В данном стандарте подробно описаны подразделения, ответственные за информационное противодействие, а именно занимающиеся сбором разведданных и проведение кибероперациий. В табл. 1 приведен пример должности специалиста по анализу системы отражения/парирования кибератак/киберугроз [14, 15].

Формирование структурных подразделений субъектом КИИ в сегодняшней непростой политической обстановке должно уделяться пристальное внимание. Наличие структурных подразделений, которые владеют основами ведения разведки в киберпространстве и умеют правильно отражать целевые атаки будет важным преимуществом как для субъектов КИИ, так и для государства.

Сотрудники данных подразделений, обладающие интеллектуальным потенциалом в области защиты ЗО КИИ, смогут обеспечить необходимую безопасность и «процветание» государства, так как они будут способны правильно использовать информационное оружие XXI века (рис. 3)[21].

Таблица 1. Пример должности специалиста по анализу системы отражения/парирования кибератак/киберугроз

Специальность/ специализация	**Описание специальности/ специализации**	**Наименование функциональной должности**	**Описание функциональной должности**
Анализ подсистемы отражения/ парирования кибератак (CDA)	Использование защитных мер и данных, добытых из различных источников для идентификации, анализа и подготовки отчёта о событиях, которые произошли или могут произойти в рамках сети, с целью защиты информации, информационных систем и сетей от возможных угроз.	Специалист по анализу системы отражения/ парирования кибератак/киберугроз	Использование данных, добытых от различных средств обеспечения кибербезопасности (например, системы оповещения в комплексах обнаружения вторжений, сетевые экраны, журналы регистрации сетевого трафика) с целью анализа событий, которые происходят в соответствующих областях обеспечения кибербезопасности, что, в свою очередь, необходимо для уменьшения негативных последствий от реализации угроз.

Помимо создания подразделений, которые будут заниматься обеспечением защиты от кибератак (кибервойны), имеется необходимость создания трех уровневой системы подразделений с подробно описанными функциями и участком работы в соответствии с приказом ФСТЭК России от 21 декабря 2017 г. №235.

Рассмотрим данные уровни.

Первый уровень состоит из структурных подразделений по безопасности, штатные работники которых должны:

- создавать, анализировать надёжность новых или существующих прикладных компьютерных систем;
- совершенствовать применение информационных технологий и требований к ним, которые определяют основную и целевую архитектуры;
- проводить исследования программного обеспечения с целью выявления новых

[21]Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем. – М.: Издательство «КДУ», 2012. – 485 с.

характеристик и потенциальных уязвимостей;

- тестировать и оценивать состояние ЗО КИИ;
- организовывать проведение оценки соответствия ЗО КИИ требованиям по безопасности и т.д.

Рис. 3. Структурная модель понятия «информационное оружие»
(Fig. 3. Structural model of the concept of "information weapons")

Второй уровень состоит из структурных подразделений по безопасности, штатные работники, которые ответственны за эксплуатацию и функционирование (сопровождение, обслуживание, ремонт) объектов безопасности ЗО КИИ, должны уметь:

- совершенствовать, настраивать и обслуживать компоненты системы;
- проектировать и внедрять пользовательские алгоритмы, бизнес-процессы и схемы сложных и масштабируемых в пределах организации наборов данных, которые используются при моделировании, интеллектуальном анализе данных и в исследовательских целях;
- обеспечивать реализацию организационных мер и применение СЗИ, эксплуатацию СЗИ;
- готовить предложения по совершенствованию функционирования службы безопасности, а также по повышению уровня безопасности ЗО КИИ и др.

Третий уровень состоит из подразделений, которые выполняют отдельные функции по обеспечению безопасности ЗО КИИ. Их сотрудники должны:

- знать организационно-распорядительную документацию организации по безопасности ЗО КИИ;
- знать инструкцию по обеспечению информационной безопасности на ЗО КИИ для работников сторонних организаций, выполняющим отдельные функции по обеспечению безопасности ЗО КИИ;

- предоставлять круглосуточную техническую поддержку СЗИ субъекту КИИ и др.

Структурные подразделения возглавляют начальники отделов, которые назначаются и освобождаются приказом руководителя субъекта КИИ. Должностные обязанности, права и ответственность начальников отделов определены в должностных инструкциях. Начальники отделов решают следующие задачи:

- осуществление руководства работой по обеспечению информационной безопасности в подразделении;
- постоянное совершенствование систем безопасности в связи усовершенствованием методов кибератак;
- участие в обеспечении строгого выполнения требований внутренних и внешних нормативных документов в области обеспечения безопасности ЗО КИИ;
- участие в разработке решений по защите информации для вновь принимаемых в эксплуатацию в подразделении объектов информатизации и т.д.

Работники структурных подразделений должны обладать соответствующими компетенциями для выполнения своих функциональных обязанностей. В данные компетенции входят знания, практические навыки и умения в области обеспечения безопасности ЗОКИИ.

Следует отметить, что 27 марта 2019 года был утвержден приказ ФСТЭК России «О внесении изменений в требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры РФ и обеспечению их функционирования», утвержденные приказом федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. №235, который является основным для разработки методики формирования требований к структурным подразделениям обеспечения безопасности ЗО КИИ.

На основании внесённых изменений к основным требованиям, определяющим необходимую компетенцию работников структурных подразделений, следует отнести:

- наличие высшего профессионального образования в области ИБ и (или) информационных технологий;
- опыт работы в области ИБ не менее определенного периода, например, не менее трех лет;
- регулярное прохождение дополнительного (специализированного) обучения (повышения квалификации) в области ИБ;
- знание требований законодательства РФ;
- знание внутренних нормативно-методических и организационно-распорядительных документов организации в сферах, определённых ФЗ №187 в области ИБ;
- знания вопросов, которые касаются средств, систем и технологий обеспечения ИБ, а также способов и практик их применения и др.

В компаниях, где преобладает государственный или частный капитал (особенно крупный), руководство заинтересовано в повышении уровня защищенности, для чего: привлекаются отечественные специалисты по информационной безопасности и выделяются дополнительные финансовые ресурсы, направленные на закупки передовых и сертифицированных (отечественных) СЗИ, обучение персонала для работы с этими СЗИ и др. Для атак на российские информационные ресурсы, как правило, используются центры управления (под командованием кибервойск) ведущих мировых государств. Данные центры имеют разные цели и задачи, одной из которых являются кибератаки (реальное воздействие на информационные системы, телекоммуникационные сети, объекты инженерной и транспортной инфраструктуры и др., то есть атаки на ЗО КИИ) [16].

В отличие от различного рода договоров о ликвидации оружия массового поражения, кибероружие ни кем не контролируется от распространения. Как следствие, такие средства могут попасть «не в те руки» и без должного регулирования странами ООН могут возникнуть «внештатные ситуации» мирового уровня [17].

Особый вопрос – система подготовки специалистов по ИБ, которой в РФ уделяется особое внимание из-за нарастания информационных угроз [18]. Поэтому, для обеспечения безопасности ЗО КИИ необходима новая и качественная подготовка кадрового потенциала, и её сохранение [19, 20]. Система структуры трудовых ресурсов организаций (независимо от форм собственности), производящих программные и программно-аппаратные средства и комплексы защиты информации, а также предоставляющие услуги по обеспечению ИБ, должны определять контингент выпускников, наиболее приемлемый для замещения вакантных должностей и др.

Заключение

Вступивший в силу с 1 января 2018 года Федеральный закон от 26.07.2017 №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» определил направление действий по обеспечению защиты значимых объектов критической информационной инфраструктуры.

Для субъектов КИИ при формировании структурных подразделений особое внимание должно уделяется подготовке и переподготовке кадров, а также взаимодействию с образовательными учреждениями, готовящими специалистов по ИБ для конкретного направления в информационном противодействии. Некоторые примеры методики, приведенные в статье, могут быть рекомендованы, как основа организации структурных подразделений в рамках приказа ФСТЭК России №235 от 21.12.2017 года и других нормативных документов для обеспечения безопасности ЗО КИИ.

При создании системы обеспечения безопасности значимых объектов КИИ необходимо учитывать следующие обстоятельства:

- рост числа кибератак на РФ (в том числе на значимые объекты КИИ) с каждым годом продолжает увеличиваться;
- русофобские настроения среди западных стран не уменьшаются;
- обязательность подготовки и сохранения кадрового потенциала для обеспечения безопасности ЗО КИИ;
- обязательность разработки системной структуры трудовых ресурсов.

СПИСОК ЛИТЕРАТУРЫ:

1. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. №1(29). С. 2–9. DOI: 10.21681/2311-3456-2019-1-2-9. URL: http://cyberrus.com/wp-content/uploads/2019/03/02-09-129-19_1.-Romashkina.pdf (дата обращения: 20.09.2019).
2. Ахромеева Т.С., Малинецкий Г.Г., Посашков С.А. Стратегии и риски цифровой реальности // Стратегические приоритеты. 2017. № 2 (14). С. 88–102. URL: https://elibrary.ru/item.asp?id=29947604 (дата обращения: 20.09.2019).
3. Мехтиева Н.Р. Информационные войны как «цифровой» аспект глобализации // Век глобализации. 2017. №3. С. 77–89. URL: https://elibrary.ru/item.asp?id=30266882 (дата обращения: 25.09.2019).
4. Отчет компании PositiveTechnologies: Актуальные киберугрозы: II квартал 2019 года // PositiveTechnologies. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2019-Q2-rus.pdf (дата обращения: 24.09.2019).
5. Отчет компании Касперский: Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2018. // Kaspersky Lab ICS CERT. URL: https://ics-cert.kaspersky.ru/media/ICS_REPORT_H22018_FINAL_RUS.pdf (дата обращения: 20.09.2019).

6. Хлопов О.А. Перспективы создания единых кибервойск США // Colloquium-journal. 2019. № 15 (39). С. 1–3. URL: https://elibrary.ru/item.asp?id=39159017 (дата обращения: 25.09.2019).
7. Шнепс-Шнеппе М.А. Сухомлин В.А. Намиот Д.Е. О сложностях киберзащиты информационных систем // International Journal of Open Information Technologies. 2018. № 7. С. 57–65. URL: https://cyberleninka.ru/article/n/o-slozhnostyah-kiberzaschity-informatsionnyh-sistem (дата обращения: 25.09.2019).
8. Гилькова О.Н. О военных и гражданских НИОКР в США // Материалы международной научно-практической конференции Научный центр «Диспут». – Вологда: ООО «Маркер», 2018. С. 64–66. URL: https://elibrary.ru/item.asp?id=36621067 (дата обращения: 25.09.2019).
9. Гохберг М., Дитковский К.А., Дьяченко Е.Л. и др. Нац. исслед. ун-т «Высшая школа эко- И60 номики». – М.: НИУ ВШЭ, 2019. – 328 с. ISBN 978-5-7598-1948-6. URL: https://www.hse.ru/data/2019/05/07/1502498137/in2019.pdf (дата обращения: 25.09.2019).
10. Дробот Г.А. США как мировой лидер: реалии, теории, перспективы // Век глобализации. 2018. № 1. С. 83–94. URL: https://elibrary.ru/item.asp?id=32595473 (дата обращения: 25.09.2019).
11. Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве // Наукоемкие технологии в космических исследованиях Земли. 2018. Т. 10. № 2. С. 52–61. URL: https://elibrary.ru/item.asp?id=34939627 (дата обращения: 23.09.2019).
12. Оюн Ч.О., Попантонопуло Е.В. Объекты критической информационной инфраструктуры // Интерэкспо Гео-Сибирь. 2018. № 9. С. 45–49. URL: https://elibrary.ru/item.asp?id=35661002 (дата обращения: 25.09.2019).
13. Презентации SOC-Forum 2018 // SOC-Forum 2018. URL: https://soc-forum-2018.ib-bank.ru/materials (дата обращения: 21.09.2019).
14. National initiative for cybersecurity education (NICE) Cybersecurity Workforce Framework // NICCS. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf (дата обращения: 14.09.2019).
15. Мельников Дмитрий А.; Гавдан Григорий П.; Корсаков Иван А. К вопросу о цели и задачах национальной образовательной инициативы США в области кибербезопасности. Безопасность информационных технологий, [S.l.], т. 25, № 2. С. 23–37, may 2018. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1107 (дата обращения: 25.09.2019). DOI: http://dx.doi.org/10.26583/bit.2018.2.02.
16. Джаббарова К.Ф. Современные аспекты кибербезопасности в мире в контексте глобальных угроз // Азимут научных исследований: экономика и управление. 2017. № 2(19). С. 323–326. URL: https://elibrary.ru/item.asp?id=29728909 (дата обращения: 25.09.2019).
17. Марченко Анатолий В.; Войналович Валерий Ю.; Воронин Сергей Н. Анализ состояния системы подготовки специалистов в области информационной безопасности. Безопасность информационных технологий, [S.l.], т. 25, № 2. С. 6–22, may 2018. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1106 (дата обращения: 25.09.2019). DOI: http://dx.doi.org/10.26583/bit.2018.2.01.
18. Ватрушкин А.А. Правовые основы обеспечения кибербезопасности критической инфраструктуры Российской Федерации // Евразийская адвокатура. 2017. №6 (31). С. 78–84. URL: https://elibrary.ru/item.asp?id=32282456 (дата обращения: 25.09.2019).
19. Морозова О.В. Семантическая доминанта «Агрессия» в американских СМИ (на материале политических публикаций о России) // филологические науки. Вопросы теории и практики. 2017. № 12-4 (78). С. 126–130. URL: https://elibrary.ru/item.asp?id=30745191 (дата обращения: 25.09.2019).
20. Гневэк О.В., Мусийчук М.В. Образ России в условиях информационной войны конца XX – начала XXI вв. Тенденции обновления политического дискурса // Материалы международной научной конференции. – Магнитогорск: Магнитогорский государственный технический университет им. Г.И. Носова, 2017. С. 292–306. URL: https://elibrary.ru/item.asp?id=32552992 (дата обращения: 25.09.2019).

REFERENCES:

[1] Romashkina N.P. Global military-political problems of international information security: trends, threats, prospects. Questions of cybersecurity. 2019. No. 1(29). P. 2–9. DOI: 10.21681 / 2311-3456-2019-1-2-9. URL: http://cyberrus.com/wp-content/uploads/2019/03/02-09-129-19_1.-Romashkina.pdf (accessed 20.09.2019) (in Russian).
[2] Akhromeeva TS, Malinetskiy G.G., Posashkov S.A. Strategies and risks of digital reality. Strategic priorities. 2017. № 2(14). C. 88–102. URL: https://elibrary.ru/item.asp?id=29947604 (accessed: 20.09.2019) (in Russian).
[3] Mehdiyev N.R. Information wars as a “digital” aspect of globalization. The Century of Globalization. 2017. № 3. P. 77–89. URL: https://elibrary.ru/item.asp?id=30266882 (accessed: 25.09.2019) (in Russian).

[4] Positive Technologies report: Current cyber threats: Q2 2019. Positive Technol-ogies. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2019-Q2-rus.pdf (accessed: 24.09.2019) (in Russian).
[5] Kaspersky company report: Threat landscape for industrial automation systems Second half of 2018. Kaspersky Lab ICS CERT. URL: https: //ics-cert.kaspersky.ru/media/ICS_REPORT_H22018_FINAL _RUS.pdf (accessed: 20.09.2019) (in Russian).
[6] Khlopov O.A. Prospects for the creation of a unified US cyber military. Colloquium-journal. 2019. № 15 (39). P. 1–3. URL: https://elibrary.ru/item.asp?id=39159017 (accessed: 25.09.2019) (in Russian).
[7] Shneps-Shneppe M.A. Sukhomlin V.A. Namiot D.E. On the difficulties of cyber defense of information systems. International Journal of Open Information Technologies. 2018. № 7. P. 57–65. URL: https://cyberleninka.ru/article/n/o-slozhnostyah-kiberzaschity-informatsionnyh-sistem (accessed: 25.09.2019) (in Russian).
[8] Gilkova O.N. About military and civilian R&D in the USA. Materials of the international scientific-practical conference Scientific Center "Disput". – Vologda: LLC Marker, 2018. P. 64–66. URL: https://elibrary.ru/item.asp?id=36621067 (accessed: 25.09.2019) (in Russian).
[9] Gokhberg M., Ditkovsky K.A., Dyachenko E.L. et al. National Research University Higher School of Economics. – Moscow: HSE, 2019. – ISBN 978-5-7598-1948-6. – 320 P. URL: https://www.hse.ru/data/2019/05/07/1502498137/in2019.pdf (accessed: 25.09.2019) (in Russian).
[10] Drobot G.A. USA as a world leader: realities, theories, prospects. Century of globalization. 2018. № 1. P. 83–94. URL: https://elibrary.ru/item.asp?id=32595473 (accessed: 25.09.2019) (in Russian).
[11] Zakharchenko R.I., Korolev I.D. Methodology for assessing the stability of the functioning of critical information infrastructure facilities operating in cyberspace. High-tech in space research of the Earth. 2018. Vol. 10. № 2. P. 52–61. URL: https://elibrary.ru/item.asp?id=34939627 (accessed: 23.09.2019) (in Russian).
[12] Oyun H.A., Papantonopoulou E.V. Objects of critical information infrastructure. Interexpo geo-Siberia. 2018. № 9. P. 45–49. URL: https://elibrary.ru/item.asp?id=35661002 (accessed: 25.09.2019) (in Russian).
[13] Presentations of the SOC-Forum 2018. SOC-Forum 2018. URL: https://soc-forum-2018.ib-bank.ru/materials (accessed: 21.09.2019) (in Russian).
[14] National initiative for cybersecuriтy education (NICE) Workforce Framework Cybersecuriтy. NICCS. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf (accessed: 14.09.2019).
[15] Melnikov, Dmitriy A.; Gavdan, Grigory P.; Korsakov, Ivan A. To the issue about the purpose and objectives the USA National initiative for cybersecurity education. IT Security (Russia), [S.l.], v. 25, n. 2. P. 23–37, may 2018. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1107> (accessed: 21.09.2019). DOI:http://dx.doi.org/10.26583/bit.2018.2.02 (in Russian).
[16] Jabbarova K.F. Modern aspects of cybersecurity in the world in the context of global threats. Azi-Mut Scientific Research: Economics and Management. 2017. № 2 (19). P. 323–326. URL: https://elibrary.ru/item.asp?id=29728909 (accessed: 25.09.2019) (in Russian).
[17] Marchenko, Anatoly V.; Voynalovich, Valery Y.; Voronin, Sergey N. The analysis of the training system for specialists working in the field of information security. IT Security (Russia), [S.l.], v. 25, n. 2. P. 6–22, may 2018. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1106> (accessed: 25.09. 2019). DOI: http://dx.doi.org/10.26583/bit.2018.2.01 (in Russian).
[18] Vatrushkin A.A. Legal framework for ensuring cybersecurity of the critical infrastructure of the Russian Federation. Eurasian Bar. 2017. № 6 (31). P. 78–84. URL: https://elibrary.ru/item.asp?id=32282456 (accessed: 25.09.2019) (in Russian).
[19] Morozov O.V. The semantic dominant «Aggression» in the American media (based on political publications on Russia). Philological Sciences. Questions of theory and practice. 2017. № 12-4 (78). P. 126–130. URL: https://elibrary.ru/item.asp?id=30745191 (accessed: 25.09.2019) (in Russian).
[20] Gnevek O.V., Musiychuk M.V. The image of Russia in the conditions of the information war of the late XX - early XXI century. Trends in updating political discourse. Materials of an international scientific conference. - Magnitogorsk: Magnitogorsk State Technical University. G.I. Nosova, 2017. P. 292–306. URL: https://elibrary.ru/item.asp?id=32552992 (accessed: 25.09.2019).

Поступила в редакцию – 23 октября 2019 г. Окончательный вариант – 23 ноября 2019 г.
Received – October 23, 2019. The final version – November 23, 2019.