Рустем В. Пенерджи[1], Григорий П. Гавдан[2]
[1,2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: Prv0@yandex.ru, https://orcid.org/0000-0003-4105-2221
[2]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

DOI: http://dx.doi.org/10.26583/bit.2020.3.03

Аннотация. Целью статьи является рассмотрение вопросов связанных с обеспечением безопасности государственных информационных систем в Российской Федерации. Актуальность этих вопросов обусловлена в первую очередь тем, что с каждым годом в России не уменьшается число кибератак (наносящих значительный ущерб государству) на различные сферы её экономики, в том числе, на её государственные информационные системы. Несколько лет назад начала реализацию национальная инициатива в области кибербезопасности – NICE (*«The National Initiative for Cybersecurity Education»*), что не обойдено вниманием российских и других специалистов в области информационной безопасности. К основным направлениям защиты информационной собственности отнесены: охрана (государственной, служебной, коммерческой, банковской, налоговой, страхования, персональных данных и др.) тайн и интеллектуальная собственность. Государственные информационные системы (ГИС) включают информационно-технологические средства и системы, при создании которых опираются на передовые научные изыскания, такие как знания, передовые технологии (ноу-хау) и др. и являются неотъемлемой частью и достаточно сложной системы государственного управления. Предметом исследования являются ГИС, как основа управления государственных органов. В работе первоочередное внимание уделено современным тенденциям в области обеспечения защиты информации ГИС, краткому обзору законодательства в области ГИС и критической информационной инфраструктуре.
Ключевые слова: государственная информационная система, государственное управление, информационная система, информационная собственность, критическая информационная инфраструктура.
Для цитирования: ПЕНЕРДЖИ, Рустем В.; ГАВДАН, Григорий П. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ. Безопасность информационных технологий, [S.l.], v. 27, n. 3, p. 26–42, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1290>. Дата доступа: 01 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.03.

Rustem V. Penerdji[1], Grigory P. Gavdan[2]
[1,2]National Nuclear Research University MEPHI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
[1]e-mail: Prv0@yandex.ru, https://orcid.org/0000-0003-4105-2221
[2]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076

Information security of state information systems

DOI: http://dx.doi.org/10.26583/bit.2020.3.03

Abstract. The purpose of the paper is to consider issues related to the security of state information systems in the Russian Federation. The relevance of these issues is primarily due to the fact that the number of cyber-attacks (causing significant damage to the state) on various areas of its economy, including its state information systems, is increasing every year in Russia. For example, the national initiative for Cybersecurity Education (NICE) was launched in the United States several years ago. This event has not escaped the attention of Russian and other experts in the field of information security (is). The main areas of information property protection include: protection (state, official, commercial, banking, tax, insurance, personal data (PD), etc.) of secrets and intellectual property. State information systems include information technology tools and systems that rely on advanced scientific research, such as knowledge, advanced

technologies (know-how), etc. Today, state information systems are an integral part of a fairly complex system of public administration. It is also important to recall the role of the Russian FSTEC regulator in ensuring information security. The subject of the research is SIS as the basis of management of state bodies. The paper focuses on current trends in the field of SIS information security, a brief overview of SIS legislation, and the critical information infrastructure (CII) of Russia's main geopolitical opponent. The main arguments for the importance of the chosen direction of work are discussed. Further research is expected to be conducted in the field of SIS security in an uncertain environment.
Keywords: state information system, public administration, information system, information property, critical information system.
For citation: PENERDJI, Rustem V.; GAVDAN, Grigory P. Information security of state information systems. IT Security (Russia), [S.l.], v. 27, n. 3, p. 26–42, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1290>. Date accessed: 01 sep. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.3.03.

Введение

Тенденции развития мирового сообщества и происходящие в мире процессы геополитического характера действительно не являются случайными. Ведущие мировые державы (такие, например, как США, Великобритания, Евросоюз, Китай, Россия и др.) и «закулисная мировая элита», оказывают существенное влияние на их формирование. Между этими оппонентами (игроками) существует геополитическое противоборство, в том числе и информационное. От этого всем этим сторонам никуда не уйти, как бы этого всем не хотелось бы. Государственные информационные системы (ст.14)[1] создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях. ГИС являются неотъемлемой частью сложной системы управления государства, которая способна обеспечить свою бесперебойную работу и должное её функционирование.

Практически каждое ведомство или министерство Российской Федерации ведут свои реестры и собирают информацию по своему профилю в рамках обозначенной деятельности. Например, Федеральная налоговая служба автоматизировала процедуру сбора налоговой отчетности и фискальных проверок и др. в режиме он-лайн; автоматизирована процедура закупок для государственных нужд посредством ведения всеми участниками единых ИС. Системы постоянно модифицируются и обновляются. Например, Государственные (Пенсионный, социального страхования, медицинского страхования и др.) фонды также ведут свои БД и соответствующие реестры и т.д. [1].

Государственные органы (ГО), организующие должное функционирование ГИС, в свою очередь обязаны предоставить необходимый доступ к информации (обеспечить её достоверность, доступность, целостность, аутентичность, актуальность и др.) в порядке, предусмотренном законодательством РФ и обеспечить требуемую защиту (информации ограниченного доступа) от модифицирования, уничтожения, неправомерного доступа, блокирования, копирования и иных неправомерных действий [2]. ГИС и др. ИС, где компрометация информационных систем может иметь весьма тяжёлые последствия является тому подтверждением и не может не привлекать к себе внимание.

К основным направлениям защиты информационной собственности относят: охрану (государственной, служебной, коммерческой, банковской, медицинской, персональных и др.) тайн и интеллектуальную собственность. Ситуации, когда, по словам секретаря Совета безопасности Российской Федерации Патрушева Н.П., основными целями иностранных спецслужб по-прежнему остаются объекты КИИ РФ (критической информационной

[1]Федеральный Закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в редакции от 18 марта 2019 г.

инфраструктуры) [3], компрометация подобных информационных систем может иметь весьма тяжёлые последствия.

Затруднения, возникающие при обеспечении ИБ современных информационных систем, во многом связаны, с:

– задержкой внесения изменений (например, в ходе обнаружения новых факторов риска) при включении их в нормативно-правовые акты (НПА) в области обеспечения безопасности информации и отсутствием соответствия между этими НПА;

– субъективностью экспертных оценок, возникающей при формировании модели угроз безопасности ИС и увеличивающейся при этом степенью неопределённости модели угроз;

– частым обнаружением новых уязвимостей и угроз в программном и аппаратном обеспечении ИС.

В соответствии с базовым законом[1] в области информатизации, информационных технологий (ИТ) и защите информации (ЗИ), информация, содержащаяся в ГИС, а также иные имеющиеся в распоряжении ГО сведения и документы являются национальными (государственными) информационными ресурсами [2]. Например, в РФ только в органах государственной власти (ОГВ) федерального и регионального уровней накоплен значительный объем информационных фондов (ИФ), объединяющих десятки тысяч баз данных (БД) [2], которые в области их защиты также требуют к себе должного внимания.

Остановимся на государственных информационных системах. Рассмотрим современные тенденции в сфере обеспечения безопасности информации и проведем их анализ.

1. Анализ современных тенденций в сфере обеспечения безопасности информации

Существующие проблемы обеспечения информационной безопасности информационных систем в РФ (в том числе и ГИС) подтверждаются:

проводимыми исследованиями (например, минимизация рисков ИБ [4], оценка рисков на основе графов атак для систем управления ИБ [5], оценка угроз безопасности ИС персональных данных (ПД) [6], обеспечение требуемой защищенности информационно-телекоммуникационных узлов [7], многофакторная классификация угроз информационной безопасности киберфизических систем [8]);

выступлениями (видеоконференции, конференции, форумы и т.д.) представителей государственных и коммерческих организаций (структур), работающих в области защиты информации и ИБ.

Программой «Цифровая экономика РФ»[2] предусматривается развитие не только в рамках совершенствования ИТ, но и в более широком смысле.

Развитие цифровой экономики охватывает восемь ключевых направлений [2], следуя логике Давосского проекта. Поэтому в настоящее время требуется не только внимание к «цифровизации общества», но и к принятию на уровне государства должных мер защиты.

1.1 Техническая проблематика

Различные отчёты отечественных и зарубежных компаний, связанные с вопросами ЗИ (ГИС, промышленные ИС и др.), подтверждают тот факт то, что за последнее время не снижается уровень компьютерных инцидентов.

Представленная на рис. 1 диаграмма распределения числа утечек по отраслям в 2017 году [9] показывает, что третье – четвертое места занимают силовые структуры и

[2]Программа «Цифровая экономика Российской Федерации», утверждена Распоряжением Правительства РФ от 28 июля 2017 г. № 1632-р.

государственные органы.

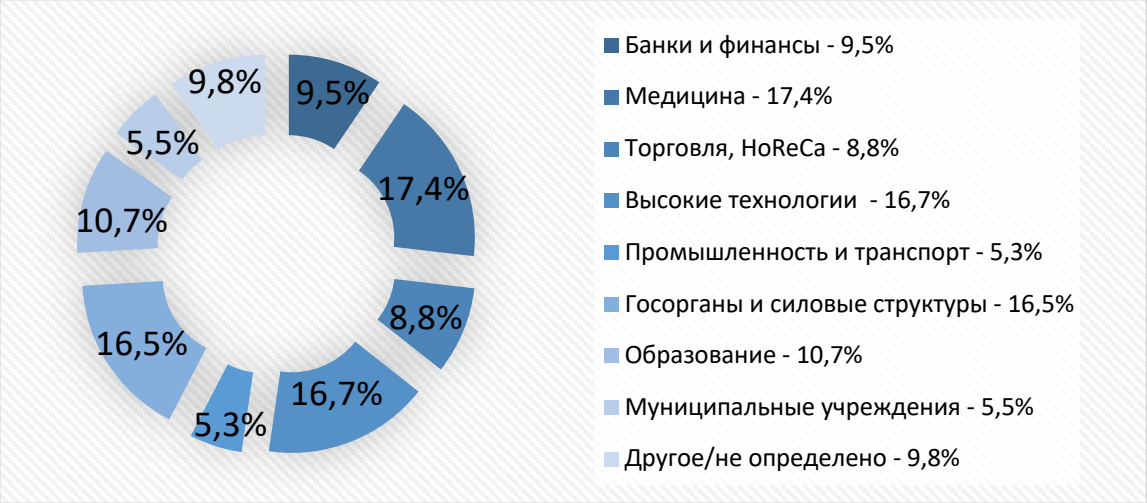

Рис. 1. Распределение числа утечек по отраслям, 2017 г.
(Fig. 1. Distribution of the number of leaks by industry, 2017)

Аналогичный отчёт за 2018 год для ГИС показывает также третье-четвертое место [10]. Диаграмма распределения числа утечек по отраслям в 2018 году [10] представлена на рис. 2.

Прогнозы по видоизменению угроз также предполагают увеличение компьютерных инцидентов с ИС. Так, например, по данным [11] основными проблемами в 2019 году были:

1) увеличение атак на промышленные ИС – за счет увеличения доступных к воздействию элементов;

2) возрастание интереса как киберпреступников, так и кибервойск;

3) недооценка общего уровня угроз: проблемы ИБ, как правило, не на слуху у широкой публики. У сотрудников же самих компаний господствует вера в непогрешимость систем аварийной защиты;

4) непонимание специфики угроз безопасности, характерных для промышленных систем и др. Этот факт подтверждается в [12].

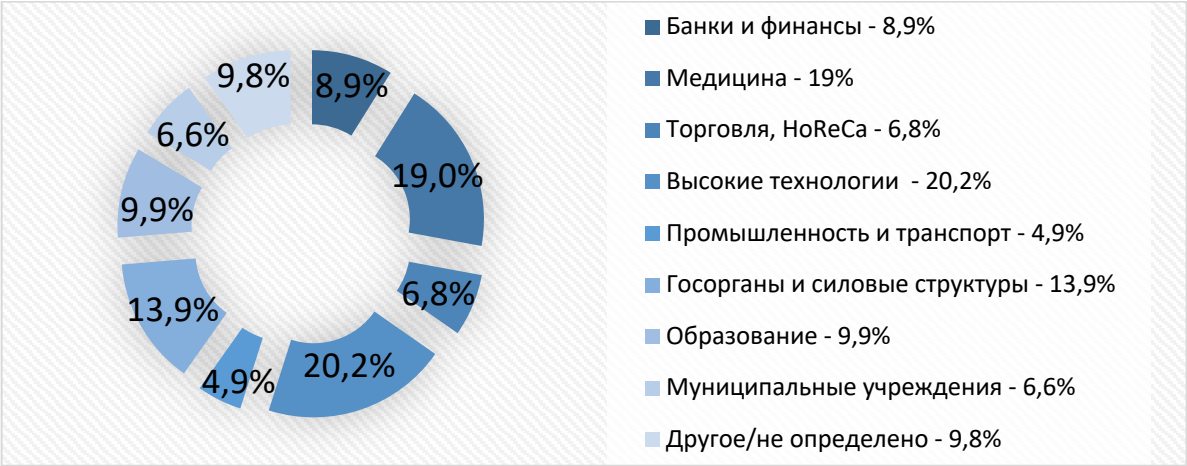

Рис. 2. Распределение числа утечек по отраслям, 2018 г.
(Fig. 2. Distribution of the number of leaks by industry, 2018)

Наиболее важными выводами являются:

1) непрекращающаяся тенденция увеличения числа уязвимостей в компонентах автоматизированных систем управления технологическими процессами (АСУ ТП) [12] (Рис. 3);

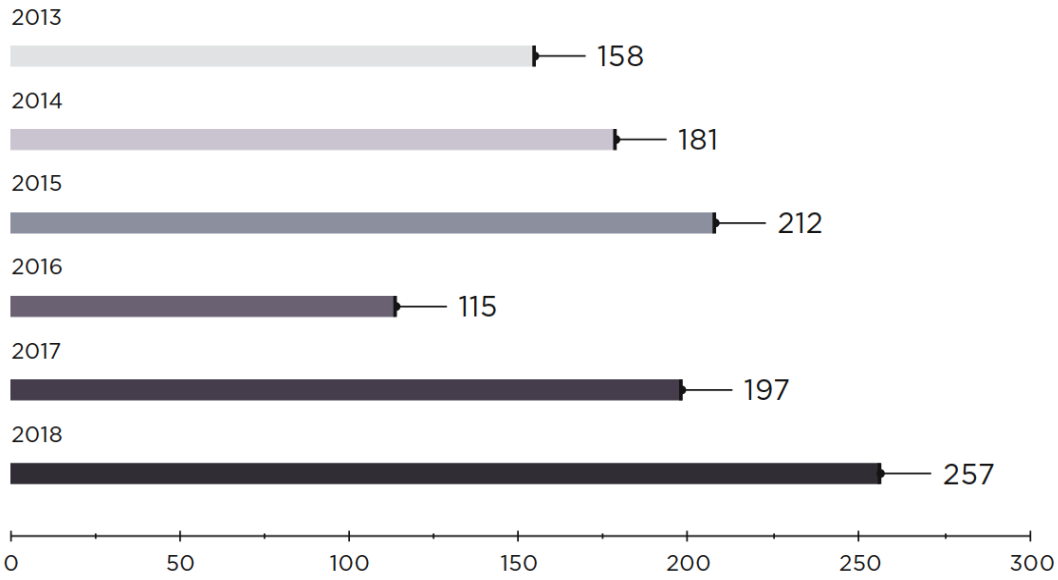

Рис. 3. Статистика обнаружения уязвимостей в компонентах АСУ ТП
(Fig. 3. The statistics of vulnerabilities in the components of the ACS of TP)

2) значительная доля уязвимостей критической и высокой степеней риска. Число уязвимостей, относящихся, в соответствии с оценкой стандарта Common Vulnerability Scoring System версии 3, к критическим и высоким степеням риска составили по итогам 2018 года, соответственно, 25% и 53% от общего числа обнаруженных уязвимостей. Соответствующая диаграмма степени риска обнаруженных уязвимостей приведена на рис. 4 [12].

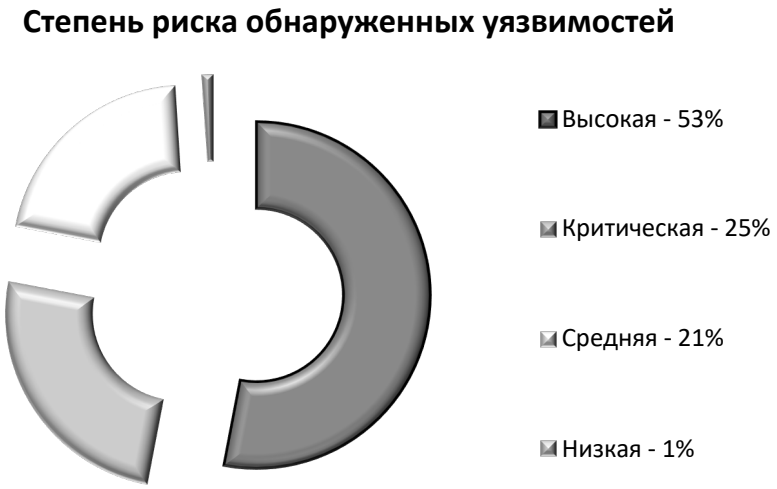

Рис. 4. Степени риска обнаруженных уязвимостей
(Fig. 4. Risk levels of detected vulnerabilities

1.2 Геополитическая составляющая

Важной тенденцией в ЗИ является милитаризация киберпространства. Весьма существенным подтверждением данного факта является то, что в настоящее время официально признано существование кибервойск двадцатью странами мира [14].

В Российской Федерации (РФ) об этом объявлено в 2013 году. В табл.1 приведены сводные данные по странам, имеющим кибервойска и оцениваемым их потенциалом, определяющимся из уровня их финансирования и ориентировочной численности [14].

В табл. 1 представлены 19 стран. Согласно этих же источников, 20-й страной является Россия. Так, специалисты компании Zecurion Analytics [15], входящей в крупную отечественную IT-компанию Zecurion, заявляют, что Россия может входить в ТОП-5 государств, обладающих развитыми кибервойсками. Подавляющее число стран, указанных в табл. 1 либо не имеют дружеских отношений с РФ, либо входят в военно-политические блоки, противостоящие РФ.

Помимо развития кибервойск, в мире уделяется внимание уровню образования широких кругов населения в области защиты информации. Например, в США несколько лет назад начала реализовываться национальная инициатива в области кибербезопасности – NICE (*«The National Initiative for Cybersecurity Education»*) [16].

По результатам исследования, приведенным в [17], национальная инициатива «ориентирована на рост общего числа работников, подготовленных для защиты национальных интересов от существующих и будущих угроз».

2. Обзор законодательства по ГИС и критической информационной инфраструктуре основного геополитического оппонента

Основным геополитическим противником РФ являются Соединённые Штаты Америки. Содержание актуальной редакции (2017 года) Стратегии Национальной Безопасности США [18]: «Китай и Россия бросают вызов американской власти, влиянию и интересам, пытаясь подорвать американскую безопасность и процветание» является тому подтверждением. В том же источнике Россия обвиняется в проведении информационных атак против т.н. «свободного мира»: «Россия использует информационные операции как часть своих (наступательных) киберусилий по влиянию на общественное мнение по всему миру. Её кампании влияния сочетают тайные разведывательные операции и ложные онлайн-персонажи с государственными средствами массовой информации, сторонними посредниками и платными пользователями социальных сетей или «троллями» [18].

Современные отрасли экономики активно внедряют новейшие цифровые решения с помощью различных объектов информационной инфраструктуры, таких например как: ИС, АСУ ТП и ИТС с целью повышения их конкурентоспособности и модернизации, с целью ускорения своего инновационного развития [19].

Согласно отчету Kaspersky ICS-CERT, в мире количество компьютерных атак с попытками внедрения вредоносных объектов на компьютеры АСУ в первом полугодии 2019 г. по сравнению с первым полугодием 2018 г. выросли незначительно, однако все равно находятся на высоких отметках.

Следует отметить о важности в РФ организации подготовки и проведения регулярных учений по киберзащите (КЗ), так же как это, например, организовано у наших оппонентов. Учения по киберзащите в настоящее время играют достаточно важную роль: в подготовке специалистов, например, разработка и внедрение систем оценки доступности для учений по киберзащите [20] в области ЗИ наравне с подготовкой кадров страны. Практическая работа и выполнение специальных упражнений повысит квалификацию, готовность и осведомленность, как специалистов, так и экспертов.

Таблица 1. Потенциал кибервойск стран мира

№	Страна	Финансирование, млн. $, в год	Число военнослужащих
1	США	7000	9000
2	Китай	1500	20000
3	Великобритания	450	2000
4	Германия	250	1000
5	Северная Корея	200	4000
6	Франция	220	800
7	Южная Корея	400	700
8	Израиль	150	1000
9	Польша	50	400
10	Япония	250	500
11	Австралия	125	300
12	Эстония	7	100
13	Иран	25	250
14	Италия	70	250
15	Нидерланды	15	150
16	Чехия	18,5	150
17	Турция	10	100
18	Канада	20	100
19	Дания	15	150

Киберпространство, как оперативная область [21], признается организацией североатлантического альянса, *North Atlantic Treaty Organization* (НАТО), наряду с сушей, морем, воздухом и космосом.

В настоящее время эксперты НАТО одобряют развитие, как оборонительного, так и оперативно кибернетического потенциала [22]. США существенно раньше озаботились защитой информации, как в ГИС, так и критической информационной инфраструктуры. В табл. 2 представлен перечень основных нормативно-правовых актов США.

Составной частью Федеральной ГИС (ФГИС) Росстандарта является Федеральный информационный фонд (ФИФ) по обеспечению единства измерений, созданный в соответствии с положениями Федерального закона № 102-ФЗ[3] и принадлежащий Федеральному агентству по техническому регулированию и метрологии (Росстандарт). В соответствии со статьей 20, сведения, содержащиеся в ФИФ, используются при оказании государственных услуг.

[3]Федеральный закон от 26.06.2008 № 102-ФЗ (ред. от 18.03.2019) «Об обеспечении единства измерений» // URL: http://www.consultant.ru/document/cons_doc_LAW_77904/ (дата обращения: 02.03.2020).

Таблица 2. Основные законодательные акты США в области ГИС и КИИ

№ п/п	Наименование НПА	Краткое описание
1	Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection 2003	Определяет национальную политику федеральных министерств и ведомств по выявлению и приоритезации важнейших объектов инфраструктуры и их защите от нападений.
2	FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems 2004	Устанавливает категории безопасности, как для информации, так и для информационных систем. Категории безопасности основаны на потенциальном воздействии на организацию в случае возникновения определенных событий, которые ставят под угрозу информацию и информационные системы, необходимые организации для выполнения возложенной на нее миссии, защиты ее активов, выполнения ее юридических обязанностей, поддержания ее повседневных функций и защиты физических лиц. Категории безопасности должны использоваться в сочетании с информацией об уязвимости и угрозах при оценке риска для организации.
3	FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems 2006	Стандарт устанавливает минимальные требования безопасности для федеральных ИС в семнадцати областях, связанных с безопасностью. Федеральные органы должны соблюдать минимальные требования безопасности, определенные в настоящем документе, путем использования средств контроля безопасности в соответствии с NIST SP800-53.
4	NIST SP800-53, Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations 2013	Целью документа является предоставление рекомендаций по выбору и конкретизации средств контроля безопасности для организаций и информационных систем, поддерживающих органы исполнительной власти федерального правительства в соответствии с требованиями публикации FIPS 200
5	NIST SP800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations 2011	Цель этого руководства – помощь организациям в разработке стратегии ISCM и реализации программы, которая обеспечивает осведомленность об угрозах и уязвимостях, видимость активов и эффективность развернутых средств контроля безопасности. Стратегия и программа ISCM поддерживают постоянную уверенность в том, что запланированные и реализованные средства контроля приведены в соответствие с допуском организационных рисков, а также способностью своевременно предоставлять информацию, необходимую для реагирования на риск.
6	Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21) 2013	Защита и обеспечение устойчивости критической инфраструктуры является законом Соединенных Штатов, который направлен на укрепление и обеспечение безопасности критической инфраструктуры страны. Президент Барак Обама выпустил PPD-21 в 2013 году для содействия большей интеграции и сотрудничеству между государственными и частными организациями. Целью директивы является снижение уязвимости, выявление и устранение угроз, минимизация последствий и ускорение усилий по реагированию и восстановлению, связанных с критической инфраструктурой.

Отметим, что областью деятельности Росстандарта в соответствии с постановлением[4] является, в том числе и область транспортных средств. Следовательно,

[4]Постановление Правительства РФ от 17 июня 2004 г. N 294 «О Федеральном агентстве по техническому регулированию и метрологии» // URL: https://base.garant.ru/12135835/ (дата обращения: 04.01.2020).

можно утверждать, что Федеральная ГИС Росстандарта является объектом КИИ, функционирующим в сфере транспорта. Одновременно можно отметить, что объектом критической информационной инфраструктуры могут являться ГИС, чему во ФСТЭК России имеются неоднократные подтверждения.

3. Модель угроз государственной информационной системы

3.1 Отличительные признаки государственных информационных систем

В соответствии со ст. 14 Федерального закона N 149-ФЗ[1] информационные системы, относящиеся к ГИС должны отвечать следующим критериям:

– в ГИС возможно размещение открытых данных (п. 4);

– создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами (п. 1);

– информация для создания и эксплуатации ГИС предоставляется как физическими лицами и организациями, так и государственными органами и органами местного самоуправления» (п. 3);

– доступ к части информации, циркулирующей в ГИС, может быть предоставлен только после авторизации в Единой системе идентификации и аутентификации (п. 4.1);

– технические средства, предназначенные для обработки информации, содержащейся в ГИС, в том числе программно-технические средства и СЗИ, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании (п. 8);

– информация, содержащаяся в государственных информационных системах, является государственными информационными ресурсами (п. 9);

– ответственными за обеспечение безопасности информации ГИС являются государственные органы (п. 9).

Для нахождения отличительных черт федеральных ГИС и определения критериев и показателей отнесения ГИС к федеральным ГИС предложено использовать «Реестр федеральных государственных информационных систем» (далее – Реестр), созданный в соответствии с Постановлением Правительства РФ №723[5] и в настоящее время размещенный на Сервере органов государственной власти Российской Федерации. Кроме того, для поиска введённых в эксплуатацию ГИС необходимо проанализировать все нормативные акты государственных органов и федеральных органов исполнительной власти, начиная с сентября 2009 года.

3.2 Анализ информационных систем

На момент прекращения актуализации в Реестре было зарегистрировано 339 федеральных ГИС, внесённых с 1988 г. по 2016 г. В табл. 3 представлен перечень некоторых «официальных» ГИС РФ.

Анализ ФГИС, входящих в Реестр проводился по критериям, представленным далее.

3.2.1 Общие особенности ФГИС

Анализ общих особенностей ФГИС проводился по следующим критериям:

– функционирование ФГИС в настоящее время: показатель бинарный, соответственно, значения – функционирует или не функционирует;

[5]Постановление Правительства РФ № 723 от 10 сентября 2009 г. «О порядке ввода в эксплуатацию отдельных государственных информационных систем» // URL: https://base.garant.ru/12169521/ (дата обращения 04.05.2020).

– представление ФГИС в сети Интернет: показатель бинарный, соответственно, значения – есть или нет.

3.2.2 Особенности ФГИС по доступу к информации

Анализ особенностей ФГИС, относящихся к доступу к циркулирующей в ней информации проводился по следующим критериям:

– наличие во ФГИС закрытого контура, для доступа к которому необходимо пройти какую-либо авторизацию: показатель бинарный, соответственно, значения – есть или нет;

– через Единую систему идентификации и аутентификации;

– через собственную систему авторизации;

– наличие во ФГИС открытого контура, для доступа к которому нет необходимости проходить какую-либо авторизацию: показатель бинарный, соответственно, значения – есть или нет;

– тип авторизации при доступе к закрытому контуру ФГИС: показатель неизвестен, возможные значения будут сформированы по результатам анализа.

3.2.3 Особенности ФГИС по вводу информации

Анализ особенностей ФГИС, относящихся к вводу информации проводился по следующим критериям:

– способ ввода информации во ФГИС в настоящее время: показатель неизвестен.

Предположительно, возможны следующие значения:

– через закрытый контур ФГИС;

– через взаимодействие с другими ИС;

– способ известен только Оператору.

3.2.4 Особенности ФГИС по организации взаимодействия с другими ИС

Анализ особенностей ФГИС, относящихся к их взаимодействию с другими информационными системами проводился по следующим критериям:

– наличие взаимодействия: показатель бинарный – взаимодействует или не взаимодействует;

– способ взаимодействия.

Предположительно, возможны следующие значения:

– с помощью собственного протокола обмена;

– с помощью утверждённого для взаимодействия ИС в РФ протокола обмена;

– протокол известен только Оператору.

3.2.5 Результаты анализа ФГИС, входящих в Реестр

По результатам анализа ФГИС, входящих в Реестр ФГИС, сформирована для дальнейшего исследования табл. 4. При анализе ФГИС, входящих в Реестр о значении конкретного показателя на основе косвенных данных, например, о способе ввода информации, взаимодействию с другими ИС и способе взаимодействия с другими ИС.

Косвенные данные подразумевают упоминание о значении показателя в сети Интернет. Оценка достоверности проводилась экспертным путём эксперта выступили исследователи.

3.3 Формирование критериев принадлежности ГИС к ФГИС

По результатам анализа принадлежности ГИС к ФГИС можно сделать следующие выводы:

– авторизация в закрытом контуре ФГИС происходит с помощью Единой системы идентификации и аутентификации, которая сама является ФГИС;

– взаимодействие ФГИС с другими информационными системами происходит по протоколам «Системы межведомственного электронного взаимодействия, СМЭВ[1]», которая сама является федеральной государственной информационной системой; введены в действие 20 февраля 2012 г. и созданной на основании п. 19 ст. 2[4].

Таблица 3. Перечень «официальных» ГИС Российской Федерации

№ п.п	Реест-ровый номер	Наименование ФГИС	Наименование оператора ФГИС	Дата ввода в эксплуа-тацию	Адрес официального сайта	Номер и дата выдачи электронного паспорта
1	1	ЕИС Роскомнадзора	Роскомнадзор	01.01.2010	www.rkn.gov.ru	ФС-77100001 от 31.03.2010
2	2	АИС ГВР	Росводресурсы	01.01.2008	voda.mnr.gov.ru	ФС-77100002 от 12.04.2010
3	5	ИТКС Контроль	Счетная палата Российской Федерации	25.12.2006	www.ach.gov.ru	ФС-77100005 от 23.04.2010
4	6	АИС РФС АПК	Минсельхоз России	01.09.2009	www.mcx.ru	ФС-77100006 от 28.04.2010
5	8	ЕИАС ФСТ России	ФСТ России	15.12.2006	www.fstrf.ru	ФС-77100008 от 12.05.2010
6	10	ИС ВПВ МИД России	МИД России	28.09.2001	www.mid.ru	ФС-77100010 от 27.05.2010
7	13	ЕБД	ФСКН России	01.01.2007	www.fskn.gov.ru	ФС-77100013 от 08.06.2010
8	14	ЕГАИС	Росалкоголь-регулирование	05.11.2008	www.fsrar.ru	ФС-77100014 от 09.06.2010
9	16	АИС Финансы	Минфин России	14.12.1999	www.minfin.ru	ФС-77100016 от 16.06.2010
10	17	АС ОПИГ МИД России	МИД России	29.12.2003	www.mid.ru	ФС-77100017 от 12.07.2010
11	18	АДИС-МВД	МВД России	22.12.2006	www.mvd.ru	ФС-77100018 от 14.07.2010
12	19	АИС «Консул ЗУ»	МИД России	23.02.2000	www.mid.ru	ФС-77100019 от 21.07.2010
13	24	ЭРПАС	Минкультуры России	06.12.2005	www.mkrf.ru	ФС-77100024 от 05.08.2010
14	25	АИС «Гражданство МИД»	МИД России	27.12.2006	www.mid.ru	ФС-77100025 от 20.08.2010
15	26	Электронный реестр судов	ФГУП Морсвязьспутник	01.03.2008	www.morflot.ru	ФС-77100026 от 06.09.2010
16	27	АИС «Загранпаспорт МИД»	МИД России	17.01.2007	www.mid.ru	ФС-77100027 от 08.09.2010
17	28	АИС УНРО	Минюст России	02.07.2007	www.minjust.ru	ФС-77100028 от 24.09.2010
18	30	АИС ЯРБ	Ростехнадзор	26.05.2009	www.gosnadzor.ru	ФС-77100030 от 06.10.2010
19	31	Инспектор	Ростехнадзор	25.02.2010	www.gosnadzor.ru	ФС-77100031 от 12.10.2010
20	32	Энергосистема-Зима	Ростехнадзор	25.02.2010	www.gosnadzor.ru	ФС-77100032 от 12.10.2010
21	33	Система каталогизации промышленной продукции для федеральных гос. нужд	ФГБУ РосНИИ ИТ и АП	28.12.2005	минобрнаки.рф	ФС-77100033 от 14.10.2010

Продолжение таблицы 3

22	34	ИСДМ-Рослесхоз	ФБУ Центральная база авиационной охраны лесов Авиалесоохрана	08.12.2005	www.rosleshoz.gov.ru	ФС-77100034 от 21.10.2010
23	35	ИАС ЕСУГИ	Росимущество	19.08.2009	www.rosim.ru	ФС-77100035 от 22.10.2010
24	37	Правовая информационная система Федерального агентства по рыболовству	Росрыболовство	15.12.2005	www.fishcom.ru	ФС-77100037 от 29.10.2010
25	38	Реестр лицензий	Росалкогольрегулирование	18.06.2009	www.fsrar.ru	ФС-77100038 от 01.11.2010
26	41	АИС «Служебный выезд»	МИД России	14.09.2007	www.mid.ru	ФС-77100041 от 11.11.2010
27	42	АИС ХБ ФМБА России	ФМБА России	01.12.2010	www.fmbaros.ru	ФС-77100042 от 22.11.2010
28	43	АИС Росздравнадзора	Росздравнадзор	31.03.2006	www.roszdravnadzor.ru	ФС-77100043 от 29.11.2010
29	45	АСВЗ	Росреестр	25.12.2010	www.rosreestr.ru	ФС-77100045 от 09.12.2010
30	48	База данных деклараций	Росалкогольрегулирование	11.11.2009	www.fsrar.ru	ФС-77100048 от 24.12.2010
31	51	ПК ИС ЕГРП	Росреестр	12.01.2015	www.rosreestr.ru	ФС-77110051 от 21.01.2011
32	52	АИС «Юстиция»	Росреестр	12.01.2015	www.rosreestr.ru	ФС-77110052 от 21.01.2011
33	53	Программное обеспечение по центральным выплатам получателям ЕДК в возмещении вреда здоровью гражданам, подвергшимся воздействию радиации вследствие радиационных аварий	Роструд	17.04.2007	www.rostrud.ru	ФС-77110053 от 31.01.2011
34	54	ЕФРСБ	Минэкономразвития России	29.12.2010	www.economy.gov.ru	ФС-77110054 от 01.02.2011
35	55	АИС РПУ	Роструд	01.01.2009	www.rostrud.ru	ФС-77110055 от 02.02.2011
36	56	АИС УП	Минэкономразвития России	22.10.2010	www.economy.gov.ru	ФС-77110056 от 08.02.2011
37	58	АИС АГС	Роструд	20.12.2006	www.rostrud.ru	ФС-77110058 от 14.02.2011
38	59	Система ФАИП	Минэкономразвития России	01.01.2011	www.economy.gov.ru	ФС-77110059 от 15.02.2011
39	60	ИС ФЦП	Минэкономразвития России	01.01.2011	www.economy.gov.ru	ФС-77110060 от 15.02.2011
40	62	Web-представительство информационно-аналитической системы «Трудовая миграция» (ИАС ТМ) «Работа в России»	Роструд	14.11.2008	www.rostrud.ru	ФС-77110062 от 15.02.2011

Таблица 4. Результаты исследования ФГИС, входящих в Реестр ФГИС

Функционирование ФГИС	Представительство ФГИС в сети Интернет	Наличие открытого контура	Наличие закрытого контура	Авторизация в закрытом контуре		
				ЕСИА	Своя СА	Н/Д
286	286	247	246	95	36	115

Продолжение Таблицы 4

Способ ввода информации			Взаимодействие ФГИС с другими ИС	Способ взаимодействия с другими ИС		
Через закрытый контур	Через взаимодействие с другими ИС	Н/Д		Через собственный протокол обмена	Через утверждённый протокол обмена	Н/Д
20	24	202	31	0	22	264

3.4 Анализ состояния баз данных угроз и уязвимостей

Для определения возможных угроз исследуемой ГИС необходимо провести анализ актуальных баз данных угроз и уязвимостей.

В этой части анализируются существующие в настоящее время БД уязвимостей с целью выбора наиболее подходящей для анализа наличия возможных уязвимостей и угроз безопасности информации объекта исследования.

3.4.1 Банк данных угроз безопасности ФСТЭК России

Банк данных угроз безопасности ФСТЭК России (БДУ ФСТЭК)[6] содержит сведения об основных угрозах безопасности информации и уязвимостях. Особое внимание уделяется угрозам, которые применимы к ГИС и АСУ производственными и технологическими процессами критически важных объектов. Ведётся данный банк, ФСТЭК России и ФАУ «ГНИИИ ПТЗИ ФСТЭК России».

В БДУ ФСТЭК содержатся как данные об угрозах безопасности информации, так и данные об уязвимостях в программном и программно-аппаратном обеспечении.

В настоящее время в БДУ ФСТЭК содержатся данные о двухсот тринадцати угрозах безопасности информации и о двадцати одной тысяче четырехстах тринадцати уязвимостях программного обеспечения. При этом, как правило, существует соответствие между уязвимостями БДУ ФСТЭК и в NVD.

Об использовании настоящего источника можно указать наличие в его реестре уязвимостей системного и общего программного обеспечения, входящего в [17].

3.4.2 База данных уязвимостей National Vulnerability Database (NVD) Национального института стандартов и технологий Министерства торговли США.

Данная база данных NVD ведётся с 1998 года и в настоящее время насчитывает более девяноста восьми тысяч уязвимостей. Нужно отметить, что не всегда имеются данные об уязвимостях в программном обеспечении российского производства.

Данная БД совместима с разработанным корпорацией MITRE Corporation (США) реестром уязвимостей CVE List (https://cve.mitre.org/cve/), ведением которого занимаются более 80 организаций, в т.ч. ведущие разработчики программного обеспечения и средств защиты информации, например, «Лаборатория Касперского».

Данный факт обуславливает, в отличие от БДУ ФСТЭК, очень быстрое пополнение реестра известных уязвимостей. В пользу принятия решения об использовании настоящего источника можно указать:

[6]Постановление Правительства РФ № 697 от 8 сентября 2010 г. «О единой системе межведомственного электронного взаимодействия» // URL: https://base.garant.ru/199319/ (дата обращения: 04.05.2019).

– большой объём накопленных данных об уязвимостях;

– продолжающееся, при разработке ГИС, использование системного и общего программного обеспечения, не входящего в «Единый реестр российских программ для электронных вычислительных машин и баз данных» [18].

3.4.3 Прочие база данных уязвимостей

Для полноты были проанализированы следующие базы данных уязвимостей.

3.4.3.1 Secunia Advisory and Vulnerability Database

Ведётся с 2003 года исследовательской компанией Secunia Research (всемирная компания с филиалами в США и Европе). Не в полной мере совместима с NVD и не совместима с БДУ ФСТЭК. Содержит свыше семидесяти тысяч записей о различных уязвимостях. Бесплатный доступ к Secunia Advisories and Vulnerability Database возможен только при некоммерческом использовании. Доступна по адресу: https://secuniaresearch.flexerasoftware.com/community/advisories/.

3.4.3.2 Open Sourced Vulnerability Database

Ведение БД было начато в 2004 году как свободно доступный проект. В 2016 году с закрытием трансформировалась в коммерческий проект – БД уязвимостей VulnDB (https://vulndb.cyberriskanalytics.com/). В настоящее время содержит свыше ста семидесяти тысяч записей.

3.4.3.3 Vulnerability Notes Database

VND (Vulnerability Notes Database, https://www.kb.cert.org/vuls). Ведётся CERT Coordination Center при университете Carnegie Mellon (США). Является агрегатором. Обновления крайне редки. По состоянию на настоящее время насчитывает не более пяти тысяч записей.

3.4.4 Итоги отбора БДУ

Исходя из анализа БД уязвимостей и угроз, по критериям соответствия среде используемого в РФ программного обеспечения, полноты содержания описаний уязвимостей и их связями с угрозами и вида доступа к информации, принято решение использовать в качестве источников информации об уязвимостях и угрозах БДУ ФСТЭК России.

3.5 Математические методы, применимые при построении модели угроз

Набор исходных данных, представляют собой конечные множества данных, для которых можно использовать математическую модель на основе теории множеств.

Построение характеристической функции, принимающей одно из двух бинарных значений «1» – «Принадлежит, истина, входит, …» или «0» – «Не принадлежит, ложно, не входит, …» становится затруднительным. Например, можно указать наличие в составе ФГИС определённой версии некоего ПО, имеющего уязвимости по данным NVD, но отсутствующем в БДУ ФСТЭК России. Иными словами, существенную часть решений будет приниматься экспертами на основании своих знаний и опыта.

Заключение

Анализ текущего состояния информационных фондов ОГВ РФ (федеральных министерств и ведомств РФ, ОГВ субъектов РФ) выявил наиболее характерные тенденции, имеющие распространение и на информационные ресурсы, и на ГИС. В работе выявлены отличительные признаки и разработаны критерии отбора федеральных ГИС.

Исходя из анализа баз и банков данных уязвимостей и угроз, проведенного по критериям соответствия среде используемого в РФ программного обеспечения, полноты содержания описаний уязвимостей и их связями с угрозами и вида доступа к информации,

принято решение использовать в качестве источников информации об уязвимостях и угрозах БДУ ФСТЭК России и в нормативно-правовых актах.

В результате проведенных исследований подтверждены: возрастающая значимость защиты государственных информационных систем; актуальность выбранной темы и принадлежность (важность отнесения) рассматриваемого объекта исследования к государственной информационной системы и критической информационной инфраструктуре.

Полученные данные предполагается в дальнейшем использовать в ходе разработки методики оценки угроз безопасности информации в государственных информационных системах.

СПИСОК ЛИТЕРАТУРЫ:

1. Горлатых, Андрей В.; Запечников, Сергей В. Построение защищенной системы управления многомерными структурами данных. Безопасность информационных технологий, [S.l.]. Т. 25, № 3. С. 16–25, сен. 2018. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1136 (дата обращения: 19.08.2020). DOI: http://dx.doi.org/10.26583/bit.2018.3.022.
2. Малюк, Анатолий А.; Гавдан, Григорий П. Формирование и использование национальных информационных ресурсов – основа развития цифровой экономики. Безопасность информационных технологий, [S.l.]. Т. 26, № 2. С. 67–85, июнь 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1200/1145. (дата обращения: 20.07.2020). DOI:http://dx.doi.org/10.26583/bit.2019.2.05.
3. О выездном совещании Секретаря Совета Безопасности России Николая Патрушева с главами регионов, входящих в состав Сибирского федерального округа. Официальные сайты органов государственной власти Российской Федерации // URL: http://www.scrf.gov.ru/news/allnews/2665/ (дата обращения 02.07.2020).
4. Баранкова И.И., Михайлова У.В., Афанасьева М.В. «Минимизация рисков информационной безопасности на основе моделирования угроз безопасности» // Динамика систем, механизмов и машин. 2019. № 4. С. 60–66. DOI: https://doi.org/10.25206/2310-9793-7-4-60-66.
5. Дойникова Е.В., Котенко И.В. «Методики и программный компонент оценки рисков на основе графов атак для систем управления информацией и событиями безопасности» // Информационно-управляющие системы. 2016. №5. С. 56–67. DOI: https://doi.org/10.15217/issn1684-8853.2016.5.54.
6. Шабуров А.С., Юшкова С.А., Бодерко А.В. «Моделирование оценки угроз безопасности информационных систем персональных данных» // Вестник ПНИПУ. Серия «Электротехника, информационные технологии, системы управления». 2013. № 7 (1). С. 149–159. УДК: 004.056.5-047.58.
7. Шинкаренко А.Ф. Методика оценивания защищенности информационно-телекоммуникационных узлов // Интеллектуальные технологии на транспорте. 2016. №1. URL: https://cyberleninka.ru/article/n/metodika-otsenivaniya-zaschischennosti-informatsionno-telekommunikatsionnyh-uzlov (дата обращения: 07.07.2020).
8. Казарин О.В., Шаряпов Р.А., Ященко В.В. Многофакторная классификация угроз информационной безопасности киберфизических систем // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2018. № 1 (1). С. 39–55. УДК 004.056.
9. Глобальное исследование утечек конфиденциальной информации в 2017 году, InfoWatch // URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2017_year.pdf?rel=1 (дата обращения: 07.05.2020).
10. Глобальное исследование утечек конфиденциальной информации в 2018 году, InfoWatch // URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2018_year.pdf?rel=1 (дата обращения: 07.05.2019).
11. Kaspersky Security Bulletin: Прогнозы по развитию угроз в сфере промышленной безопасности на 2019 год. АО «Лаборатория Касперского» // URL: https://securelist.ru/ksb-threat-predictions-for-industrial-security-in-2019/92848/ (дата обращения: 07.05.2020).
12. Уязвимости в АСУ ТП: итоги 2018 года. «Positive Technologies» // URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-vulnerabilities-2019-rus.pdf (дата обращения: 07.05.2020).
13. Рябова В. Китай признал существование кибервойск. D-Russir.ru // URL: https://d-russia.ru/kitaj-priznal-sushhestvovanie-kibervojsk.html (дата обращения: 07.07.2020).

14. Zecurion Analytics «Кибервойны 2017: Баланс сил в мире». Аналитический центр Zecurion // URL: https://www.zecurion.ru/upload/iblock/cb8/cyberarmy_research_2017_fin.pdf (дата обращения: 07.05.2020).
15. Аналитики назвали Россию в числе пяти стран с лучшими кибервойсками. Лента новостей. РБК // URL: https://www.rbc.ru/politics/10/01/2017/58747b439a7947526d203417 (дата обращения: 07.07.2020).
16. National initiative for cybersecurity education (NICE) // URL: https://www.nist.gov/itl/applied-cybersecurity/nice (дата обращения: 02.05.2020).
17. 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, май 2018. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1107. (дата обращения: 05.06.2020). DOI: http://dx.DOI.org/10.26583/bit.2018.2.02.
18. NATIONAL SECURITY STRATEGY of the United States of America DECEMBER 2017 // URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (дата обращения: 04.05.2020).
19. Салкуцан, Алексей А.; Гавдан, Григорий П.; Полуянов, Андрей А. Методика определения критических процессов на объектах информационной инфраструктуры. Безопасность информационных технологий, [S.l.]. Т. 27, № 2. С. 18–34, июнь 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1268/1187. DOI: http://dx.doi.org/10.26583/bit.2020.2.02 (дата обращения: 26.07.2020).
20. Банк данных угроз безопасности информации Федеральной службы по таможенному и экспортному контролю Российской Федерации // URL: https://bdu.fstec.ru (дата обращения: 04.05.2020).
21. Mauno Pihelgas. Design and Implementation of an Availability Scoring System for Cyber Defence Exercises. (This paper was accepted to the 14th International Conference on Cyber Warfare and Security: ICCWS 2019 and the final version of the paper is included in the Conference Proceedings. ISBN: 978-1- 912764-11-2; ISSN: 2048-9870).URL:https://ccdcoe.org/uploads/2020/02/M_Pihelgas-Design_and_Implementation_of_an_Availability_Scoring_System_for_Cyber_Defence_Exercises.pdf (дата обращения: 02.05.2020).
22. 12th International Conference on Cyber Conflict 20/20 VISION: THE NEXT DECADE Copyright © 2020 by NATO CCDCOE Publications. All rights reserved. URL: https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.pdf (дата обращения: 02.05.2020).

REFERENCES:

[1] Andrey V. Gorlatyh, Sergey V. Zapechnikov. Building secure multidimensional data management system. IT Security (Russia), [S.l.]. V. 25, n. 3. P. 16–25, sep. 2018. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1136. (accessed: 19.08.2020). DOI: http://dx.doi.org/10.26583/bit.2018.3.02 (in Russian).
[2] MALYUK, Anatoly A.; GAVDAN, Grigory P. Development and use of national information resources as the basis for digital economy development. IT Security (Russia), [S.l.]. V. 26, n. 2. P. 67–85, june 2019. ISSN 2074-7136. URL: <https://bit.mephi.ru/index.php/bit/article/view/1200 (accessed: 20.07.2020). DOI: http://dx.doi.org/10.26583/bit.2019.2.05 (in Russian).
[3] About the visiting meeting of the Secretary of the Security Council of Russia Nikolai Patrushev with the heads of the regions that make up the Siberian Federal district. Official websites of state authorities of the Russian Federation. Available on: URL: http://www.scrf.gov.ru/news/allnews/2665/ (accessed: 02.07.2020) (in Russian).
[4] Barankova I.I., Mikhailova U.V., Afanasyeva M.V. Minimization of information security risks based on modeling security threats. Dynamics of Systems, Mechanisms and Machines (Dynamics). 2019. № 4. P. 60–66. DOI: https://doi.org/10.25206/2310-9793-7-4-60-66 (in Russian).
[5] Dojnikova E.V., Kotenko I.V. TECHNIQUES AND SOFTWARE TOOL FOR RISK ASSESSMENT ON THE BASE OF ATTACK GRAPHS IN INFORMATION AND SECURITY EVENT MANAGEMENT SYSTEMS. Saint-Petersburg Institute for Informatics and Automation of the RAS. 2016. №5. P. 56–67. DOI: https://doi.org/10.15217/issn1684-8853.2016.5.54 (in Russian).
[6] Shaburov A.S., Yushkova S.A., Boderko A.V. Modelling of evaluation of security threat for informational systems dealing with personal data. Vestnik PNIPU. Seriya «Elektrotekhnika, informacionnye tekhnologii, sistemy upravleniya». 2013. № 7 (1). S. 149–159. UDC: 004.056.5-047.58 (in Russian).
[7] Shinkarenko A.F. The method of estimation of the security of information and telecommunication. Intellectual Technologies on Transport. 2016. №1. URL: https://cyberleninka.ru/article/n/metodika-otsenivaniya-zaschischennosti-informatsionno-telekommunikatsionnyh-uzlov (in Russian).

[8] Kazarin O.V., Sharyapov R.A., Yashchenko V.V. Multifactorial classification of threats to information security of cyber-physical systems. Vestnik RGGU. Seriya «Informatika. Informacionnaya bezopasnost'. Matematika». 2018. № 1 (1). S. 39–55. UDC 004.056 (in Russian).
[9] Global study of confidential information leaks in 2017, InfoWatch. URL:https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2017_year.pdf?rel=1 (accessed: 07.05.2020) (in Russian).
[10] Global study of confidential information leaks in 2018, InfoWatch. URL:https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2018_year.pdf?rel=1 (accessed: 07.05.2019) (in Russian).
[11] «Kaspersky Security Bulletin: Kaspersky Security Bulletin: Forecasts for the development of threats in the field of industrial security for 2019. «Kaspersky Lab». URL: https://securelist.ru/ksb-threat-predictions-for-industrial-security-in-2019/92848/ (accessed: 07.05.2020) (in Russian).
[12] Vulnerabilities in automated process control systems: 2018 results. «Positive Technologies» // URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-vulnerabilities-2019-rus.pdf (accessed: 07.05.2020) (in Russian).
[13] Ryabova V. China has recognized the existence of cyber warfare. D-Russir.ru. URL: https://d-russia.ru/kitaj-priznal-sushhestvovanie-kibervojsk.html (accessed: 07.07.2020) (in Russian).
[14] Zecurion Analytics: Cyberwar 2017: Balance of power in the world. Analytical center Zecurion. URL: https://www.zecurion.ru/upload/iblock/cb8/cyberarmy_research_2017_fin.pdf (accessed: 07.05.2020) (in Russian).
[15] Analysts named Russia among the five countries with the best cyber forces. News feed.. RBC.RU. URL: https://www.rbc.ru/politics/10/01/2017/58747b439a7947526d203417 (accessed: 07.07.2020) (in Russian).
[16] National initiative for cybersecurity education (NICE) Workforce Framework Cybersecurity. NICCS. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf (accessed: 02.05.2020).
[17] 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: 05.06.2020). DOI: http://dx.doi.org/10.26583/bit.2018.2.02 (in Russian).
[18] NATIONAL SECURITY STRATEGY of the United States of America DECEMBER 2017. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (accessed: 04.05.2020).
[19] Salkutsan Alexei A., Gavdan Grigory P., Poluyanov Andrey A. The method of identifying critical processes at information infrastructure facilities. IT Security (Russia), [S.l.]. V. 27, n. 2. P. 18–34, june 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1268/1187.
DOI: http://dx.doi.org/10.26583/bit.2020.2.02 (accessed: 26.07.2020).
[20] Data Bank of information security threats of the Federal service for customs and export control of the Russian Federation. URL: https://bdu.fstec.ru (accessed: 04.05.2020).
[21] Mauno Pihelgas. Design and Implementation of an Availability Scoring System for Cyber Defence Exercises. (This paper was accepted to the 14th International Conference on Cyber Warfare and Security: ICCWS 2019 and the final version of the paper is included in the Conference Proceedings. ISBN: 978-1- 912764-11-2; ISSN: 2048-9870). URL: https://ccdcoe.org/uploads/2020/02/M_Pihelgas_-_Design_and_Implementation_of_an_Availability_Scoring_System_for_Cyber_Defence_Exercises.pdf. (accessed: 02.05.2020).
[22] 12th International Conference on Cyber Conflict 20/20 VISION: THE NEXT DECADE Copyright © 2020 by NATO CCDCOE Publications. All rights reserved. URL: https://ccdcoe.org/uploads/2020/05/CyCon_2020_book.pdf (accessed: 02.05.2020).

Поступила в редакцию - 16 июля 2020 г. Окончательный вариант - 20 августа 2020 г.
Received - July 16, 2020. The final version - August 20, 2020.