Григорий П. Гавдан[1], Рустем В. Пенерджи[2]
[1]Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, Москва, 115409, Россия
[2]ФГУП «Всероссийский Научно-исследовательский институт метрологической службы», Озерная ул., 46, Москва, 119361, Россия
[1]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[2]e-mail: Prv0@yandex.ru, https://orcid.org/0000-0003-4105-2221

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

DOI: http://dx.doi.org/10.26583/bit.2020.4.07

Аннотация. Целью написания статьи является рассмотрение вопросов, связанных с обеспечением безопасности информации информационных систем (ИС). Актуальность работы обусловлена, прежде всего, тем, что число кибератак на различные сферы экономики российского государства не уменьшается, а с каждым годом продолжает расти. Наблюдается растущий интерес к информации, циркулирующей в государственных органах управления (всех уровней) и государственных информационных систем (ГИС). Порой важные стратегические (государственные) задачи зачастую приходится отодвигать на «задний» план перед необходимостью решения срочных (важных сиюминутных) тактических задач. ГИС это неотъемлемая часть достаточно сложной системы управления, а (само) управление (фактически) становится ситуационным, а значит, и роль структур государственного управления, и ГИС, в этих условиях не утратила своей актуальности. Предметом исследования в работе является обеспечение безопасности ГИС в условиях неопределенности. Для достижения поставленной цели в работе проводится анализ нормативно правовых актов Российской Федерации. ГИС рассмотрены, как объекты компьютерных атак в условиях неопределенности. Разработана методика категорирования ГИС. В статье рассмотрены основные определения, аргументы и приведены источники, подтверждающие важность оценки угроз безопасности информации ГИС. В результате проведенных в работе исследований подтверждены возрастающая значимость защиты и актуальность разработки методики по оценке угроз безопасности информации. Вывод: правильно поставленная работа (с исходными данными) для проведения исследования в условиях высокой степени их неопределенности является ключевым моментом в решении любых задач, связанных с обеспечением информационной безопасности, в том числе и ГИС. Результаты исследования могут быть использованы при разработке методики оценки угроз безопасности государственных информационных систем.

Ключевые слова: безопасность информации, государственная информационная система, государственные органы управления, информационная система, объект компьютерных атак, оценки угроз безопасности информации, управление.

Для цитирования: ГАВДАН, Григорий П.; ПЕНЕРДЖИ, Рустем В. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ. Безопасность информационных технологий, [S.l.], v. 27, n. 4, p. 77–94, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1308>. Дата доступа: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.07.

Grigory P. Gavdan[1], Rustem V. Penerdji[2]
[1]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoe sh., 31, Moscow, 115409, Russia
[2]All-RUSSIAN RESEARCH INSTITUTE OF METROLOGICAL SERVICE, Ozernaya str., 46, Moscow, 119361, Russia
[1]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[2]e-mail: Prv0@yandex.ru, https://orcid.org/0000-0003-4105-2221

Ensuring the security of state information systems in conditions of uncertainty

DOI: http://dx.doi.org/10.26583/bit.2020.4.07

Abstract. The paper addresses issues related to information security of information systems (IS). The Relevance of the work is primarily due to the fact that the number of cyber-attacks on various sectors of the Russian economy is not decreasing, but keeps growing every year. There is an increasing interest in the information circulating in government authorities (at all levels) and SIS. Sometimes important strategic (state) tasks often have to be relegated to the "background" before the need to solve urgent (important short-term) tactical tasks. Today, SIS is an integral part of a rather complex management system, and (itself) management (in fact) becomes situational, which means that the role of public administration structures, and SIS, in these conditions has not lost its relevance. The subject of the research is to ensure the security of SIS in conditions of uncertainty. To achieve this goal, the paper uses the method of analysis of regulatory legal acts of the Russian Federation. SIS data are considered as objects of computer attacks under conditions of uncertainty. The structure of the SIS categorization methodology was developed. The paper discusses the main definitions, arguments, and sources that confirm the importance of assessing threats to the security of SIS information. As a result of the research the increasing importance of protection and the relevance of developing a methodology for assessing information security threats are confirmed. Conclusion: correctly set work (with initial data) for conducting research in conditions of a high degree of their uncertainty is a key point in solving any problems related to information security, including SIS. The results of the study can be used to develop a methodology for assessing threats to the security of state information systems.

Keywords: information security, state information system, state management bodies, information system, object of computer attacks, information security threat assessment, management

For citation: GAVDAN, Grigory P.; PENERDJI, Rustem V. Ensuring the security of state information systems in conditions of uncertainty. IT Security (Russia), [S.l.], v. 27, n. 4, p. 77–94, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1308>. Date accessed: 18 nov. 2020. DOI: http://dx.doi.org/10.26583/bit.2020.4.07.

Введение

Всё чаще ведущие мировые эксперты обращают внимание на то, что сегодня мир вступил *в эпоху новой научно-технической революции*. Современное *коммуникационное*, быстро меняющееся общество вступило в информационный (постиндустриальный) период. Таким образом, мы (общество) все становимся свидетелями ситуации, когда проблемы (того или иного вида деятельности) *информационного общества* превосходят проблемы индустриализации производства[1].

Научно-техническая революция изменила очень многое, однако сейчас в обществе назрели перемены, в образе жизни, во внутреннем мире людей, поэтому можно говорить о социально-технологической революции, которая раздвигает рамки давосского проекта [1] и других технократических проектов будущего. Всё это зачастую связано с военными, политическими, конкурентными (борьбой) или экономическими «играми»; с расширением различных систем и сетей; с возможностью несанкционированного доступа к создаваемой, обрабатываемой, передаваемой и хранимой информации; с экономическим и промышленным шпионажем и др. Развитие методов, средств и форм (автоматизация процессов обработки, передачи, хранения и распространение информации; защита информации от незаконного изменения, уничтожения и хищения и др., а также их повсеместное применение) делает защищаемую информацию *более уязвимой* [2]. Действия злоумышленников могут быть направлены на информационные системы, IT-инфраструктуру компании, мобильные

[1]Малюк А.А. Основы политики безопасности критических систем информационной инфраструктуры. Курс лекций. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2019. – 314 с.

устройства, рабочие компьютеры, другие технические средства и, наконец, на любого человека как на элемент киберпространства [3].

Утверждается, что в прогнозный период развития информационные технологии будут способствовать реализации национальной программы «Цифровая экономика Российской Федерации» (например, налоговый маневр и др.). России (сегодня) предстоит обеспечить решение первоочередных задач[2] формирования цифровой экономики, в том числе:

– совершенствование регуляторной и нормативной среды;

– увеличение внутренних затрат на развитие цифровой экономики Российской Федерации (Министерство экономического развития Российской Федерации);

– обработки и хранения больших объемов данных;

– создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи;

– повышение уровня информационной безопасности во всех сферах деятельности;

– обеспечение подготовки высококвалифицированных кадров для экономики.

Так, например, в [3] за II квартал 2019 г. отмечаются следующие тенденции [3]:

– количество уникальных инцидентов остается высоким (превосходит показатель I квартала на 3%);

– целенаправленные атаки преобладают над массовыми атаками (их доля составила 59%. Это на 12 % пунктов больше, чем в I квартале);

– более половины всех компьютерных преступлений совершаются с целью кражи информации (это прямая финансовая выгода в 42% атак против частных лиц и в 30% атак на юридические лица);

– персональные данные (ПДн) – основной тип украденной информации в атаках на юридические лица (29%) (частные лица наиболее часто рискуют учетными записями и данными своих банковских карт – соответственно 44% и 34% от всего объема информации, украденной у частных лиц);

– уверенный рост курса биткойна, так объемы скрытого майнинга выходят на прежний уровень;

– набирают обороты Атаки MageCart на онлайн-ресурсы;

– специалистами отмечаются вредоносные JavaScript-снифферы, в том числе и на сайтах без функции оплаты;

– не уменьшается доля заражений вредоносным программным обеспечением (ПО) среди государственных учреждений (62% против 44% в I квартале 2019 г.). Наиболее часто в минувшем квартале, например, атакам троянов шифровальщиков;

– группировка RTM продолжает активно атаковать одну из слабо защищенных отраслей (промышленный сектор) [3].

Весьма существенное увеличение зарегистрированных преступлений наблюдается в IT-сфере. За 8 месяцев текущего года правоохранители выявили 180 153 (+66,8 %) преступления, которые были совершены с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации [4].

К глубокому сожалению, в России многие (изначально) экономические программы и бизнес практики оказались и/или продолжают оказываться трудно реализуемыми, ущербными, а то и вовсе заброшенными. Усложненность и парадоксальность развития экономических программ и бизнес-практик постоянно требует качественного обновления

[2]Прогноз социально-экономического развития Российской Федерации на 2021 год и на плановый период 2022 и 2023 годов. Министерство экономического развития Российской Федерации, 2019. – 94 с. URL: https://www.economy.gov.ru/material/file/956cde638e96c25da7d978fe3424ad87/Prognoz.pdf.

знаний, накопления опыта и навыков [5], чего не происходит. Большинство существующих решений достаточно плохо справляются с выявлением внешне легитимных действий злоумышленников и защитой ИТ-инфраструктуры, а потому в настоящее время активно применяется поведенческий анализ.

Перевод в сотрудников на удаленный режим работы из-за эпидемии COVID-19 привел не только к сокращению рабочих мест, но и к увеличению рисков. Пользователи через общедоступные сети для выполнения своей должностной работы массово заходят в корпоративные информационные системы, которые не обеспечены необходимой защитой.

Злоумышленник становятся изобретательнее, а, поэтому обеспечивать безопасность становится всё сложнее [5]. Он стал более изощренным: ведёт незаметные целевые атаки и может скачивать информацию ограниченного доступа, не привлекая к себе внимания [4]. Следовательно, существующие информационно-технологические разработки и программы должны учитывать и возникающие изменения, например, нарастание угроз, происходящие вокруг изменения и др. Органы государственной власти сегодня не являются исключением, которым для управления важно иметь хорошую и защищенную систему управления, работа которой направлена на разработку и построение целостной модели развития государства для его процветания, существования и выживания, в том числе и *в условиях неопределенности.*

Развитие (на перспективу) будущих теорий и практик общества в условиях неопределенности требует адекватного и ясного целеполагания действий. Так, например, достаточно ясное представление о серьёзных угрозах критической сферы народного хозяйства страны (национальная безопасность) за счет широкого внедрения современных информационных технологий (ИТ) сегодня можно найти в различных источниках[1]. Так, ГИС включают в себя 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 [5].

Обратимся к определению, *государственные информационные системы* (ГИС) – это федеральные и региональные информационные системы (ИС), созданные на основании (соответственно) федеральных законов, законов субъектов РФ, на основании правовых актов госорганов. Они являются важной и неотъемлемой частью [6] сложной системы государственного управления и (ст.14)[3] созданы в целях реализации полномочий государственных органов и обеспечения обмена информацией.

Органы государственной власти разных уровней имеют в настоящее время значительные объемы информационных фондов, объединяющихся в десятки тысяч (баз данных), которые в области защиты информации (ЗИ) требуют к себе должного внимания. Следовательно, информационная инфраструктура, в том числе и её ГИС, будут продолжать оставаться одним из основных и важных объектов защиты [6].

Меры защиты информации (ЗИ) ГИС реализуются и выбираются с учетом *угроз безопасности информации* применительно к субъектам и объектам доступа (аппаратный, системный, прикладной и сетевой уровни); в среде виртуализации и облачных вычислений и т.д. Здесь необходимо также учитывать:

а) значения всех факторов, влияющих на требуемый уровень защиты информации ГИС (значения таких факторов в лингвистических переменных в виде унифицированной схемы представлены в работе Малюка А.А.[1], табл. XII.1);

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

б) организационные и технические меры ЗИ ГИС, которые определяются:

– масштабом ГИС;

– назначением ГИС;

– распределенностью сегментов ГИС.

в) затруднения, возникающие сегодня при обеспечении безопасности информации современных информационных систем, во многом связаны с:

– частым обнаружением новых уязвимостей и угроз в программном и аппаратном обеспечении информационных систем;

– задержкой при включении обнаруженных факторов риска в разные нормативно-правовые акты (НПА) РФ в области обеспечения безопасности информации и отсутствием соответствия между этими НПА;

– субъективностью экспертных оценок, возникающей при формировании модели угроз безопасности информационных систем и увеличивающейся при этом степенью неопределённости модели угроз.

Защита информации ГИС обеспечивается проведением таких мероприятий, как

– формированием требований к ЗИ ГИС;

– разработкой системы ЗИ ГИС;

– внедрением системы ЗИ ГИС;

– проведением аттестации ГИС по требованиям ЗИ;

– обеспечением ЗИ ГИС в ходе эксплуатации аттестованной ГИС;

– обеспечением ЗИ после принятия решения об окончании обработки информации;

– обеспечением ЗИ при выводе из эксплуатации, аттестованной ГИС и др.

Интерес к вопросам обеспечения безопасности информации ГИС продолжает расти. Это связывают, прежде всего, с

– небывалым повышением значимости информации (масштаб) как общественного (государственного) ресурса;

– существенными изменениями в организации информационно-технологических сетей и информационных технологий;

– возникающей опасностью злоумышленных действий по отношению к её законным участникам;

– наличием богатейшего опыта организации различных защитных мер бизнес процесса и др.;

– значимыми достижениями научных исследований в области защитных мер бизнес процессов;

– возросшей ролью государственных информационных ресурсов необходимых для обеспечения управления, жизнедеятельности государства.

Заметно усиление тенденций направленных:

– на повышение квалификации злоумышленников проводящих компьютерные атаки;

– на добывание злоумышленниками любой ограниченного доступа информации (государственной, коммерческой тайн, в том числе компрометирующей информации) ГИС;

– на увеличение частоты самих компьютерных атак на крупные мировые компании;

– на блокирование работы ГИС и вывод их из строя.

Так, в настоящее время, *не многие заказчики и операторы ГИС* понимают важность комплексной защиты информации в ИС. Использование полученной злоумышленником

информации может нанести серьезный ущерб. Именно поэтому необходимо осознанно подходить к выбору средств защиты информации в ГИС [7].

Перейдём к рассмотрению нормативно-правовых актов, регулирующих объекты КИИ и ГИС РФ.

1. Нормативно-правовые акты, регулирующие объекты КИИ и ГИС РФ

1.1 Критерии отбора нормативно-правовых актов

Отбор нормативно-правовых актов выполнялся по следующим критериям:

– областью регулирования НПА должна быть КИИ и ГИС;

– источником НПА должны быть федеральные органы исполнительной власти РФ и регуляторы в части защиты информации;

– НПА должны присутствовать в открытом доступе (документы, содержащие сведения, содержащую государственную тайну и конфиденциальную информацию не анализировались).

В настоящее время в Российской Федерации действуют следующие нормативно–правовые акты, регулирующие критическую информационную инфраструктуру (КИИ).

1.2 Перечень нормативно-правовых актов, применимых к объекту исследований

1.2.1 Законы и указы, применяемые к объекту исследований

В настоящее время в РФ действуют следующие НПА, регулирующие создание и функционирование объектов КИИ.

Так, основными концептуальными документами РФ в сфере информационной безопасности являются:

– Стратегия национальной безопасности РФ № 683 от 31.12.2015;

– Доктрина информационной безопасности РФ № 6646 от 05.12.2016;

– Стратегия развития информационного общества в РФ на 2017 – 2030 годы № 203 от 09.05.2017.

Основополагающими НПА Российской Федерации в указанной области являются:

– Федеральный закон № 187-ФЗ от 26 июля 2017 года;

– Закон Российской Федерации № 5485-1 от 21.07.1993;

– Указ Президента Российской Федерации № 1203 от 30.11.1995.

1.2.2 Подзаконные акты РФ, применяемые к объекту исследований

Во исполнение требований вышеприведенных законодательных актов разработаны, введены в действие и скорректированы следующие нормативные акты:

– Постановление Правительства РФ № 127 от 08.02.2018;

– Постановление Правительства РФ № 162 от 17.02.2018;

– Приказ ФСТЭК России № 31 от 14.03.2014;

– Приказ ФСТЭК России № 227 от 06.12.2017;

– Приказ ФСТЭК России № 235 от 21.12.2017;

– Приказ ФСТЭК России № 236 от 22.12.2017;

– Приказ ФСТЭК России № 239 от 25.12.2017;

– Приказ ФСБ Российской Федерации № 366 от 24.07.2018;

– Приказ ФСБ Российской Федерации № 367 от 24.07.2018;

– Приказ ФСБ Российской Федерации № 368 от 24.07.2018.

1.2.3 Методические документы РФ, применимые к объекту исследований

Помимо действующих нормативных актов необходимо вспомнить ещё и о Методических документах ФСТЭК России, например, таких как:

– «Меры защиты информации в государственных информационных системах»[4];
– «Методика моделирования угроз безопасности информации»[5] (проект).

1.3 Обзор законодательства по ГИС и КИИ основного геополитического противника

Различные отрасли экономики сегодня активно стоят на внедрении новых цифровых решений, которые позволят с помощью автоматизированных систем управления технологическими процессами, информационно-телекоммуникационных систем (сетей) и информационных систем осуществить модернизацию и повысить тем самым свою конкурентоспособность. Чаще всего приобретая такие решения, руководство предприятий или организаций не хотят (или не задумываются) уделять требуемого внимания вопросам обеспечения защиты информации [8] считая, что на этом можно сэкономить деньги.

В настоящее время считается, что основным геополитическим противником для США являются Китай и Российская Федерация. Содержание (является тому подтверждением) актуальной (редакция 2017 г.) Стратегии Национальной Безопасности США: «Китай и Россия бросают вызов американской власти, влиянию и интересам, пытаясь подорвать американскую безопасность и процветание» [9].

В [9] Россия обвиняется (*не обоснованно*) в проведении информационных атак против т.н. «свободного мира»: «Россия (по всему миру) использует информационные операции как часть (наступательные) киберусилий по влиянию на общественное мнение. Её кампании влияния сочетают тайные разведывательные операции и ложные онлайн-персонажи с государственными СМИ, посредниками и платными пользователями социальных сетей или «троллями» [10]. Наряду с сушей, морем, воздухом и космосом, *киберпространство*, признается организацией североатлантического альянса (НАТО) как оперативная область [11]. Эксперты НАТО одобряют развитие, как оборонительного, так и оперативно кибернетического потенциала [12] государства. К слову сказать, США существенно раньше всех озаботились защитой информации, как в ГИС, так и критической информационной инфраструктуре (*Federal Information and Information Systems* и *Critical Infrastructure*).

В США и странах запада на основе финансирования научно-исследовательских проектов различного вида и рода направлений заметно развитие и стремительный подъем информационных технологий (ИТ). К тому же в США сосредоточены ведущие научно-технические кластеры мира. Например, в США с 2015 г. по 2019 г. в области финансирования научных разработок в военной и гражданской сфере продолжает прослеживаться динамика (это сотни млрд долларов) роста вложений [13]. Благодаря такому внедрению научных разработок (значительный объем ИТ в США продается за рубеж) и развитию информационной сферы. Поэтому Америка остаётся (сегодня) абсолютным мировым лидером [13]. В настоящее время возникает большое количество вопросов, на которые необходимо дать точные ответы. Так, примером может послужить, определение критических процессов ГИС в условиях неопределённости и др.[6]

2. Разработка структуры методики категорирования Федеральной ГИС

2.1 Принадлежность объекта исследований к критической информационной

[4]Методический документ. «Меры защиты информации в государственных информационных системах». Утвержден ФСТЭК России 11 февраля 2014 г.
[5]Проект Методического документа. «Методика моделирования угроз безопасности информации». ФСТЭК России 2020 г.
[6]Проблемные вопросы процедуры категорирования объектов КИИ // Единый портал электронной подписи. URL: https://iecp.ru/news/item/423941-problemnyye-voprosy-protsedura-kategorirovaniya-kiya-obyekty (дата обращения: 12.08.2020).

инфраструктуре

В случае с ФГИС Росстандарта, субъектом КИИ может быть «как юридическое лицо, которому ФГИС принадлежит на праве собственности – Федеральному агентству по техническому регулированию и метрологии, так и оператору информационной системы»[7].

В случае, когда оператор планирует расширение функциональных возможностей ИС, которое может повлечь за собой её отнесение (принадлежность) к КИИ, необходима проверка (изменение) правоустанавливающих документов оператора.

При проверке необходимо удостовериться, что сферы применения 187-ФЗ указанные в Уставе организации-оператора (раздел «Цели и предмет деятельности предприятия») и в Едином государственном реестре юридических лиц (ОКВЭД – Общероссийский классификатор видов экономической деятельности) имеют место.

В данном случае предполагается, что расширение функциональных возможностей ФГИС будет касаться области транспорта и/или связи. Так как у оператора в правоустанавливающих документах данные сферы деятельности отсутствуют, следовательно, необходимо запланировать внесение в них изменений.

Помимо внесения изменений в правоустанавливающие документы, рекомендуется издать внутренний нормативный акт оператора (приказ, распоряжение), подтверждающий планируемое расширение функциональных возможностей эксплуатируемой ИС с подтверждением принадлежности в этом случае к элементам КИИ.

2.2 Содержание работ по категорированию объектов критической информационной инфраструктуры

Структурная схема работ по категорированию объектов КИИ ФСТЭК России приведена на рис. 1 [14]. В соответствии с п. 5[8], процесс категорирования включает :

– определение процессов, выполняющихся в рамках реализации функций субъекта КИИ, а именно:

а) управленческих процессов;

б) технологических процессов;

в) производственных процессов;

г) финансово-экономических процессов;

д) иных процессов.

– выявление среди перечисленных выше так называемых критических процессов, то есть тех, нарушение штатного режима функционирования которых или полное прекращение функционирования может привести к негативным последствиям:

а) в социальной сфере;

б) в политической жизни;

в) в сфере экологии;

г) в экономике государства;

д) в сфере обеспечения обороноспособности и безопасности;

е) в области поддержания правопорядка.

– «выявление объектов КИИ, которые обрабатывают информацию, необходимую для обеспечения функционирования критических процессов, а также могут ими управлять

[7]Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

[8]Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

или их контролировать»;

– «создание перечня объектов КИИ, которые подлежат категорированию»;

– «в соответствии с перечнем показателей критериев значимости, оценка масштаба последствий к которым могут привести инциденты ИБ на объектах КИИ»;

– «присвоение каждому из объектов КИИ соответствующей категории значимости (возможно представление обоснованного решения об отсутствии необходимости присвоения категорий)».

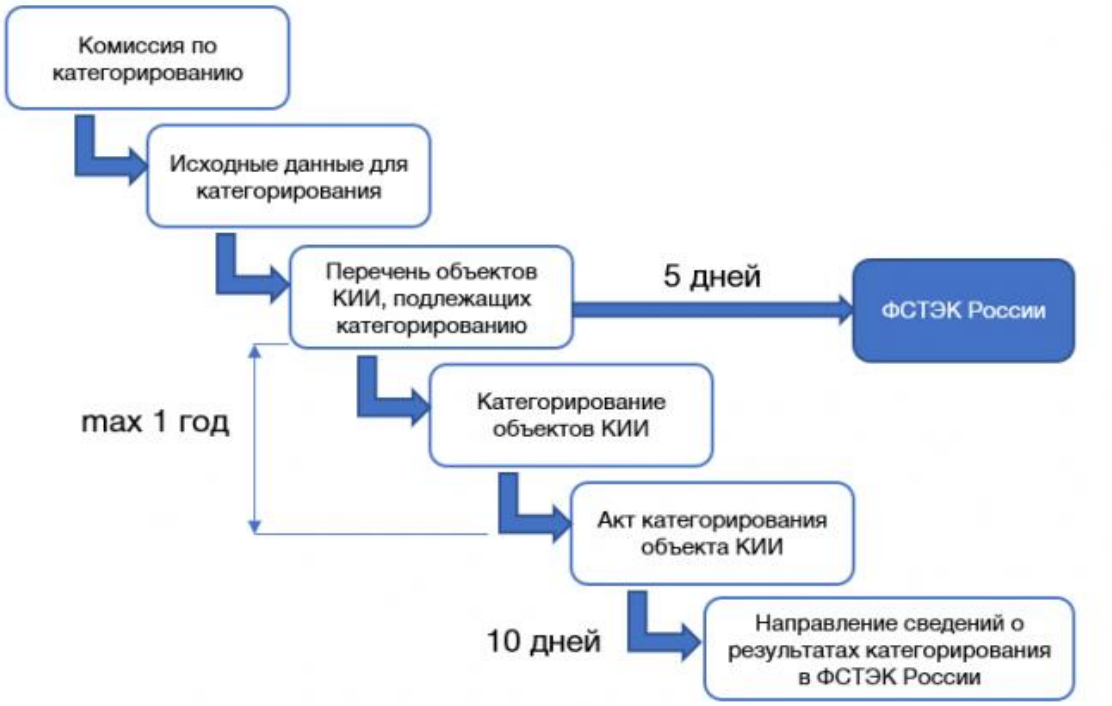

Рис. 1. Схема категорирования объектов КИИ
(Fig. 1. The scheme of categorization of objects CII)

По результатам исследований, ГИС находятся на первом месте среди прочих объектов целенаправленных компьютерных атак (APT), где злоумышленника интересует конкретная компания или государственная организация. Так, отмечено, «главное – это преобладание целенаправленных атак над массовыми атаками, и их доля составила 65% против 59% во II квартале [4].

Наибольший интерес для злоумышленников представляют *государственные учреждения*, промышленные компании, финансовый сектор и сфера науки и образования» [15]. Категории объектов компьютерных атак представлены на рис. 2.

В III квартале 2019 г. доля кибератак, направленных на кражу информации, выросла до 61% в атаках на юридические лица и до 64% в атаках на частных лиц (58% и 55% во втором квартале) [15]. При этом доля финансово мотивированных кампаний не превышает 31%.

Как указано Игорем Ляпуновым на BIS Summit Ekaterinburg, вице-президентом ПАО «Ростелеком» по информационной безопасности [16], «Существенно вырастет число атак, направленных на объекты КИИ и органы государственной власти, в том числе со стороны профессиональных группировок с инструментарием уровня government-stated» или «У атак на объекты КИИ нет монетизации, их задача – *получить контроль над инфраструктурой*».

Прогнозы на 2020 год для ГИС эту тенденцию сохранили [17], [18]: «Атак на критическую инфраструктуру будет больше – в этом сходятся во мнении эксперты *Group-IB, Trend Micro* и *Chronicle*. Промышленный шпионаж, атаки с помощью традиционного вредоносного ПО или вымогателей, атаки на цепочки поставок – варианты могут быть различны [17]. Атаки ожидаются как на предприятия энергетики, промышленные системы и системы жизнеобеспечения, так и на *ресурсы государственной власти*» и т.д.

Рис. 2. Категории объектов компьютерных атак
(Fig. 2. Categories of objects of computer attacks)

3. ГИС, как объект компьютерных атак в условиях неопределенности

3.1 Тенденция к увеличению использования понятия неопределённости

Заметно, что число работ, использующих термин «неопределенность», постоянно растёт. Подтверждением данного утверждения служат результаты анализа публикационной активности.

3.2 Анализ публикационной активности

Анализ публикационной активности отечественных ученых и специалистов по теме неопределенности проводился по Российскому индексу научного цитирования (РИНЦ)». Рассмотренная «база научных публикаций ScienceDirect», которая составляет основу, индекса научного цитирования Scopus является тому подтверждением. Например, динамика зарубежных научных публикаций по теме «неопределенность» с 1991 по 2011 гг.

Согласно другим источникам интерес к данной тематике до 2019 г. не пропал и количество научных публикаций по теме «неопределенность» не уменьшилась.

3.3 Введение понятия «неопределённости».

Впервые понятие неопределённости было упомянуто [20] при формулировании понятия «информация». Информация, в соответствии с [20] – «”нечто”, что уменьшает неопределённость», т.е. в первоначальном смысле она являлась некоей мерой информации.

В настоящее время общепризнанного определения данного понятия, пусть даже в какой-либо отдельной области нет. В рамках настоящей работы под неопределённостью предполагается понимать «отсутствие или недостаток информации о чём-либо».

3.3.1 Классификация неопределённости

Для целей настоящего исследования будем использовать классификацию, приведенную в [21]. В настоящее время различают неопределенность *трех видов* (родов):

– «неопределенность среды или первого рода»;

– «неопределенность выбора принятия решения или второго рода»;

– «неопределенность будущей реализации принятого решения, она же третьего рода» [21].

Неопределенность 1-го рода – это неопределённость разнообразия и нестабильности окружающей среды. Данный род неопределенности не подчиняется наблюдателям или лицам, принимающим решение. Это – непрогнозируемое изменение внешних условий.

Неопределенность 2-го рода – это неопределённость выбора решения при необходимости его принятия.

Неопределенность 3-го рода – это неопределённость реализации принятого решения и последствий, наступающих после его принятия.

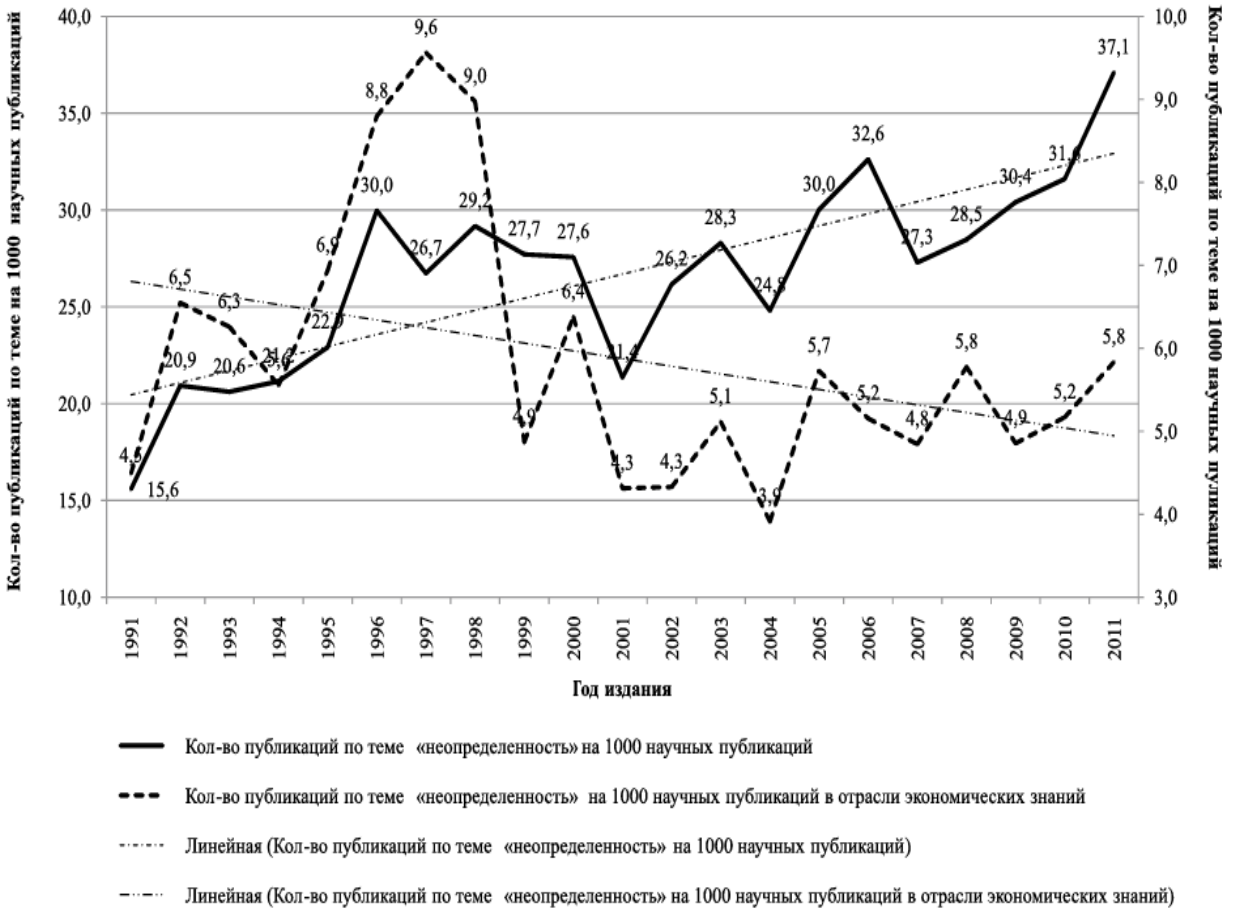

Рис. 3. Динамика зарубежных научных публикаций по теме «неопределенность» с 1991 по 2011 гг. по тематической направленности
(Fig. 3. Dynamics of foreign scientific publications on the topic «uncertainty» from 1991 to 2011 by thematic focus)

3.4 Неопределённость при обеспечении безопасности информации

Применительно к обеспечению безопасности информации термин неопределённость можно использовать следующим образом.

3.4.1 Неопределённости первого рода

К неопределённости первого рода или среды целесообразно отнести неопределённости, возникающие при несоответствии требований НПА как одних к другим, так и внешним условиям.

Проиллюстрировать несоответствие требований различных НПА можно сопоставлением[9,10,11] в части состава мер защиты информации.

К примеру, мера с кодом ЗИС. 21[8,9] сформулирована как «Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и т.п.», а в другом[10] как «Запрет несанкционированной удаленной активации периферийных устройств» и т.д. В качестве примера несоответствия внешним условиям, можно привести используемые для оценки угроз[9,12]. В обоих документах ставится задача уменьшения субъективности и неопределённости экспертных оценок, при отсутствии перечня конкретных мер по реализации. Также к неопределённости первого рода целесообразно отнести быстро меняющуюся ситуацию с разработкой и внедрением новых технологий. В [22] отмечено, что «Эпоха интернета и больших данных несет с собой поток информации, которую можно использовать для принятия решений. В этой ситуации проблемой для своевременного и точного принятия решений является уже не отсутствие информации, а риск невозможности понимания и управления присущей ей неопределенностью, возникающей из-за ненадежности, неполноты, обманчивости и её противоречивости» [22].

Данное обстоятельство ведёт к неопределённости второго рода – формирования решения.

3.4.2 Неопределённости второго рода

При повсеместном стремлении руководства нашего государства к внедрению так называемой цифровой экономики, которая формулируется, как хозяйственная деятельность важно помнить о том, что перегибы во всех областях к хорошим результатам никогда не приводили. Ключевым фактором производства здесь являются данные в цифровом виде (обработки больших объемов и использования результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг)»[13], где неопределённости первого рода возрастают. Например, там же упоминаются туманные вычисления, для которых отсутствует нормативная база по обеспечению безопасности информации. Более простой пример: как, при формировании модели угроз, определить границы защищаемого объекта, если часть вычислений выполняется в облаке.

3.4.3 Неопределённости третьего рода

[9]Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 28.05.2019) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

[10]Приказ ФСТЭК России от 14.03.2014 № 31 (ред. от 09.08.2018) «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

[11]Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ».

[12]Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России, 2008.

[13]Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы».

К неопределенности третьего рода или неопределённость реализации принятого решения и последствий, наступающих после его принятия целесообразно отнести эксплуатацию информационной системы в условиях вредоносных воздействий. Изучение данного вида неопределённости выходит за пределы темы настоящей работы.

3.4.4 Учёт неопределённости при обеспечении безопасности информации

При наличии неопределённостей первого и второго рода, становится актуальной задача их учёта при обеспечении безопасности информации в ГИС.

Для этого, с учётом неопределённостей, необходимы как разработка математической модели угроз (МУ) безопасности информации, так и проекта методики, позволяющего оценить угрозы безопасности информации в ГИС.

Для постановки задачи можно использовать формулировку: «необходимо разработать методику М, позволяющую по множеству исходных данных сформировать множество актуальных угроз **Ω*** и получить значения субъективной вероятности p(ω) реализации каждой из угроз безопасности информации (УБИ), при этом неопределенность H(**Ω***) состояния безопасности информации в информационной системе с применением методики М должна быть меньше, чем та же неопределенность, но без применения методики М» [23].

3.5 Разработка методики оценки угроз безопасности информации в ГИС

При наличии неопределённостей первого и второго рода, становится актуальной задача их учёта при обеспечении безопасности информации ГИС. Данный проект методики оценки угроз безопасности информации в ГИС предусматривает меры по снижению неопределенности при оценке угроз. В рамках работы ГИС считается автоматизированной системой (АС), созданной в защищённом исполнении.

В соответствии с п. 5.9[14], стадии создания подобной АС соответствуют требованиям документа по стандартизации[15].

3.5.1 Особенности стадий создания информационных систем

Методика содержит перечень работ, выполняемых на следующих стадиях создания ИС[13]:

– «формирования требований к АС»;
– «разработки концепции АС»;
– «техническое задание на создание АС»;
– «эскизный проект АС»;
– «технический проект АС»;
– «рабочая документация на АС»;
– «ввод АС в действие»;
– «сопровождение АС».

При этом создаваемая МУ используется на всех стадиях жизненного цикла ИС.

3.5.2 Снижение неопределённости при моделировании угроз

Создание множества УБИ ГИС (в работе) выполняется на основании исследования выбранных угроз из БДУ ФСТЭК России (*https://bdu.fstec.ru/threat*), анализа используемого в информационной системе программного обеспечения и сопоставления совпадений с использованием экспертных оценок для оценки реализуемости этих угроз.

[14]ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения – Москва. ФГУП «СТАНДАРТИНФОРМ», 2018.
[15]ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» – Москва. ФГУП «СТАНДАРТИНФОРМ», 2009.

При этом угрозы, признанные нереализуемыми, остаются в создаваемой БДУ с присвоением числового показателя, оповещающего о нереализуемости. На каждом этапе создания должна происходить переоценка показателей реализуемости угроз.

3.5.2.1 Снижение неопределенности на этапе формирования требований, разработки концепции и создания технического задания на создание АС.

На данном этапе снижение неопределённости первого рода выполняется:

– формированием баз данных угроз в соответствии с [24];

– экспертной оценкой каждой УБИ из сформированной модели МУ с присвоением признака реализуемости.

Снижение неопределённости второго рода выполняется использованием для формирования экспертного мнения группы экспертов с принятием согласованного решения по каждой УБИ.

3.5.2.2 Снижение неопределенности на этапе создания эскизного и технического проектов и разработки рабочей документации АС.

На данном этапе снижение неопределённости первого рода выполняется:

– актуализацией созданной МУ в соответствии с выбранными БДУ;

– экспертной оценкой каждой УБИ из сформированной МУ с присвоением признака реализуемости.

Снижение неопределённости второго рода выполняется использованием для формирования экспертного мнения группы экспертов с принятием согласованного решения по каждой УБИ.

3.5.2.3 Снижение неопределенности на этапе ввода в действие и эксплуатации АС.

На данном этапе снижение неопределённости первого рода выполняется:

– актуализацией созданной МУ в соответствии с выбранными БДУ и актуальными НПА и методическими документами;

– экспертной оценкой каждой УБИ из сформированной БДУ с присвоением признака реализуемости;

Снижение неопределённости второго рода выполняется выполнением проведением тестирования на проникновение для АС с корректировкой созданной МУ.

Следует отметить отсутствие в ряде исходных данных однозначного соответствия с источниками реестра угроз, упомянутых ранее. Здесь важно помнить, что:

– практическое использование любых моделей оценки уязвимости упирается в ограничения (неполнота и недостоверность исходных данных);

– правильно поставленная работа с исходными данными в условиях их неопределенности является ключевым моментом в решении любых задач, связанных с обеспечением ИБ не только ГИС;

– принципиальным моментом практической реализации является построение адекватных моделей рассматриваемых систем (процессов).

Заключение

Анализ эксплуатируемых информационных фондов (ИФ) органов государственной власти РФ выявляет наиболее характерные тенденции проблемного характера, имеющие распространение на:

– информационные ресурсы, информационные системы и ГИС;

– объекты информатизации органов государственной власти РФ и субъектов РФ и др.

Результаты анализа и их оценка состояния эксплуатируемых информационных фондов позволяет сделать выводы, на основании которых можно сказать, что необходима методика оценки угроз безопасности информации ГИС, которая бы предусматривала меры по снижению неопределенности при оценке этих угроз. Для постановки задачи в работе использовалась формулировка: «необходимо разработать методику, позволяющую по множеству исходных данных сформировать множество актуальных угроз и получить значения субъективной вероятности реализации каждой угрозы БИ. При этом важно, чтобы неопределенность $H(\Omega^*)$ состояния безопасности информации в ИС с применением методики M должна быть меньше, чем та же неопределенность, но без применения методики M». Для решения такой задачи требуется учитывать много факторов, например, к основным можно отнести:

- вероятности возникновения различных угроз информации;
- стоимость реализации способов и средств ЗИ;
- наличие заинтересованных сторон;
- подготовка персонала по защите информации ГИС.

Вывод. Выбор методов, способов и средств защиты информации в ГИС является достаточно сложной оптимизационной задачей. Поэтому правильно поставленная работа с исходными данными (для проведения исследования) в условиях высокой степени их неопределенности является ключевым моментом в решении любых задач, связанных с обеспечением информационной безопасности, в том числе и ГИС.

СПИСОК ЛИТЕРАТУРЫ:

1. Ахромеева Т.С., Малинецкий Г.Г., Посашков С.А. Стратегии и риски цифровой реальности // Стратегические приоритеты. 2017. № 2 (14). С. 88–102. URL: http://sec.chgik.ru/ctrategii-i-riski-tsifrovoy-realnosti/ (дата обращения: 20.09.2020).
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, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1200/1145/ (дата обращения: 20.08.2020). DOI: http://dx.doi.org/10.26583/bit.2019.2.05.
3. 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: 24.09.2020).
4. Статистические данные о зарегистрированных преступлениях на территории Российской Федерации в январе–августе 2019 года. URL: https://genproc.gov.ru/smi/news/genproc/news-1703326// (дата обращения: 20.11.2019).
5. Пенерджи, Рустем В.; Гавдан, Григорий П. Информационная безопасность государственных информационных систем. Безопасность информационных технологий, [S.l.]. Т. 27, №. 3. С. 26–42, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1290 (дата обращения: 25.10.2020). DOI: http://dx.doi.org/10.26583/bit.2020.3.03.
6. Рудницкий Е. Поведенческий анализ для защиты инфраструктуры: хакеры и коронавирус меняют рынок ИБ решений. URL: http://www.itsec.ru/articles/povedencheskij-analiz-dlya-zashchity-infrastruktury-hakery-i-koronavirus-menyayut-rynok-ib-reshenij?utm_medium=email&_hsmi=98246397&_hsenc=p2ANqtz-8Lx6jOBvC9ynjJlcgSG0fIaacWQafeSfWuo7a8edWxKBXjnbS4e-Sw8S_rlu52-lyunSBIVR3N0qFsxRHV5YcWuqH2aQ&utm_content=98246397&utm_source=hs_email (дата обращения: 26.10.2020).
7. Жумаева А.П., Ялбаева В.А., Селифанов В.В., Макарова Д.Г., Звягинцева П.А., Чернов Д.В. О выборе средств защиты информации для государственных информационных систем. Известия Тульского государственного университета. Технические науки. 2018. №10. С. 52–58. URL: https://www.elibrary.ru/item.asp?id=36617998/ (дата обращения: 28.09.2020).
8. 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, 2020. ISSN 2074-7136.

URL: https://bit.mephi.ru/index.php/bit/article/view/1268/1187. (дата обращения: 03.09.20200). DOI: http://dx.doi.org/10.26583/bit.2020.2.02.

9. Рябова В. Китай признал существование кибервойск. D-Russir.ru. URL: https://d-russia.ru/kitaj-priznal-sushhestvovanie-kibervojsk.html (дата обращения: 09.08.2020).
10. 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: 04.09.2019).
11. 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: 02.09.2020).
12. 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: 02.09.2020).
13. Гавдан, Григорий П.; Иваненко, Виталий Г.; Салкуцан, Алексей а. Обеспечение безопасности значимых объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.]. Т. 26, № 4. С. 69–82, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1232/1165 (дата обращения: 03.09.2020). DOI: http://dx.doi.org/10.26583/bit.2019.4.05.
14. Щелкачев И.В. Правила категорирования объектов КИИ РФ. URL: https://d-russia.ru/wp-content/uploads/2018/06/2_pravila_kategorirovaniya_obektov_kii.pdf (дата обращения: 26.09.2020).
15. Positive Technologies: «Кибератаки все чаще носят целенаправленный характер». Итоги третьего квартала 2019 года. Журнал ПЛАС. По материалам Positive Technologies. URL: https://plusworld.ru/daily/cat-security-and-id/positive-technologies-kiberataki-vse-chashhe-nosyat-tselenapravlennyj-harakter/ (дата обращения: 26.09.2020).
16. Ляпунов И. Кибер атаки на критически важные для РФ объекты участились в десятки раз. РБК. ДИП. URL: https://www.rbc.ru/ekb/13/02/2019/5c641f829a794756010d719d (дата обращения: 27.09.2020). R-Vision. Прогнозы по информационной безопасности на 2020 года.
17. Anti-Malware.ru «Прогноз развития киберугроз и средств защиты информации 2020» URL: https://www.anti-malware.ru/analytics/Threats_Analysis/cyber-threats-and-security-tools-evolving-2020-forecast/ (дата обращения: 27.09.2020).
18. Кузьмин Е.А. Организационно-экономические системы в условиях неопределённости и определённости: оценка значений энтропии и негэнтропии // Управленец. 2012. № 11-12. С. 44–54. URL: https://cyberleninka.ru/article/n/organizatsionno-ekonomicheskie-sistemy-v-usloviyah-neopredelennosti-i-opredelennosti-otsenka-znacheniy-entropii-i-negentropii (дата обращения: 26.09.2020).
19. National initiative for cybersecurity education (NICE). URL: https://www.nist.gov/itl/applied-cybersecurity/nice. (дата обращения: 15.09.2020).
20. Авдийский В.И., Безденежных В.М. Неопределённость, изменчивость и противоречивость в задачах анализа рисков поведения экономических систем // Эффективное антикризисное управление. 2011. № 3. С. 46–61. URL: https://elibrary.ru/item.asp?id=16753895 (дата обращения: 15.09.2020). eLIBRARY ID: 16753895.
21. Audun Jøsang, Jin-Hee Cho, Feng Chen. Uncertainty Characteristics of Subjective Opinions // Conference: 2018 International Conference on Information Fusion (FUSION). URL: https://www.duo.uio.no/bitstream/handle/10852/72014/JCC2018-FUSION.pdf?sequence=1 (дата обращения: 12.09.2020).
22. Ильченко А.Н. Математическая модель и методика оценки угроз безопасности информации в информационной системе в условиях неопределенности. С. 60–65 // Сборник докладов XXIII пленума ФУМО ВО ИБ и Всероссийской научной конференции "Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации" (ИНФОБЕЗОПАСНОСТЬ -2019) (дата обращения: 15.06.2020).
23. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty (дата обращения: 15.09.2020).

REFERENCES:

[1] Akhromeeva TS, Malinetskiy G.G., Posashkov S.A. Strategies and risks of digital reality. Strategic priorities. 2017. № 2(14). P. 88–102. URL: http://sec.chgik.ru/ctrategii-i-riski-tsifrovoy-realnosti/ (accessed: 20.09.2020) (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, no. 2. P. 67–85, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1200 (accessed: 20.08.2020). DOI: http://dx.doi.org/10.26583/bit.2019.2.05. (in Russian).

[3] Positive Technologies report: Current cyber threats: Q2 2019. Positive Technologies URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2019-Q2-rus.pdf. (accessed: 24.09.2020) (in Russian).

[4] Statisticheskiye dannyye o zaregistrirovannykh prestupleniyakh na territorii Rossiyskoy Federatsii v yanvare–avguste 2019. URL: https://genproc.gov.ru/smi/news/genproc/news-1703326/. (accessed: 20.09.2020).

[5] Penerdji, Rustem V.; Gavdan, Grigory P. Information security of state information systems. IT Security (Russia), [S.l.]. V. 27, no. 3. P. 26–42, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1290 (accessed: 25.10.2020). DOI: http://dx.doi.org/10.26583/bit.2020.3.0 (in Russian).

[6] Rudnitskiy E. Povedencheskiy analiz dlya zashchity infrastruktury: khakery i koronavirus menyayut rynok IB resheniy. URL: http://www.itsec.ru/articles/povedencheskij-analiz-dlya-zashchity-infrastruktury-hakery-i-koronavirus-menyayut-rynok-ib-reshenij?utm_medium=email&_hsmi=98246397&_hsenc=p2ANqtz-8Lx6jOBvC9ynjJlcgSG0fIaacWQafeSfWuo7a8edWxKBXjnbS4e-Sw8S_rlu52-lyunSBIVR3N0qFsxRHV5YcWuqH2aQ&utm_content=98246397&utm_source=hs_email (accessed: 26.10.2020) (in Russian).

[7] Zhumaeva A.P., Erbaeva V.A., Selifanov V.V., Makarov G.D., Zvyagintsev P.A., Chernov D.V. On the choice of means of information security for government information systems. Izvestiya Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki. 2018. №. 10. P. 52–58. URL: https://www.elibrary.ru/item.asp?id=36617998 (accessed: 28.09.2020) (in Russian).

[8] Salkutsan, Alexei A.; Gavdan, Grigory P.; Poluyanov, Andrey A. The methodology for critical processes identifying at information infrastructure facilities. IT Security (Russia), [S.l.]. V. 27, no. 2. P. 18–34, 2020. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1268/1187 (accessed: 09.08.2020). DOI: http://dx.doi.org/10.26583/bit.2020.2.02 (in Russian).

[9] Ryabova V. Kitay priznal sushchestvovaniye kibervoysk. D-Russir.ru. URL: https://d-russia.ru/kitaj-priznal-sushhestvovanie-kibervojsk.html (accessed: 09.08.2020) (in Russian).

[10] 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: 04.09.2019).

[11] 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: 02.09.2020).

[12] 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: 02.09.2020).

[13] Gavdan, Grigory P.; Ivanenko, Vitaliy G.; Salkutsan, Alexei A. Security of significant objects ofcritical information infrastructure. IT Security (Russia), [S.l.]. V. 26, no. 4. P. 69–82, 2019. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1232 (accessed: 03.09.2020). DOI: http://dx.doi.org/10.26583/bit.2019.4.05 (in Russian).

[14] Shchelkachev I.V. Pravila kategorirovaniya obyektov CII RF of the Russian Federation. URL: https://d-russia.ru/wp-content/uploads/2018/06/2_pravila_kategorirovaniya_obektov_kii.pdf. (accessed: 26.09.2020). (in Russian).

[15] Positive Technologies: «Kiberataki vse chashche nosyat tselenapravlennyy kharakter». Itogi tretyego kvartala 2019. PLUS Journal. On materials Positive Technologies. URL: https://plusworld.ru/daily/cat-security-and-id/positive-technologies-kiberataki-vse-chashhe-nosyat-tselenapravlennyj-harakter/ (accessed: 26.09.2020).

[16] Lyapunov I. Kiber-ataki na kriticheski vazhnyye dlya of the Russian Federation obyekty uchastilis v desyatki raz. RBK. DIP. URL: https://www.rbc.ru/ekb/13/02/2019/5c641f829a794756010d719d (accessed: 27.09.2020). R-Vision. Prognozy po informatsionnoy bezopasnosti na 2020. (in Russian).

[17] Anti-Malware.ru «Prognoz razvitiya kiberugroz i sredstv zashchity informatsii 2020». URL: https://www.anti-malware.ru/analytics/Threats_Analysis/cyber-threats-and-security-tools-evolving-2020-forecast/ (accessed: 27.09.2020).

[18] Kuzmin E.A. Organizatsionno-ekonomicheskiye sistemy v usloviyakh neopredelennosti i opredelennosti: otsenka znacheniy entropii i negentropii. Upravlenets. 2012. № 11-12. S. 44–54. URL: https://cyberleninka.ru/article/n/organizatsionno-ekonomicheskie-sistemy-v-usloviyah-neopredelennosti-i-opredelennosti-otsenka-znacheniy-entropii-i-negentropii (accessed: 26.09.2020) (in Russian).

[19] National initiative for cybersecurity education (NICE) Workforce Framework Cybersecurity. NICCS. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf (accessed: 15.09.2020).

[20] Avdiyskiy V.I. Bezdenezhnykh V.M. Neopredelennost, izmenchivost i protivorechivost v zadachakh analiza riskov povedeniya ekonomicheskikh sistem // Effektivnoye antikrizisnoye upravleniye. 2011. № 3. S. 46–61. URL: https://elibrary.ru/item.asp?id=16753895 (accessed: 15.09.2020). eLIBRARY ID: 16753895. (in Russian).

[21] Audun Jøsang, Jin-Hee Cho, Feng Chen. Uncertainty Characteristics of Subjective Opinions // Conference: 2018 International Conference on Information Fusion (FUSION). URL: https://www.duo.uio.no/bitstream/handle/10852/72014/JCC2018-FUSION.pdf?sequence=1 (accessed: 12.09.2020).

[22] Ilchenko A.N. Matematicheskaya model i metodika otsenki ugroz bezopasnosti informatsii v informatsionnoy sisteme v usloviyakh neopredelennosti. S. 60-65. Sbornik dokladov XXIII plenuma FUMO VO IB i Vserossiyskoy nauchnoy konferentsii "Fundamentalnyye problemy informatsionnoy bezopasnosti v usloviyakh tsifrovoy transformatsii" (INFOBEZOPASNOST -2019) (accessed: 15.06.2020) (in Russian).

[23] Bazovaya model ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty (accessed: 15.09.2020) (in Russian).

Поступила в редакцию – 27 октября 2020 г. Окончательный вариант – 09 ноября2020 г.
Received – October 27, 2020. The final version – November 09, 2020.