Олег Г. Евдокимов[1], Григорий П. Гавдан[2], Сергей А. Резниченко[3]
[1]Управление ФСТЭК России по Центральному федеральному округу,
Севастопольский пр-кт, 56/40, Москва, 117342, Россия
[1,2,3]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[3]Финансовый университет при правительстве Российской Федерации,
Ленинградский пр-кт, 49, Москва, 125993, Россия
[3]Российский государственный университет нефти и газа (НИУ) им. И.М. Губкина,
Ленинский пр-кт, 65, корпус 1, Москва, 119991, Россия
[3]Российский государственный гуманитарный университет,
Миусская площадь, 6, Москва, 125047, Россия
[1]e-mail: okei67@mail.ru, https://orcid.org/0000-0001-5801-3638
[2]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[3]e-mail: rsa_5@bk.ru, https://orcid.org/0000-0002-1539-0457

ПОДХОД К ОЦЕНКЕ ЭФФЕКТИВНОСТИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ

DOI: http://dx.doi.org/10.26583/bit.2022.2.05

Аннотация. Целью статьи является определение возможных подходов к оценке эффективности системы обеспечения информационной безопасности (СОИБ) распределенной системы передачи данных (РСПД), относящейся к значимому объекту критической информационной инфраструктурой. При разработке СОИБ, необходимо уже на этапе проектирования архитектуры РСПД выявить возможные внешние и внутренние источники угроз безопасности информации, разработать модель нарушителя и модель угроз информационной безопасности (ИБ). Одной из основных проблем в создании СОИБ РСПД является отсутствие и/или недостаточная подготовка кадров в области ИБ; большая финансовая нагрузка на создание и модернизацию аппаратно-программных средств и др. В качестве исследуемой СОИБ РСПД предложена модель РСПД (структурная схема РСПД и схема размещения компонентов СОИБ на специальной вычислительной технике). В работе предложен подход к оценке эффективности СОИБ РСПД основанный на использовании метода экспертных оценок для выбранной модели, что необходимо для достижения требуемого уровня безопасности. Рассмотрены аспекты по оценке эффективности СОИБ РСПД на примере организации технических мер обеспечения ИБ РСПД. Данная оценка эффективности СОИБ РСПД позволяет выявить слабые места и поможет оперативно принять меры к их устранению, что при возникновении компьютерных атак или инцидентов может существенно снизить риски. Предложенный подход можно интегрировать в существующие практики оценки эффективности ИБ.

Ключевые слова: информационная безопасность, объект критической информационной инфраструктуры, передача данных, распределенная система, система обеспечения информационной безопасности.

Для цитирования: ЕВДОКИМОВ, Олег Г.; ГАВДАН, Григорий П.; РЕЗНИЧЕНКО, Сергей А. ПОДХОД К ОЦЕНКЕ ЭФФЕКТИВНОСТИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ. Безопасность информационных технологий, [S.l.], т. 29, № 2, с. 57–70, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1418. DOI: http://dx.doi.org/10.26583/bit.2022.2.05.

Oleg G. Evdokimov[1], Grigory P. Gavdan[2], Sergey A. Reznichenko[3]
[1]The Department of the FSTEC of Russia for the Central Federal District,
Sevastopol Avenue, 56/40, Moscow, 117342, Russia
[1,2,3]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia
[3]Financial University under the Government of the Russian Federation,
Leningradsky Avenue, 49, Moscow, 125993, Russia
[3]Gubkin Russian State University of Oil and Gas (National Research University),

Leninsky Avenue, 65, building 1, Moscow, 119991, Russia
[3]Russian State University for the Humanities,
Miusskaya Square, 6, Moscow, 125047, Russia
[1]e-mail: okei67@mail.ru, https://orcid.org/0000-0001-5801-3638
[2]e-mail: GPGavdan@mephi.ru, https://orcid.org/0000-0003-3185-3076
[3]e-mail: rsa_5@bk.ru, https://orcid.org/0000-0002-1539-0457

An approach to evaluating the effectiveness of the information security system for a distributed data transmission system

DOI: http://dx.doi.org/10.26583/bit.2022.2.05

Abstract. The purpose of the paper is to identify possible approaches to assessing the effectiveness of the information security system (EISS) for a distributed data transmission system (DDTS) related to a significant object of critical information infrastructure. When developing the EISS, it is necessary to identify possible external and internal sources of threats to information security already at the design stage of the DDTS architecture as well as to develop a model of the violator and a model of information security threats (IS). One of the main problems in the creation of EISS DDTS is the lack and/or insufficient training in the field of information security; a large financial burden on the creation and modernization of hardware and software, etc. The DDTS model (a block diagram of the DDTS and the layout of the components of the DDTS on special computing equipment) is proposed for the EISS DDTS under study. The paper proposes an approach to assessing the effectiveness of the EISS DDTS based on the use of the method of expert assessments for the selected model, which is necessary to achieve the required level of safety. The aspects of assessing the effectiveness of the EISS DDTS are considered using the example of the organization of technical measures to ensure the IB DDTS. This assessment of the effectiveness of the EISS DDTS allows you to identify weaknesses and help you quickly take measures to eliminate them, which in the event of computer attacks or incidents can significantly reduce the risks. The proposed approach can be integrated into existing practices for assessing the effectiveness of information security.

Key words: information security, object of critical information infrastructure, data transmission, distributed system, information security system.
For citation: EVDOKIMOV, Oleg G.; GAVDAN, Grigory P.; REZNICHENKO, Sergey A. An approach to evaluating the effectiveness of the information security system for a distributed data transmission system. IT Security (Russia), [S.l.], v. 29, no. 2, p. 57–70, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1418. DOI: http://dx.doi.org/10.26583/bit.2022.2.05.

Введение

За последние годы, как показывает практика, мировые державы продолжают уделять достаточно большое внимание обеспечению и поддержанию высокого уровня защиты информации (ЗИ), циркулирующей и используемой в таких областях, как цифровая экономика, обороноспособность государства, торгово-промышленные и топливно-энергетические направления, информационная инфраструктура, социальные сферы, средства массовой информации, мультимедиа и др.

Информация сегодня обязательная составляющая общественной жизни, но с другой стороны – это ценный продукт, который требует в значительной мере затрат на обеспечение её безопасности. Так, сети электросвязи, информационные системы (ИС), информационно-телекоммуникационные системы и сети (ИТКС), информационные инфраструктуры (ИИ), автоматизированные системы управления (АСУ) и АСУ технологическими процессами (АСУ ТП), на которые сегодня осуществляются компьютерные атаки могут прекратить своё функционирование и/или может сильно нарушится состояние их защищённости, чем наносится различной степени тяжести урон бизнес-процессу организации (предприятию, государству или личности). С появлением в

2017 г. ФЗ[1]-187 кроме систем необходимо отнести ещё и объекты ИС, ИТКС, АСУ субъектов критической информационной инфраструктуры (КИИ) и сети электросвязи, используемые для организации взаимодействия таких объектов.

Достаточно большой рост интереса к проблемам информационной безопасности (ИБ), в настоящее время связывают, прежде всего, с бурным развитием крупномасштабных распределённых информационных систем и сетей. Объекты, которые используют современные технологии, являются потенциальной мишенью для различных категорий злоумышленников, вооруженных специальными информационными технологиями новых поколений [1].

1. Преступные деяния злоумышленников в информационной инфраструктуре

Стремительное развитие и подъем ИТ в странах запада основывается на хорошем финансировании научно-исследовательских проектов различного вида направлений. Не секрет, что в США в настоящее время сосредоточены ведущие научно-технические кластеры Мира. Финансирование в гражданской и военной сфере с 2021 г. научных разработок не уменьшилось. Так, в США, благодаря развитию и внедрению своих научных разработок, значительный объем информационных технологий продаётся полным ходом за рубеж, тем самым, США остаётся абсолютным лидером в сфере ИТ [2].

Монополисты отвергают идею полного своего управления информационными потоками, циркулирующими в среде «Internet», перед другими государствами и наднациональным органом организации объединённых наций (ООН), отстаивая тем самым свои интересы (в том числе интересы и коммерческих структур подконтрольных администрации). Монография Елина В.М. [2] является тому подтверждением, в ней рассмотрены проблемы обеспечения ИБ как составной части национальной безопасности, проводится подробный анализ законодательных актов Российской Федерации и зарубежных государств в области ИБ. В анализе законодательных актов зарубежных государств делается акцент на доминирующее положение США в киберпространстве современного Мира [3], а значит право [4] на информационное пространство практически полностью ими монополизировано.

В сфере киберпространства [5], во многих странах мира, продолжается рост различного уровня и масштаба преступных деяния [5]. Не являются исключением и значимые объекты КИИ (ЗОКИИ). При возникновении (в информационном пространстве) какого-либо рода или вида конфликтов они могут и становятся для атакующей стороны основной целью.

Вступивший в январе 2018 г. в силу Федеральный закон № 187-ФЗ вызвал множество дискуссий со стороны субъектов КИИ [6], в то же время, как в периодической научной и технической литературе вопросы обеспечения безопасности ЗОКИИ пока ещё не получили должного освещения. Работа научными работниками и государственными служащими ведётся, о чём свидетельствуют (новые) публикации, выступления на форумах и принятие новых нормативно правовых документов РФ[2,3] в области КИИ и ИБ.

---

[1]Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ. Закон вступил в силу с 1 января 2018 г. URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 20.02.2022).

[2]Указ Президента Российской Федерации «О Межведомственной комиссии Совета Безопасности Российской Федерации по вопросам обеспечения технологического суверенитета государства в сфере развития критической информационной инфраструктуры Российской Федерации» от 14.04.2022 № 203. URL: http://publication.pravo.gov.ru/Document/View/0001202204140035 (дата обращения: 25.04.2022).

[3]Указ Президента Российской Федерации «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» от 01.05.2022 № 250. URL: http://publication.pravo.gov.ru/Document/View/0001202205010023?index=0&rangeSize=1 (дата обращения: 25.04.2022).

Обеспечение ИБ в России регулируются нормативными правовыми актами, в которых отражаются основные компоненты стратегии; представляются системы норм и требований по обеспечению национальной безопасности в сфере информации и её комплексной защиты. Рассматривая и анализируя нормативные правовые акты, можно уверенно сказать, что информационная борьба — это реальность. В данном контексте такую информацию можно и необходимо рассматривать как элемент национальной безопасности (Государства). Объектом информационного воздействия в настоящее время может стать любая ИС, ИТКС, ИИ, АСУ и др. Информационные системы – это достаточно сложный «механизм», который состоит из различных элементов, связанных между собой и осуществляющими различные виды обмена данными. Данные элементы можно разделить на такие группы, как аппаратная часть; программное обеспечение; персонал.

Отражение или предотвращение угроз и вызовов со стороны некоторых государств блока НАТО (США, Евросоюза и др.) в сфере ИБ – неотъемлемая часть национальной безопасности государства. В современных условиях значительно меняются формы, методы и средства борьбы. Задача обеспечения ИБ (ОБИ) приобретает особое значение. В информационном пространстве эти угрозы касаются всех сфер жизнедеятельности как отдельно взятого человека, так и любого государства в целом. Важным вопросом, как для частных лиц, организаций, предприятий, компаний, так и для любого государства является создание, получение, обработка, сохранение и передача информации, доступной ограниченному кругу лиц.

Многие организации России, и в первую очередь Федеральная служба по техническому и экспертному контролю (ФСТЭК России), продолжают активно участвовать в разработке и внесении изменений в подзаконные акты в сфере обеспечения безопасности КИИ, чтобы в должной мере субъекты обеспечили безопасность своих ЗОКИИ на всей территории РФ[4,5,6,7,8].

По данным Национального координационного центра по компьютерным инцидентам (НКЦКИ) США и Евросоюз являются основными источниками компьютерных атак [7].

[4]Приказ ФСТЭК России от 27.03.2019 № 64 «О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. № 235». URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/288-prikazy/1882-prikaz-fstek-rossii-ot-27-marta-2019-g-n-64 (дата обращения: 20.03.2022).

[5]Приказ ФСТЭК России №59 от 21.03.2019 «О внесении изменений в форму направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, утвержденную приказом ФСТЭК №236 от 22.12.2017». URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/288-prikazy/1864-prikaz-fstek-rossii-ot-21-marta-2019-g-n-59 (дата обращения: 21.04.2022).

[6]Приказ ФСТЭК России №60 от 26.03.2019 «О внесении изменений в Требования по обеспечению безопасности значимых объектов КИИ РФ, утвержденные приказом ФСТЭК №239 от 25.12.2017». URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/288-prikazy/1865-prikaz-fstek-rossii-ot-26-marta-2019-g-n-60 (дата обращения: 20.02.2022).

[7]Федеральный закон от 26.07.2017 № 193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации». URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/285-zakony/1705-federalnyj-zakon-ot-26-iyulya-2017-g-n-193-fz (дата обращения: 20.02.2022).

[8]Постановление Правительства Российской Федерации от 13 апреля 2019 г. № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127». URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/287-postanovleniya/1863-postanovlenie-pravitelstva-rossijskoj-federatsii-ot-13-aprelya-2019-g-n-452 (дата обращения: 20.02.2022).

Различные хакерские группировки получают на ведение своей незаконной деятельности спонсорскую поддержку от разного уровня структур. Для совершения таких кибератак злоумышленниками используются специальное кибернетическое наступательное оружие, которое предоставляет уникальные возможности по созданию деструктивного эффекта в нанесении максимального экономического ущерба субъекту атаки [8]. Как отмечают авторы [9]: «Кибервойна уже началась. Всё чаще хакеры проникают в сети и инфраструктуру, припасают на будущее «черные ходы» и логические бомбы, и делают это уже сейчас, в мирное время». Мехтиева Н.Р. в статье «Информационные войны как «цифровой» аспект глобализации» [10] пишет: «Субъектами противостояния в кибервойне оказываются как отдельные государства, целенаправленно стремящиеся избежать военного столкновения путем перевода противоборства в информационную плоскость, так и анонимные интернет-сообщества, проводящие хакерские атаки против различных государств, их политических, экономических или информационных институтов».

Правительство России по госпрограммам и непрограммным направлениям осуществляет расходы на научные исследования и разработки для аналитической «группировки». Из этих документов следует, что в 2021 г. государство больше всего направило на исследования по программе «Научно-технологическое развитие России» (НТР) – 249 млрд руб. [11], примерно 51% от общего «исследовательского» бюджета.

В рамках программы НТР в 2021 г. по объему финансирования исследований госпрограмма «Космическая деятельность России» получит 82,3 млрд руб. (с увеличением до 85-86 млрд руб. в 2022–2023 гг.).

2022 г. планируется проводить различные направления господдержки бизнеса во многих секторах экономики и производства. Некоторые из них уже приняты, другие – пока обсуждаются.

В сфере ИТ, например в РФ, планируются такие меры господдержки как [11]:

– переход на российскую систему доменных имен, отказ от иностранных хостингов и усиление парольной политики для государственных сайтов (меру планирует ввести Правительство РФ);

– освобождение ИТ-организаций от налогового, валютного и др. видов государственного и муниципального контроля (мера введена Правительством РФ);

– бесплатная выдача российских сертификатов для сайтов (меру предложило Минцифры);

– обеспечение ускоренного импортозамещение ПО на объектах критической информационной инфраструктуры (КИИ) за счет целевого бюджетного финансирования (Указ подписан);

– предоставление грантов на разработку и развитие ИТ-продуктов (снизив требование к обязательному внебюджетному софинансированию проектов до 20%, а в отдельных случаях – до 0% (Указ подписан);

– упрощение порядка проведения закупок отечественных критически важных разработок в области ИТ для обеспечения государственных и муниципальных нужд или проводимых отдельными видами юридических лиц (Указ подписан).

При эксплуатации программных, аппаратных и аппаратно-программных средств ЗИ возникают вопросы, связанные с оценкой эффективности различных систем безопасности и повышения надёжности их функционирования при проведении на ИС, ИТКС, ИИ, АСУ целенаправленных компьютерных атак с целью нарушения их функционирования.

В настоящее время существуют различные методики определения эффективности ИБ (характеристик систем ЗИ и др.) [12–13]. Совокупность методов анализа рисков ИБ базируется на двух моделях:

– первая модель определяет риск на основе сопоставления соответствия объекта защиты набору требований по ИБ, которые исходят из стандартов, нормативно-правовых актов и условий эксплуатации систем;

– вторая модель определяет риск на основе оценки вероятностей реализации угроз и атак и величин получения потенциально возможного материального ущерба [13].

Для гибкой и эффективной управленческой функции, а также оперативного сбора и передачи данных между регионами создается распределённая сеть передачи данных (РСПД), которая объединяет магистральные узлы связи системы передачи данных (УС СПД) федеральных округов, УС СПД регионов и сети клиентских подключений.

2. Распределенная сеть передачи данных

РСПД предоставляет услуги по передаче информационного, технологического, корпоративного и мультимедийного трафика (телефония и видеоконференцсвязи); трафика управления для взаимодействия с системой управления и мониторинга и с системой обеспечения ИБ (СОИБ); для организаций с корпоративной или открытой сетями. Примерная структурная схема РСПД приведена на рис. 1.

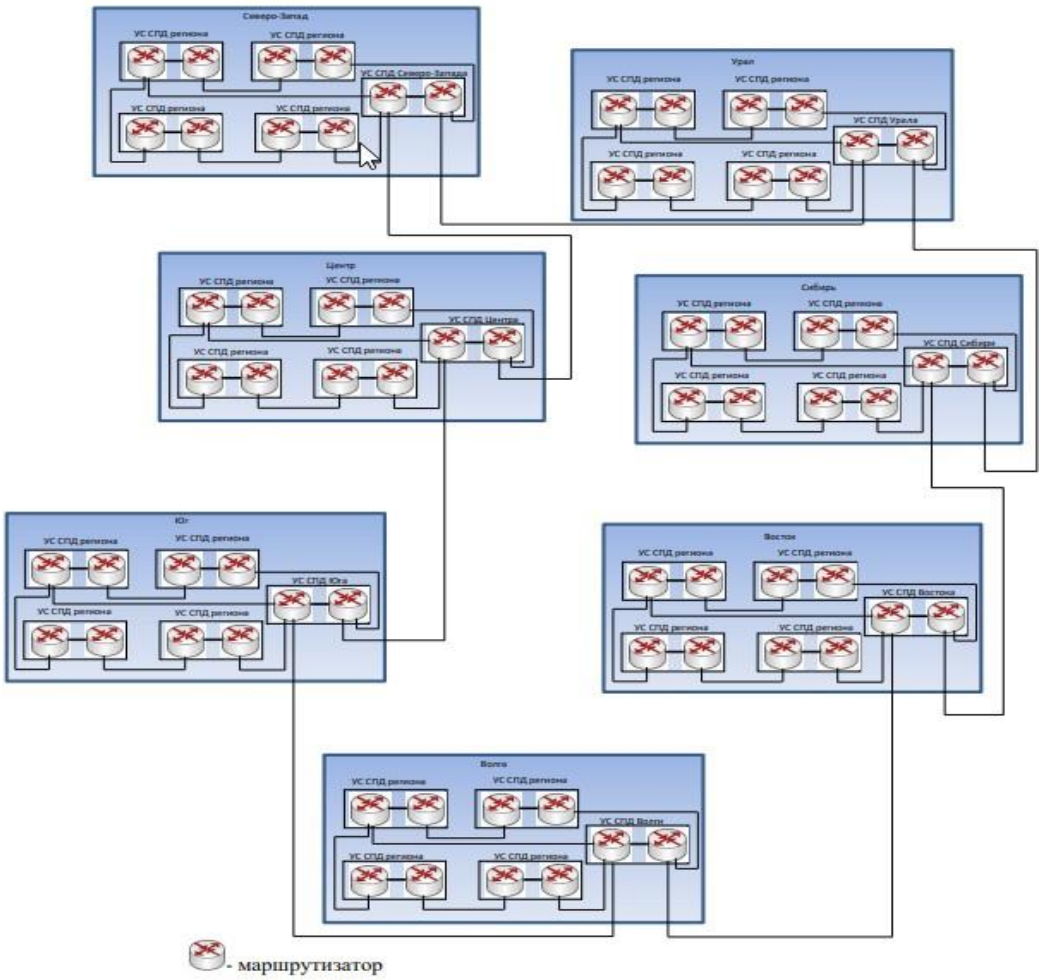

Рис. 1. Примерная структурная схема распределенной сети передачи данных
Fig. 1. An approximate block diagram of a distributed data transmission network

Важно. При создании единого УС СПД все оборудование располагается на одном объекте, при структуре разнесенного распределенных УС СПД основное оборудование

размещается на одном объекте, а резервирующее на другом объекте, что позволяет повысить надежность и получить меньшую вероятность отказа.

Выбор расположения УС СПД определяется каждым собственником РСПД, исходя из определенных им критериев.

Вывод. *Для обеспечения ИБ и целостности структуры РСПД необходимо создание СОИБ. Такая система позволит остановить несанкционированный доступ к информации и элементам РСПД, что с большой вероятностью предотвратит появление компьютерной атаки или инцидента.*

3. Система обеспечения информационной безопасности РСПД

Система обеспечения информационной безопасности сети (сетей) электросвязи (СОИБ) – это совокупность организационно-технической структуры и/или исполнителей, задействованных в обеспечении информационной безопасности сети (сетей) электросвязи и используемых ими «механизмов» обеспечения безопасности (различных средств защиты), взаимодействующая с органами управления сетью (сетями) связи, функционирование которой осуществляется по нормам, правилам и обязательным требованиям, установленным федеральными органами исполнительной власти, уполномоченными в областях связи, обеспечения безопасности и технической защиты информации[9].

СОИБ состоит из сил обеспечения ИБ и средств обеспечения безопасности, которые применяются ими. Структурная схема СОИБ приведена на рис. 2.

Рис. 2. Структурная схема СОИБ
Fig. 2. Structural diagram of ISMS

Данная система функционирует в соответствии с организационно-распорядительной документацией и руководствуется ей на всех этапах жизненного цикла РСПД.

Схема размещения компонентов СОИБ на вычислительной инфраструктуре приведена на рис. 3.

СОИБ должна обеспечить:

[9]ГОСТ Р 53110-2008 Система обеспечения информационной безопасности сети связи общего пользования.

– предупреждение неправомерного (несанкционированного) доступа (НПД и НСД) к информации и к услугам связи, сетевому оборудованию;

– предотвращение компьютерных инцидентов при компьютерной атаке;

– своевременное восстановление РСПД.

В качестве основных технических средств можно применять комплексы и системы, способные решать задачи своевременного обнаружения и предотвращения вторжения, предоставления достоверной информации клиенту и возможности оказания противодействия несанкционированным действиям, возникновению нештатных ситуаций.

В качестве основных целей можно выбрать: обеспечение конфиденциальности, оперативности, и эффективности органов управления СОИБ; обеспечения эффективного информационного взаимодействия СОИБ; повышение качества управленческих решений и совершенствования анализа принимаемых и принятых решений; обеспечения требуемых уровней безопасности, сохранности, полноты и достоверности информации РСПД; защиты от НПД, НСД и использования РСПД. Оценка эффективности СОИБ РСПД является непрерывным процессом и подразумевает постоянное проведение анализа в динамическом режиме.

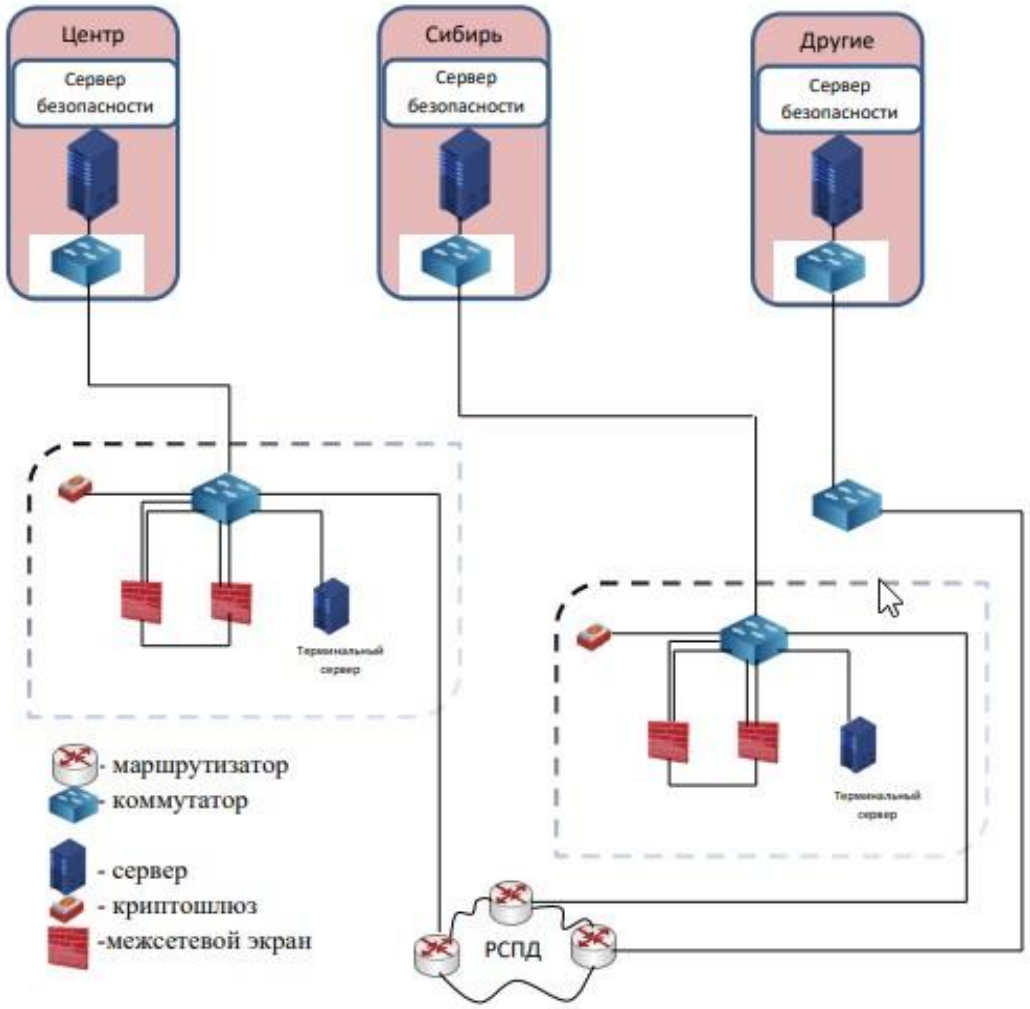

Рис. 3. Схема размещения компонентов СОИБ на вычислительной инфраструктуре
Fig. 3. The layout of the components of the ISMS on the computing infrastructure

Модели процессов ЗИ являются основными элементами научно-методологического базиса теории защиты информации. Проблеме моделирования систем и процессов ЗИ уделяется значительное внимание в ряде научных публикаций [14]. Результат анализа

моделей и их системной классификации, разработка обобщенной модели процессов ЗИ рассматривается многими авторами. Например, системное изложение в [15–17]. Учитывая важное значение в формировании перспективных планов организации соответствующих работ в решении стратегических проблем ЗИ остановимся на ней.

Вывод. *Значительное внимание при создании СОИБ следует уделять вопросам соотношения технических средств и организационных мер, что непосредственно показывает зависимость от вида угроз и вероятностного характера их возникновения и последствий от их реализации.*

4. Оценка системы обеспечения ИБ РСПД в условиях неопределенности

Ежегодно в мире количество и «качество» кибератак на ЗОКИИ продолжает расти. Однако многие компании, понимая наличие угроз, не могут правильно организовать и противодействовать их реализации.

В [18] отмечено: «Функционирование объектов критической информационной инфраструктуры в новой среде – киберпространстве, порождает новые уязвимости и угрозы, и требует разработки нового инструментария обеспечения устойчивости функционирование в условиях компьютерных атак». В [19] отмечено: «В настоящее время крупные компании и государственные структуры подсчитывают потенциальные убытки, которые могут возникнуть».

Ситуацию, в которой нельзя или практически нельзя определить вероятность потенциальных результатов принятого решения называют неопределённой, то есть, когда имеют место требующие учёта факторы новы и сложны, и от них невозможно получить релевантную информацию и, как следствие, невозможно предсказать исход принятого решения. Так как факторы, пока ещё новы и сложны, то организации будет достаточно сложно определить эффективность своей СОИБ РСПД.

Заметим, что достаточно редко (на практике) принимаются решения в условиях *полной неопределенности*. Как правило, имеется некоторая возможность доопределить [20] первоначально совершенно неопределенную ситуацию, но это уже др. тема.

Важно заметить, что одним из основных факторов неопределенности в оценке результатов работы СОИБ РСПД является сама система и результат (на ней) человеческой деятельности. Поэтому необходимо уметь (и правильно использовать полученные данные) оценивать риск потерь или выигрыша от принятия той или иной альтернативы.

4.1. Оценка подразделений, входящих в СОИБ РСПД

При оценке подразделения, ответственного за ИБ необходимо обратить внимание на количественный и качественный состав данного подразделения (СОИБ). Руководитель и сотрудники данного подразделения должны отвечать требованиям нормативно-правовых актов (НПА), которые предусмотрены к уровню образования, переподготовки (повышения квалификации) и стажу работы.

Теоретическая подготовка проверяется методом письменного или устного тестирования по основным вопросам обеспечения ИБ, а также знаниям НПА и внутренних организационно распорядительных документов (ОРД). Для других подразделений оценка проводится на теоретическом уровне и по практическому выполнению ими должностных инструкций по обеспечению ИБ. При удовлетворении требованиям предусмотренных НПА и ОРД можно сделать вывод, подразделения и их сотрудники соответствуют должному уровню для эффективного выполнения возложенных на них задач [21].

4.2 Оценка организационно-распорядительной документации

Оценка ОРД. Вначале рассматривается наличие и достаточность ОРД.

В дальнейшем необходимо выделить из всей массы ОРД, те документы, которые определены НПА в обязательном порядке. Выполнить оценку данных документов на состав и содержание, а также на соответствие НПА.

Документы, которые разработаны организацией самостоятельно необходимо рассмотреть и оценить с точки зрения их достаточности и целостности. В данных документах должна прослеживаться взаимосвязь между собой и с ОРД, которые обязательны к разработке в соответствии с НПА.

Особо стоит обратить внимание на доведение ОРД до должностных лиц и сотрудников организации, которые участвуют в обеспечении ИБ.

Выполнение этих требований позволит сделать вывод о том, что ОРД действительно эффективно влияет на организацию обеспечения ИБ РСПД.

4.3 Оценка технических мер в СОИБ РСПД

Оценка технических мер производится исходя из состава и схемы построения СОИБ.

В соответствии с уязвимостью программных и аппаратно-программных средств и на основании моделей угроз и нарушителя определяется состав технических мер.

При удовлетворении требованиям по защите от угроз безопасности информации и «закрытию» уязвимостей, необходимо технические меры (ТМ) рассмотреть со стороны их готовности. В частности, схемы построения СОИБ РСПД.

СОИБ должна функционировать круглосуточно в режиме 365/24/7 и для повышения готовности иметь резервирование. Резервирование и малое время восстановления повышает такой показатель как коэффициент готовности. Коэффициент должен быть рассчитан как для аппаратной, так и программной составляющих и не должен быть ниже предъявленных в техническом задании к нему требований, как правило, не ниже 0,95.

Если данные условия по оценке технических мер выполняются, то можно сделать вывод, что данная составляющая эффективна.

4.4. Оценка эффективности СОИБ РСПД. Метод экспертных оценок

Оценка эффективности СОИБ предполагает проведения отдельной оценки каждой составляющей данной системы со стороны организационных и технических мер защиты. Для того чтобы выполнить качественно оценку эффективности СОИБ РСПД сначала необходимо ознакомитьсяс обобщённой моделью процессов защиты информации. В [12] обращено внимание на то, что «применённая модель в принципе позволяет решать все задачи моделирования систем и процессов ЗИ. Однако, чтобы воспользоваться этой обобщенной моделью [12 рис. V.1], должны быть известны функциональные зависимости значений показателей от всех обобщенных параметров и зависимость самих параметров от размеров ресурсов, вкладываемых в реализацию соответствующих процессов».

На практике из-за отсутствия таких данных не удаётся выполнить требуемые условия. Поэтому рассматриваемую модель применяют только в совокупности с неформальными методами анализа и прогнозирования, с применением алгоритма автоформализации знаний эксперта-аналитика, где использование энтропии системы может быть продуктивным подходом.

Многие отечественные методики и подходы [11-12] опираются на такую группу методов творческого мышления, как эвристические методы. Внутри данной группы принято выделение отдельной подгруппы: метод «мозгового штурма», экспертный метод, метод синетики, метод контрольных опросов, метод фокальных объектов, метод «маленьких человечков», интегральный метод «Метра» и метод записной книжки Хефеле.

Использование метода экспертных оценок предполагает наличие (подбор) экспертов, организацию проведения опроса с процедурой экспертизы, обработку результатов опроса экспертов.

В частности, для оценки эффективности СОИБ РСПД, необходимо провести следующие оценки:

– укомплектованности и уровня подготовки сотрудников подразделений, отвечающих за безопасность РСПД, эксплуатирующего подразделения и подразделения обеспечивающего функционирование РСПД;

– достаточность и целостность организационно-распорядительной документации и применяемых мер по выполнению требований к обеспечению безопасности в ходе создания и эксплуатации РСПД;

– достаточность и готовность применяемых технических мер по обеспечению требований безопасности информации РСПД.

Рассмотрим метод экспертных оценок для СОИБ РСПД (с проведением последующего анализа полученных результатов для формирования отчета и включением в акт того или иного ЗОКИИ).

Для определения состояния ИБ в автоматизированных системах на основании полученных (сформированных) тестов можно использовать показатель, применённый для оценки уровня защищенности, на оценках тестируемого [18]. Указанный уровень определяется по результатам ответов сотрудниками организации на предлагаемые экспертами n вопросов.

Предварительно экспертами определены коэффициенты важности (КВ), например, *технических мер* СОИБ РСПД – P_j, $j = \overline{1,n}$ для каждого задаваемого вопроса, с использованием метода относительного ранжирования. Такой метод позволит выполнить сравнение двух ближайших элементов (проигнорировав все остальные).

Эксперт принимает решение путём голосования и т.д. После формирования КВ *технических мер* СОИБ РСПД нормализуем их по формуле

$$PN_j = {\mathrm{P}_j}\Big/{\sum_{j=1}^{n} \mathrm{P}_j},$$

таким образом, чтобы выполнилось условие

$$\sum_{j=1}^{n} PN_j = 1.$$

Вводим лингвистическую переменную (ЛП) *технических мер* СОИБ РСПД – «уровень защищенности». Базовый терм-множество представляем пятью нечёткими термами $\mathrm{T} = \{\mathrm{T}_1, \mathrm{T}_2, \mathrm{T}_3, \mathrm{T}_4, \mathrm{T}_5\}$, имеющими соответственно названия «низкий» (Н), «ниже среднего» (НС), «средний» (С), «выше среднего» (ВС) и «высокий» (В).

Диапазон носителей (изменения параметров) X_i, $i = \overline{1,L}$ (где L = 5 – количество термов) отображаемый на универсальное множество U = [0, 4].

Функции принадлежности μ_i, $i = \overline{1,L}$ определяем следующим образом:

$$\mu_i = \frac{1}{1+(x-i+1)^2}.$$

В результате получаем следующие эталонные нечёткие числа (НЧ), отражающие введенную переменную ЛП *технических мер* СОИБ РСПД.

Воспользуемся уже найденными (некоторыми) значениями и формулами: значения ЛП [21, с. 384, (20.4)] и их графическим изображением [21, с. 385, рис. 20.1]; и формулами: пересчёта фиксированного значения X_j^* [21, с. 384, (20.5)], функции принадлежности $\mu_i^j(U_j^*)$ [21, с. 385, (20.6)], и показателя уровня защищенности $\mu_s(\mathrm{X}_j^*)$ [21, с. 385, (20.7)].

В завершение, из полученных значений формируем показатель уровня защищенности *(технических мер* СОИБ РСПД*)*, образованный на основании следующего нечеткого логического выражения:

$$\mu_s(\mathrm{X}_j^*).$$

Данный показатель позволяет определить выбор принятия решения по выполняемым *техническим мерам* СОИБ РСПД. Такие вычисления необходимо выполнить и для других показателей СОИБ РСПД.

Вывод. *При условии, если все рассмотренные оценки показателей эффективности СОИБ РСПД будут соответствовать выбранным требованиям защита будет обеспечена должным образом.*

Заключение

Одной из основных проблем в создании СОИБ РСПД является отсутствие и/или недостаточная подготовка кадров в области ИБ; большая финансовая нагрузка на создание и модернизацию аппаратно-программных средств и др. Приступая к созданию СОИБ, необходимо ещё на этапе проектирования архитектуры РСПД выявить возможные внешние и внутренние источники угроз безопасности информации, разработать модель нарушителя и модель угроз информационной безопасности. При оценке эффективности необходимо учитывать изменения структуры СОИБ РСПД, в том числе численный и качественный состав подразделений, обеспечивающий информационную безопасность (ИБ), аппаратно-программных средств и их обновления, наличие новых угроз и уязвимостей и др.

Представленный в работе подход к оценке эффективности управленческой функции, а также оперативного сбора и передачи данных между регионами на основе применения СОИБ при построении и эксплуатации предложенной системы РСПД создаёт методологическую основу для дальнейшего проведения исследований в направлении разработки типовых методик СОИБ РСПД. Полученные показатели уровня защищенности $\mu_s(\mathrm{X}_j^*)$ (для каждой из принимаемых мер) помогут эксперту определиться с принятием правильного решения по всем рассматриваемым (выполняемым) мерам обеспечения безопасности ИБ в РСПД. Разработанный подход может быть полезен при оценке эффективности СОИБ не только в РСПД, но и в других системах при разработке модели защиты информации в АСУ и ИС, а также при формировании требований к качеству систем (времени реакции на запрос пользователя, коэффициенту готовности, ресурсоемкости и др.). Дальнейшее исследование следует проводить для других практик и их сравнительного анализа.

СПИСОК ЛИТЕРАТУРЫ:

1. Крючков А.В., Прус Ю.В., Резниченко С.А. Технологические основы национальной информационной безопасности. Сборник статей, Международной научно-практической конференции Российского государственного гуманитарного университета. 2018, с. 58–63. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-2-2022-36/ (дата обращения: 25.02.2022).
2. Мальцев В.Н., Прус Ю.В., Резниченко С.А. Аспекты информационной безопасности на начальном этапе создания инновационных продуктов. Сборник статей, Международной научно-практической конференции Российского государственного гуманитарного университета. 2021, с. 173–183. URL: https://elibrary.ru/item.asp?id=47238106 (дата обращения: 25.02.2022).
3. Дробот Г.А. США как мировой лидер: реалии, теории, перспективы. Век глобализации. 2018, № 1, с. 83–94. URL: https://elibrary.ru/item.asp?id=32595473 (дата обращения: 25.02.2022).
4. Елин В.М. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом, монография, УДК 341.231, ББК 67.404.2, Е51, ISBN 978-5-9909450-7-4. URL: https://elibrary.ru/item.asp?id=28108297 (дата обращения 24.11.2021).
5. Group-IB представила отчет о киберпреступности и призвала рынок к хантингу. Group-IB. URL: https://www.group-ib.ru/media/hi-tech-crime-trends-2018/ (дата обращения: 20.09.2021).
6. ТБ Форум 2019: завершился крупнейший съезд руководителей по безопасности. BIS JOURNAL. URL: https://ib-bank.ru/bisjournal/news/10743 (дата обращения: 20.09.2021).

7. Выступление заместителя директора НКЦКИ Н.Мурашко. URL. https://ren.tv/news/v-mire/369494-nkski-rossiiskeresursu-podvergaiutsia-massirovannym-atakam-iz-za-rubezha (дата обращения: 20.04.2022).
8. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы. Вопросы кибербезопасности. 2019, № 1(29), с. 2–9. URL: https://elibrary.ru/item.asp?id=37085067. DOI: http://dx.doi.org/10.21681/2311-3456-2019-1-2-9. (дата обращения: 20.04.2022).
9. Ахромеева Т.С., Малинецкий Г.Г., Посашков С.А. Стратегии и риски цифровой реальности. Стратегические приоритеты. 2017, № 2 (14), с. 88–102. URL: https://elibrary.ru/item.asp?id=29947604 (дата обращения: 20.11.2021).
10. Мехтиева Н.Р. Информационные войны как «цифровой» аспект глобализации. Век глобализации. 2017, № 3, с. 77–89. URL: https://elibrary.ru/item.asp?id=30266882 (дата обращения: 25.03.2022).
11. Сайт: РБК – ТВ. Подробнее на РБК: Государство сократит расходы на исследования и разработки. Незначительно снизится только финансирование военных изысканий. URL: https://www.rbc.ru/economics/06/10/2020/5f7b372b9a7947fe8e8d644f (дата обращения: 25.04.2022).
12. Скрыпников А.В., Попов А.Д., Рогозин Е.А., Хвостов В.А. Экспериментальный метод определения вероятностно-временных характеристик систем защиты информации от несанкционированного доступа в автоматизированных информационных системах. Вестник Воронежского государственного университета инженерных технологий. 2017, т. 79, № 4, с. 90–96. URL: https://elibrary.ru/item.asp?id=32585436. DOI: https://doi.org/10.20914/2310-1202-2017-4-90-96 (дата обращения: 25.04.2022).
13. Дровникова И.Г., Змеев А.А., Попов А.Д., Рогозин Е.А. Методика исследования вероятностно-временных характеристик реализации сетевых атак в программной среде имитационного моделирования. Вестник Дагестанского государственного технического университета. Технические науки. 2017, т. 44, № 4, с. 99–113. URL: https://elibrary.ru/item.asp?id=32855669. DOI: https://doi.org/10.21822/2073-6185-2017-44-4-99-113 (дата обращения: 25.04.2022).
14. Баранова Е.К., Бабаш А.В. Моделирование системы защиты информации. 3-е изд., перераб. и доп. М.: РИОР: ИНФРА-М, 2020. – 320 с. URL: https://elibrary.ru/item.asp?id=26014789 (дата обращения: 25.04.2022).
15. Малюк А.А. Теория защиты информации: Монография. М.: Горячая линия – Телеком, 2012. – 128 с.
16. Малюк А.А. Информационная безопасность: Концептуальные и методологические основы защиты информации. М.: Горячая линия – Телеком, 2004. – 128 с.
17. Малюк А.А. Основы политики безопасности критических систем информационной инфраструктуры. М.: Горячая линия – Телеком, 2019. – 314 с.
18. Захарченко Р.И., Королев И.Д. Методика оценки устойчивости функционирования объектов критической информационной инфраструктуры, функционирующей в киберпространстве. Наукоемкие технологии в космических исследованиях Земли. 2018, т. 10, № 2, с. 52–61. URL: https://elibrary.ru/item.asp?id=34939627 (дата обращения: 25.03.2022).
19. Оюн Ч.О., Попантонопуло Е.В. Объекты критической информационной инфраструктуры. Интерэкспо Гео-Сибирь. 2018, № 9, с. 45–49. URL: https://elibrary.ru/item.asp?id=35661002 (дата обращения: 25.03.2022).
20. Сиротский Алексей А., Резниченко Сергей А. Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов. Безопасность информационных технологий, [S.l.], 2021, т. 28, № 3, с. 103–117, URL: https://elibrary.ru/item.asp?id=46709372. DOI: http://dx.doi.org/10.26583/bit.2021.3.09 (дата обращения: 25.03.2022).
21. Грибунин В.Г. Комплексная система защиты информации на предприятии. М.: Издательский центр «Академия», 2009. – 416 с. ISBN 978-5-7695-5448-3. URL: https://bookskeeper.ru/knigi/obrazovanie/84115-kompleksnaya-sistema-zaschity-informacii-na-predpriyatii.html (дата обращения: 25.03.2022).

REFERENCES:

[1] Kryuchkov A.V., Prus Yu.V., Reznichenko S.A. Technological foundations of national information security. Collection of articles, International scientific and practical conference of the Russian State University for the Humanities. 2018, p. 58–63. URL: https://qje.su/ekonomicheskaya-teoriya/moskovskij-ekonomicheskij-zhurnal-2-2022-36/ (accessed: 25.02.2022) (in Russian).
[2] Maltsev V.N., Prus Y.V., Reznichenko S.A. Aspects of information security at the initial stage of creating innovative products. Collection of articles of International scientific-practical conference of the Russian state University for the Humanities. 2021, p. 173–183. URL: https://elibrary.ru/item.asp?id=47238106 (accessed: 25.02.2022) (in Russian).

[3] Drobot G.A. USA as a world leader: realities, theories, prospects. Century of globalization. 2018, no. 1, p. 83–94. URL: https://elibrary.ru/item.asp?id=32595473 (accessed: 25.02.2022) (in Russian).
[4] Elin V.M. Comparative analysis of legal support of information security in Russia and abroad, monograph, UDC 341.231, BBK 67.404.2, E51, ISBN 978-5-9909450-7-4. URL: https://elibrary.ru/item.asp?id=28108297 (accessed: 24.11.2021) (in Russian).
[5] Group-IB presented a report on cybercrime and called on the market to hunt. Group-IB. URL: https://www.group-ib.ru/media/hi-tech-crime-trends-2018/ (accessed: 20.12.2021) (in Russian).
[6] TB Forum 2019: the largest congress of security managers has ended. BIS JOURNAL. URL: https://ib-bank.ru/bisjournal/news/10743 (accessed: 20.12.2021) (in Russian).
[7] Speech by the Deputy Director of SIC KI N.Murashko. URL. https://ren.tv/news/v-mire/369494-nkski-rossiiskeresursu-podvergaiutsia-massirovannym-atakam-iz-za-rubezha (accessed: 20.04.2022) (in Russian).
[8] Romashkina N.P. Global military-political problems of international information security: trends, threats, prospects. Questions of cybersecurity. 2019, no. 1(29), p. 2–9. DOI: https://elibrary.ru/item.asp?id=37085067 (accessed: 20.04.2022) (in Russian).
[9] Akhromeeva TS, Malinetskiy G.G., Posashkov S.A. Strategies and risks of digital reality. Strategic priorities. 2017, no. 2(14), p. 88–102. URL: https://elibrary.ru/item.asp?id=29947604 (accessed: 20.11.2021) (in Russian).
[10] Mehdiyev N.R. Information wars as a “digital” aspect of globalization. The Century of Globalization. 2017, no. 3, p. 77–89. URL: https://elibrary.ru/item.asp?id=30266882 (accessed: 25.03.2022) (in Russian).
[11] Read more on RBC: The state will reduce research and development costs. Only the financing of military research will decrease slightly. URL: https://www.rbc.ru/economics/06/10/2020/5f7b372b9a7947fe8e8d644f (accessed: 25.04.2022) (in Russian).
[12] Skrypnikov A.V., Popov A.D., Rogozin E.A., Khvostov V.A. Computational experiment for the purpose of determining the probabilistic and temporal characteristics of information security systems against unauthorized access in automated information systems. Proceedings of the Voronezh State University of Engineering Technologies. 2017, vol. 79, no.4, p. 90–96. URL: https://elibrary.ru/item.asp?id=32585436. DOI: http://doi.org/10.20914/2310-1202-2017-4-90-96 (accessed: 25.04.2022) (in Russian).
[13] Drovnikova I.G., Zmeev A.A., Popov A.D., Rogozin E.A. Methodology for investigating the probability-time characteristics of network attacks in the simulation modelling software environment. Herald of Dagestan State Technical University. Technical Sciences. 2017, vol. 44, no. 4, p. 99–113. URL: https://elibrary.ru/item.asp?id=32855669. DOI: https://doi.org/10.21822/2073-6185-2017-44-4-99-113 (accessed: 25.04.2022) (in Russian).
[14] Baranova E.K., Babash A.V. Modeling of the information security system. 3rd ed., reprint. and additional. M.: RIOR: INFRA-M, 2020. – 320 p. URL: https://elibrary.ru/item.asp?id=26014789 (accessed: 25.04.2022) (in Russian).
[15] Malyuk A.A. Theory of information protection: Monograph. M.: Hotline – Telecom, 2012. – 128 p. (in Russian).
[16] Malyuk A.A. Information security: Conceptual and methodological foundations of information protection. M.: Hotline – Telecom, 2004. – 128 p. (in Russian).
[17] Malyuk A.A. Fundamentals of the security policy of critical information infrastructure systems. M.: Hotline – Telecom, 2019. – 314 p. (in Russian).
[18] Zakharchenko R.I., Korolev I.D. Methodology for assessing the stability of the functioning of critical information infrastructure facilities operating in cyberspace. High-tech in space research of the Earth. 2018, vol. 10, no. 2, p. 52–61. URL: https://elibrary.ru/item.asp?id=34939627 (accessed: 25.03.2022) (in Russian).
[19] Oyun H.A., Papantonopoulou E.V. Objects of critical information infrastructure. Interexpo geo-Siberia. 2018, no. 9, p. 45–49. URL: https://elibrary.ru/item.asp?id=35661002 (accessed: 25.03.2022) (in Russian).
[20] Sirotskiy Alexei A., Reznichenko Sergei A. A formalized model of an organization information security audit for compliance with the requirements of standards. IT Security (Russia), [S.l.], 2021, vol. 28, no. 3, p. 103–117, ISSN 2074-7136. URL: https://elibrary.ru/item.asp?id=46709372. DOI: http://dx.doi.org/10.26583/bit.2021.3.09 (accessed: 25.03.2022) (in Russian).
[21] Gribunin V.G. Integrated information security system at the enterprise. M.: Publishing Center "Academy", 2009. – 416 p. ISBN 978-5-7695-5448-3. URL: https://bookskeeper.ru/knigi/obrazovanie/84115-kompleksnaya-sistema-zaschity-informacii-na-predpriyatii.html (accessed: 25.03.2022) (in Russian).

Поступила в редакцию – 21 января 2022 г. Окончательный вариант – 19 мая 2022 г.
Received – January 21, 2022. The final version – May 19, 2022 г.