ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056, 346.244
DOI: 10.21822/2073-6185-2022-49-3-74-81 Обзорная статья / Review article

Угрозы информационной безопасности госкорпораций Российской Федерации

И.А. Лоскутов[1], С.А. Резниченко[2]
[1]Научно-производственная корпорация «Космические системы мониторинга, информационно-управляющие и электромеханические комплексы имени А.Г. Иосифьяна»
(АО «Корпорация «ВНИИЭМ»),
[1]107078, г. Москва, ул. Вольная, 30, стр. 10, Россия,
[1,2] Национальный исследовательский ядерный университет «МИФИ»,
[1,2]115409, г. Москва, Каширское шоссе, 31, Россия,
[2]Финансовый университет при Правительстве Российской Федерации,
[2]125167, г. Москва, Ленинградский пр-т, 49/2,
[2]Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина»,
[2]119991, г. Москва, Ленинский пр-т, 65, Россия

Резюме. Цель. Целью исследования является структурирование общедоступной информации для определения отличительных особенностей, присущих госкорпорациям РФ и описание угроз, возникающих в результате их непрерывного функционирования. **Метод**. В качестве методов научного познания используются: систематизация, описание, анализ, дедукция. Характеристики госкорпораций формируются на основе данных, полученных как из нормативно-правовой базы, так и по результатам анализа современных исследований по теме. **Результат.** Проведена систематизация угроз информационной безопасности госкорпораций; рассматриваются наиболее распространенные их классификации; отмечается возрастающая активность злоумышленников относительно объектов критической информационной инфраструктуры и выявлены возможные последствия для госкорпораций после «успешно» проведённой на ней компьютерной атаки. Комплексный анализ позволил подробно охарактеризовать объект исследования, тем самым конкретизировав значимые аспекты его функционирования. Определены наиболее значимые угрозы угроз госкорпораций России; отмечена важность обеспечения информационной безопасности и показаны 15 факторных влияний «успешной» кибератаки. **Выводы**. Материалы, представленные в работе, могут послужить базисом для дальнейших исследований по направлению, а также формирования принципов защиты от выявленных угроз.

Ключевые слова: информационная безопасность, госкорпорации, угрозы, компьютерные атаки

Для цитирования: И.А. Лоскутов, С.А. Резниченко. Угрозы информационной безопасности госкорпораций Российской Федерации. Вестник Дагестанского государственного технического университета. Технические науки. 2022; 49(3):74-81. DOI:10.21822/2073-6185-2022-49-3-74-81

Threats to information security of state corporations of the Russian Federation

I.A. Loskutov, S.A. Reznichenko
[1]A.G. Iosifian' Joint Company 'Research and Production Corporation 'Space Monitoring Systems,
[1]30 Volnaya Str., p. 10, Moscow 107078, Russia,
[1,2] National Research Nuclear University MEPHI,
[1,2]31 Kashirskoe highway, Moscow 2115409, Russia,
[2]Financial University under the Government of the Russian Federation,
[2]49/2 Leningradsky Ave., Moscow 125167, Russia,
[2]I.M. Gubkin Russian State University of Oil and Gas (National Research University),
[2]65 Leninsky Ave., Moscow 2119991, Russia

Abstract. Objectives. Structuring of publicly available information to identify the distinctive features inherent in state corporations of the Russian Federation and to describe the threats arising as a result of their continuous operation. **Method**. The following methods of scientific cognition are used: systematization, description, analysis, deduction. The characteristics of state corporations are formed on the basis of data obtained both from the regulatory framework and by means of analysis of modern research in the field. In the future, the systematization of knowledge about the threats of state corporations is carried out, the most common classifications are considered, the increasing activity of intruders regarding critical information infrastructure objects is noted, and possible consequences for the state corporation after a successful computer attack on them are noted. **Result**. In this paper, a study was conducted on a little–covered area in the scientific literature - the protection of Russian state corporations. A comprehensive analysis made it possible to characterize the object of research in detail, thereby specifying the significant aspects of its functioning. Next, the most significant threats of Russian state corporations were shown, the importance of ensuring information security was noted and 15 factor influences of a successful cyberattack were shown. **Conclusions**. The conducted research is of an overview nature. The materials presented in the paper can serve as a basis for further research in the direction, as well as the formation of principles of protection against the mentioned threats.

Keywords: information security, IS, state corporations, threats, computer attacks

For citation: I.A. Loskutov, S.A. Reznichenko. Threats to information security of state corporations of the Russian Federation. Herald of the Daghestan State Technical University. Technical Science. 2022; 49 (3): 74-81. DOI: 10.21822 /2073-6185-2022-49-3-74-81

Введение. Глобализация мира постоянно требует реакции на вновь появляющиеся вызовы. С целью облегчения поиска выбора верного пути и стратегии развития многие компании объединяются в группы, образуя тем самым различные коммерческие сообщества.

Аналогичным путем действует и государственная политика в областях, связанных с решением стратегически важных вопросов, затрагивающих области национальных интересов. Результатом таких объединений в Российской Федерации с 1999 года становятся «госкорпорации» [1].

В целом, проведение исследований госкорпораций с точки зрения угроз ее информационной безопасности не ново. Являясь по своей сути объединением предприятий в одном структурном блоке, госкорпорации представляют собой мишень интересов для других государств и их шпионских организаций, а также отдельных незаконопослушных личностей.

Поскольку госкорпорации по своей сущности направлены на решение определенных национальных интересов государства, сохранение информации, имеющей особое значение, а также недопущение дисбаланса техпроцесса изготовления научных знаний и изделий, вызванных внешними злонамеренными воздействиями, становятся главными приоритетами организации.

Впервые, в нашем отечестве, официальная терминология была введена в статье 7.1 Федерального закона от 1996 г. №7-ФЗ [2].

Хотя по своей сущности государственные корпорации во многом напоминают фонды [3], в них присутствуют функции, свойственные как всем типам данного организационного объединения, так и конкретному виду экономической деятельности.

Кроме того, отличительная черта госкорпораций от прочих видов кооперации кроется в двойственности их функционирования с точки зрения нормативно-правовых актов.

В отмеченной работе [3] поднимается проблема регулирования их затрат с помощью органов власти, которая до сих пор не предусмотрена, из-за чего невозможно прозрачно оценить работоспособность столь больших экономических механизмов. Затронув тематику обобщающих факторов, с целью подробного определения особенностей, присущих госкорпорациям, стоит показать характеристики, свойственные всем отмеченным некоммерческим единицам [4]:

- базисное имущество выделено государством на безвозмездной основе;

- пока существует госкорпорация, обязательства России ее никак не касаются, обратное - аналогично; исключением является целевое создание госкорпорации, с соответствующей нормативно-правовой базой, в которой прописаны данные обстоятельства;
- имущество, переданное во владение госкорпорации, используется только по назначению (направлению деятельности, обозначенному при его создании);
- любая правомерная предпринимательская деятельность, связанная с направлением госкорпорации не запрещена;
- органы власти любой инстанции не вправе вмешиваться в функционирование госкорпорации, кроме случаев, закрепленных в федеральных нормативно-правовых актах;
- возможны временные рамки существования и функционирования госкорпораций [5];
- учредителем является государство [6];
- членство в госкорпорациях невозможно;
- форма собственности – госкорпоративная [7, с.11].

Достаточно многогранное описание характеристик госкорпораций не показывает всю вариативность их функционирования.

Для создания общей картины, описывающей характер деятельности необходимо отметить, что госкорпорации бывают двух видов [7]:

- функционирующие за счет товаро-имущественных взаимодействий (создающие/ использующие);
- выполняющие задачи, носящие организационный и / или координационно-распорядительный характеры.

Целевое предназначение госкорпораций определяется на основании потребности страны в решении проблем, как определенной отрасли, так и региона (ов), в котором (ых) будут представлены офисы и филиалы.

Среди положительных аспектов, как правило, выделяют [8]:

- развитие выбранного экономического сектора;
- долгосрочная занятость экономического сектора с минимизаций политического влияния;
- развитие инновационной политики экономического сектора;
- определение ответственных исполнителей тех или иных решений;
- обеспечение финансовыми потоками со стороны государства (исчезает необходимость в постоянном поиске инвесторов);
- выполнение требований модернизации отрасли, указанных в декадных разрабатываемых стратегиях развития;
- развитие частного предпринимательства, задействованного в кооперациях с госкорпорациями по отрасли;
- совершенствование и отработка новых подходов в части административного управления;
- удовлетворение потребности региона (ов) функционирования в части обеспечения рабочих мест [9].

Ключевой особенностью, на наш взгляд, является имущество, которое выделяется государством при создании госкорпораций.

Ранее упомянутая характеристика требует особого внимания, поскольку, в отличие от передачи помещений, техники и технологий, иных интеллектуальных и материальных элементов, чаще всего подразумевается передача заводских комплексов [10].

Таким образом, госкорпорация есть ни что иное как – управляющий дивизион.

Постановка задачи. Осознание данного факта приводит к логичному умозаключению о необходимости создании в госкорпорациях сложного многоуровневого регулирования, которое подтверждено все большему выходу новых законодательных актов.

Особенно это касается области информационной безопасности, т.к. передача данных как внутренняя, так и внешняя совмещена с определенными рисками и необходимостью создания

информационных «маячков» – категорий, присваиваемых каждому структурному подразделению и помещению внутри подконтрольных госкорпорации заводских комплексов.

Посему, для обеспечения должного уровня защиты столь значимых объектов необходимо постоянно апеллировать данными по основным угрозам, направленные на дестабилизацию функционирования предприятий госкорпораций.

Методы исследования. Поскольку госкорпорации относятся к объектам критической информационной инфраструктуры (КИИ) следует указать типы угроз, которые будут подразумеваться в работе. В соответствии с Федеральным законом от 2017 г. № 187-ФЗ [11] под угрозами КИИ следует понимать компьютерные атаки.

Тем самым, проводится явное разграничение с другими внешними воздействиями, которые могут оказать негативные и даже разрушительные эффекты, как например с электромагнитными, крайне подробно описанными во второй главе книги [12], хоть и предназначенной в первую очередь для разработки средств авиационной и радарной техники.

Покажем классификацию наиболее значимых методов компьютерных атак [13-14]:
отказ в обслуживании (DoS атака); логическая бомба; вредоносное программное обеспечение; троянский конь; вирус; червь; спам рассылка; ботнет; фишинг; парольные атаки; и др.

Каждая из указанных атак имеет свои отличительные характеристики, о которых немало написано в научной литературе. Они проявляются во взаимодействии с атакуемой системой. Поэтому оправданно также разделять угрозы по целям, которые будут достигнуты в случае плохой киберзащиты.

Информация, в результате атаки, может быть незаконно [15]: прочитана; изменена; уничтожена.

Кроме того, наличие незаконного программного продукта (ПП), может проявляться как: пассивное; активное.

В первом случае, вредоносный ПП будет предоставлять доступ к информации, но не вредить системе, во втором – целенаправленно дестабилизировать ее.

Также необходимо показать способы добычи информации: через легальные каналы; через недекларированные каналы.

Стоит обратить внимание, что в работе [15] освещался еще один классификационный элемент – программные закладки, однако в соответствии с РД от 1999 г. № 114 [16], он относится к недекларированным возможностям, тем самым в выделении его как отдельно значимого нет необходимости.

Существует множество других классификаций угроз, однако, на наш взгляд, уже создана достаточно полная картина способов добычи информации. Единственное –необходимо определить наиболее опасные методы компьютерных атак, среди показанных выше.

В случае атаки DoS, червей, ботнета, фишинга, парольных атак и спам-рассылки, последствия для КИИ будут проявляться в виде замедления передачи данных, потери конфиденциальной информации, находящейся на компьютерах, предназначенных для работ с внешними представителями, поскольку именно они требуют подключения к сети Интернет. Угрозу от них стоит рассматривать как среднюю по степени важности.

Логические бомбы, аналогично троянским коням, вредоносным ПП и вирусам наиболее опасны, в случае их непосредственной интеграции в локальную сеть заводского комплекса, тем самым, можно констатировать потребность обеспечения первостепенной защиты именно от данных типов угроз.

Важно отметить, что в случае деления госкорпорации на подразделения, территориально удаленные от головного здания, возможно стороннее незаконное проникновение в локальную сеть предприятия. В данном случае, атаки, описанные ранее как среднеопасные стоит переквалифицировать в «требующих особого внимания», аналогично вредоносному ПП и т.п. Далее стоит акцентировать внимание на таком важном моменте, как вероятность возникновения кибер атаки.

Обсуждение результатов. На рис.1 показана карта потенциальных угроз на 2020 г. [17, с.10]. В соответствии с исследованиями компании Check Point Software Technologies LTD, Россия относится к странам со средней вероятностью нападения.

Рис.1. Карта распределения потенциальных кибератак
Fig.1. Distribution map of potential cyber attacks

Градация света от серого к более темному (яркому) на рис. 1 обозначает вероятность возникновения в той или иной стране киберинцидента.

В целом тенденция распространения вредоносных программ, проведенная компанией SONICWALL за первое полугодие 2020 г., рис.2 [18, с.11], показывает аналогичную картину.

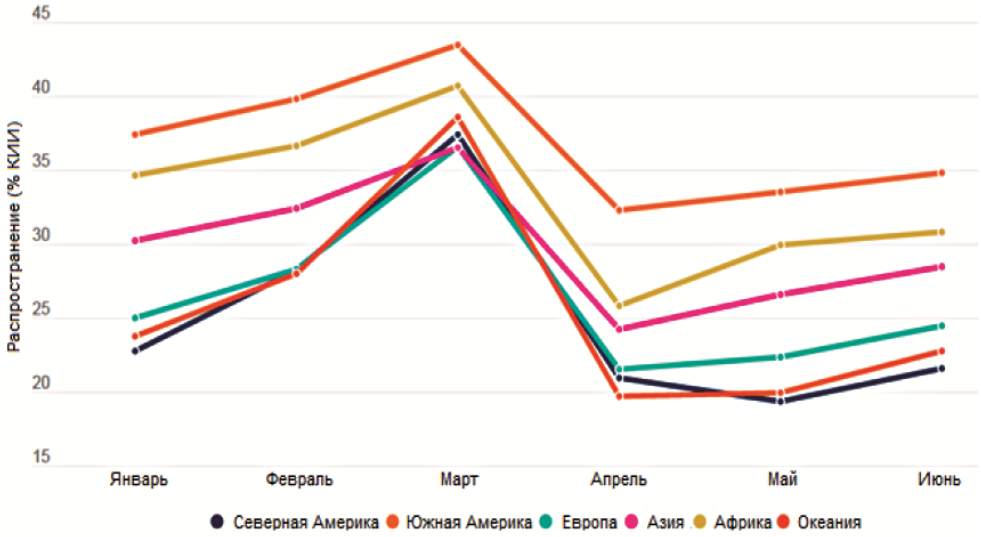

Рис.2. График распространения вредоносных программ
Fig.2. Malware distribution chart

Однако необходимо отметить, что статистика по среднему распределению не указывает конкретные данные по количеству атак.

На основании материалов компании Positive Technologies [19], нападения на объекты КИИ в Российской Федерации выросли более чем на 90% в 2020 году по сравнению с предыдущим отчетным периодом, рис.3.

Данный показатель подтверждает явную потребность в обеспечении должной системы защиты на таких производствах. Кроме того, нельзя не отметить тот разрушительный эффект, который оказывают сетевые атаки на госкорпорации.

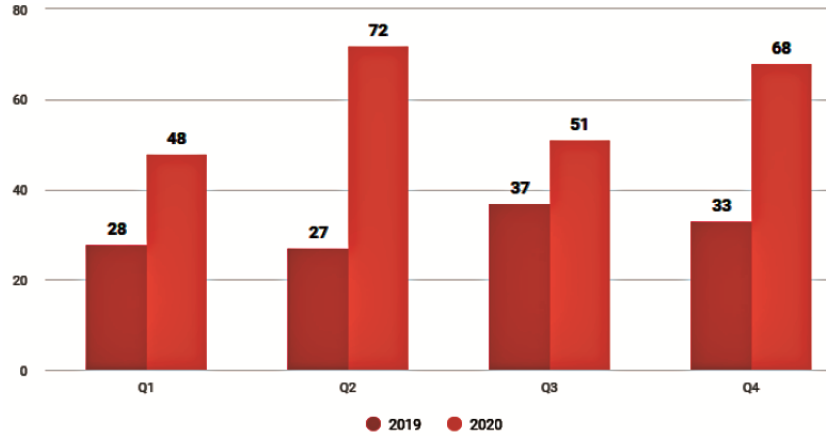

Рис.3. Количество кибернетических нападений на КИИ
Fig.3. Number of cyber attacks on CII

В соответствии с [20], [21, с.6] выделяются 14 факторных влияний на подвергшуюся кибератаке фирму:

- дополнительная трата финансов, в т.ч. на гонорары адвокатам и судебные издержки;
- восстановление системы и приведение в соответствие нормативным требованиям;
- уведомление клиентов о нарушении;
- обеспечение защиты данных клиентов после нарушения;
- проведение технического расследования;
- осуществление связи с общественностью;
- проведение улучшения в области кибербезопасности;
- увеличение страховых взносов;
- увеличение трат на привлечение заемных средств;
- ликвидация последствий сбоя в работе или разрушения;
- потеря интеллектуальной собственности;
- обесценивание торгового имени;
- необходимость возвращения фирменной значимости в отношениях с клиентами;
- необходимость расчета ущерба и упущенной выгоды по контракту.

Поскольку госкорпорации в соответствии с ранее упомянутой статьей 7.1 Федерального закона от 1996 г. №7-ФЗ [2] обязана публиковать бухгалтерскую отчетность, полная применимость указанных факторных влияний для таких организаций не вызывает сомнений.

Делая акцент на последствиях угроз, нельзя обойти вниманием такое понятие, как информационное противоборство. В [22] были отмечены два поколения, которые разнятся степенью влияния и подходами к процессу атаки, а также их характеристиками. Применительно к данной работе относится последний пункт второго поколения, выливающийся в потерях в той или иной сфере деятельности (т.е. можно рассмотреть, как дестабилизация функционирования предприятия госкорпорации).

Тем самым следует создать 15-е факторное влияние: восстановление производства в максимально короткий срок для обеспечения должного функционирования в области национальных интересов.

Вывод. Проведенный в работе анализ носит обзорный характер и затрагивает ключевые моменты информационной безопасности госкорпораций Российской Федерации.

На основании результатов исследования была сформирована база знаний, которая позволяет подробно охарактеризовать объект исследования, конкретизировать значимые аспекты его функционирования; систематизировать наиболее значимые угрозы информационной безопасности госкорпораций; предварительно оценить вероятность возникновения кибератак на госкорпорациях; выявить факторные влияния «успешно» проведенной компьютерной атаки. Информация, представленная статье, может быть использована как базис для дальнейших ис-

следований по направлению информационной безопасности, а также формирования принципов защиты от компьютерных угроз госкорпораций.

Библиографический список:

1. Степанов К.С. Реализация государством предпринимательской функции через институт госкорпорации // Вестник Саратовского государственного социально-экономического университета. - 2011. - N 1(35). - С.36-38.
2. Федеральный закон от 12.01.1996 N7-ФЗ «О некоммерческих организациях»
3. Аштаева С.С. Государственные корпорации в России, их становление и роль в развитии экономики // Право и государство: теория и практика. - 2013. - N 12(108). - С.140-146.
4. Панфилов К.С. Экономическое и политическое измерение эффективности российских государственных корпораций // Бизнес. Общество. Власть. - 2019. - № 2(32). - С.45-63.
5. Аштаева С.С. Госкорпорации в современной России: функции, структура и особенности деятельности // Вестник Калмыцкого института гуманитарных исследований РАН. - 2012. - Т. 5. - N 1. С.113-116.
6. Моралес К., Грищенко А.И. Корпорации в России и зарубежных правопорядках: понятие и сущность (государственные корпорации в современной России на примере Государственной корпорации "Росатом) // Энергетическое право. - 2009. - N 1. - С.19-29.
7. Каплин С.Ю. Государственная корпорация как субъект права: автореф. на соиск. ученой степ. канд. юр. наук. 12.00.01 – Теория и история права и государства; история учений о праве и государстве - Казань: 2011. - 26 с.
8. Нехайчик В.К. Административно-правовой статус и функции государственных корпораций в системе субъектов органов исполнительной власти Российской Федерации: проблемные вопросы // Сибирская финансовая школа. - 2016. - N 3(116). - С.11-16.
9. Цыгалов Ю.М., Бутова Т.В., Ординарцев И.И. Эффективность государственных корпораций в развитии депрессивных регионов // Управленческое консультирование. - 2017. - N 10(106). - С.46-58.
10. Биченов Д.Г. Каболов В.В. Законодательство о государственных корпорациях // Наука и современность – 2017: сборник материалов L Международной научно-практической конференции, Новосибирск, 20 января – 17 февраля 2017 года. - Новосибирск: Общество с ограниченной ответственностью "Центр развития научного сотрудничества", 2017. - С.166-172.
11. Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»
12. Electronic Warfare and Radar Systems. Engineering Handbook. - Point Mugu: Naval Air Warfare Centre Weapons Dision, 2013. - 455 p.
13. Li Y., Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments // Energy Reports. - 2021. - 11 p.
14. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студентов учреждений среднего профессионального образования, обучающихся по группе специальностей 2200 "Информатика и вычислительная техника". - М.: Форум, 2009. - 415 с.
15. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации: учебное пособие. СПб.: НИУ ИТМО, 2011. - 112 с.
16. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. N 114
17. Cyber attack trends: 2020 mid-year report. - Tel Aviv: Check Point Software Technologies LTD, 2021. - 27 p.
18. Mid-year update. 2020 SonicWall Cyber threat reports. - Milpitas: SonicWall Inc., 2020. - 30 p.
19. Актуальные киберугрозы: итоги 2020 года. - URL**:** https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/ (дата обращения 08.10.2021).
20. Mossburg E., Gelinne J., Calzada J. Beneath the surface of a cyber attack: A deeper look at business impacts. Technical Report. - London: Deloitte Development LLC. - 2016. - 28 p.
21. Isaca's cybersecurity nexus. http://new.groteck.ru/images/catalog/39049/5818630bf28bcbd9a93f676aa7169fae.pdf (дата обращения 09.10.2021).
22. Фалеев М.И., Черных Г.С. Угрозы национальной безопасности государства в информационной сфере и задачи МЧС России в этой области деятельности//Стратегия гражданской защиты: проблемы и исследования. - 2014. - Т.4. – N 1(6). - С.21-34.

References:

1. Stepanov K.S. State entrepreneurial function in the institution of state corporation. *Vestnik Saratov State Socio-economic University*. 2011;1(35):36-38. (In Russ)
2. Federal law from 12.01.1996 N7-FL "On non-profit organizations"(In Russ)
3. Ashtaeva S.S. State corporations in Russia, their formation and role in the development of the economy. *Law and State: the theory and practice.* 2013;12(108):140-146. (In Russ)
4. Panfilov K.S. Economic and political dimensions of the effectiveness of russian state corporations. *Business. Society. Rule*. 2019;2(32):45-63. (In Russ)

5. Ashtaeva S.S. State corporations in modern russia: functions, structure and peculiarities of activity. *Bulletin of the Kalmyk Institute for Humanities of the RAS.* 2012; 5(1):113-116. (In Russ)
6. Morales K., Grishchenko A.I. Corporations in Russia and foreign legal systems: the concept and essence (state corporations in modern Russia on the example of the State Corporation Rosatom). *Energy Law.* 2009; 1:19-29. (In Russ)
7. Kaplin S.Yu. State corporation as a subject of law: abstract. on the job. scientific step. candidate of legal sciences. 12.00.01 – Theory and history of law and the state; history of the teachings of law and the state - Kazan: 2011; 26 p. (In Russ)
8. Nekhajchik V.K. Administrative legal status and functions of the state corporations in system of subjects of executive authorities of the Russian Federation: problematic issues. *Siberian Financial School*. 2016; 3(116):.11-16. (In Russ)
9. Tsygalov Yu.M., Butova T.V., Ordinartsev I.I. Efficiency of the State Corporations in Depressive Regions Development. *Administrative Consulting*. 2017; 10(106):.46-58. (In Russ)
10. Bichenov D.G. Kabolov V.V. Legislation on state corporations. *Science and modernity – 2017: collection of materials of the L International Scientific and Practical Conference, Novosibirsk,* January 20 – February 17, 2017. - Novosibirsk: Limited Liability Company "Center for the Development of Scientific Cooperation", 2017;166-172. (In Russ)
11. Federal Law from 26.07.2017 № 187-FL "On the Security of the Critical Information Infrastructure of the Russian Federation"(In Russ)
12. Electronic Warfare and Radar Systems. Engineering Handbook. - Point Mugu: Naval Air Warfare Centre Weapons Dision, 2013; 455.
13. Li Y., Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*. 2021; 11.
14. Shangin V.F. Information security of computer systems and networks: a textbook for students of secondary vocational education institutions studying in the group of specialties 2200 "Computer Science and computer engineering". M.: Forum, 2009; 415. (In Russ)
15. Gatchin Yu.A., Klimova E.V. Introduction to complex protection of informatization objects: textbook. St. Petersburg: SRI ITMO, 2011; 112. (In Russ)
16. Guidance document. Protection against unauthorized access to information. Part 1. Information security software. Classification according to the level of control of the absence of undeclared opportunities. Approved by the decision of the Chairman of the State Technical Commission under the President of the Russian Federation dated June 4, 1999;114 (In Russ)
17. Cyber attack trends: 2020 mid-year report. Tel Aviv: *Check Point Software Technologies* LTD, 2021; 27.
18. Mid-year update. 2020 SonicWall Cyber threat reports. *Milpitas: SonicWall Inc*., 2020; 30.
19. Current cyber threats: results of 2020. URL**:** https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/ (Date of treatment 08.10.2021). (In Russ)
20. Mossburg E., Gelinne J., Calzada J. Beneath the surface of a cyber attack: A deeper look at business impacts. Technical Report. London: Deloitte Development LLC. 2016; 28.
21. Isaca's cybersecurity nexus. http://new.groteck.ru/images/catalog/39049/5818630bf28bcbd9a93f676aa7169fae.pdf (Date of treatment 09.10.2021).
22. Faleev M.I., Chernykh G.S. Threats to the national security of the state in the information sphere and the tasks of the MES of Russia in this field of activity. *Civil protection strategy: problems and research.* 2014; 1(6):.21-34. (In Russ)

Сведения об авторах:
Лоскутов Иван Андреевич, инженер – конструктор в отделе 55; магистрант; faxvex@ya.ru
Резниченко Сергей Анатольевич, кандидат технических наук, доцент; rsa_5@bk.ru
Information about authors:
Ivan A. Loskutov, Engineer-constructor in the Department 55, Master's Student; faxvex@ya.ru
Sergey A. Reznichenko, Cand.Sci. (Eng.), Assoc. Prof.; rsa_5@bk.ru
Конфликт интересов/Conflict of interest.
Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.
Поступила в редакцию/Received 01.08.2022.
Одобрена после рецензирования/ Reviced 26.08.2022.
Принята в печать/Accepted for publication 26.08.2022.