СБОРНИК **НАУЧНЫХ ТРУДОВ НГТУ. – 2019. – № 3–4 (96).** – 84–95

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.054.53 DOI: 10.17212/2307-6879-2019-3-4-84-95

РАЗРАБОТКА МЕТОДИКИ АУДИТА КИБЕРБЕЗОПАСНОСТИ ГИС, ОТНОСЯЩИХСЯ К ОБЪЕКТАМ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ*

В.Р. АН[1], В.В. СЕЛИФАНОВ[2], В.А. ТАБАКАЕВА[3], С.А. БУЛАРГА[4], А.С. ВОРОЖЦОВ[5]

[1] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, магистрант кафедры вычислительной техники. E-mail: vovan2011nsk@mail.ru*

[2] *630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, старший преподаватель кафедры защиты информации. E-mail: sfo1@mail.ru*

[3] *630108, РФ, г. Новосибирск, ул. Плахотного, 10, Сибирский государственный университет геосистем и технологий, магистрант кафедры фотоники и приборостроения. E-mail: tabakaeva1997@mail.ru*

[4] *111024, РФ, г. Москва, ул. Авиамоторная, 8а, Московский технический университет связи и информатики, доцент кафедры интеллектуальных систем в управлении и автоматизации. E-mail: s.bularga@gmail.ru*

[5] *111024, РФ, г. Москва, ул. Авиамоторная, 8а, Московский технический университет связи и информатики, кандидат технических наук, доцент кафедры интеллектуальных систем в управлении и автоматизации. E-mail: as.vorojcov@mail.ru*

В настоящей статье рассматривается проблема разработки методики аудита кибербезопасности государственных информационных систем, относящихся к объектам критической информационной инфраструктуры Российской Федерации. В соответствии с требованиями законодательства государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры будет проводиться с 2021 года. Однако в настоящее время не существует утвержденной и/или общепринятой методики аудита кибербезопасности ГИС, относящихся к объектам КИИ, в ходе государственного (межведомственного) контроля, в связи с этим возникает проблема интерпретации его результатов. На данный момент существует множество международных и отечественных рекомендаций и практик по проведению аудита кибербезопасности информационных систем, но они не соответствуют существующим и вновь принимаемым документам в сфере обеспечения кибербезопасности значимых объектов критической информационной инфраструктуры Российской Федерации и не мо-

* Статья получена 29 ноября 2019 г.

гут быть применимы без существенной доработки. Авторы рассматривают задачи, которые необходимо решить для разработки методики аудита, в том числе проводят анализ существующих законодательных, нормативных правовых актов Российской Федерации и уполномоченных в данной области федеральных органов исполнительной власти, методических документов и стандартов, а также возможных причин существующей ситуации. В результате исследования предложен алгоритм возможных действий при проведении аудита кибербезопасности в ходе проведения государственного контроля значимых объектов критической информационной инфраструктуры Российской Федерации, полученный в результате компиляции международных практик (стандартов) и требований, принятых в Российской Федерации, а также требования к необходимому инструментарию – к системам анализа уязвимостей и вспомогательному программному обеспечению (системам управления базами данных).

Ключевые слова: информационная безопасность, кибербезопасность, значимый объект, критическая информационная инфраструктура, государственная информационная система, межведомственный контроль, методика аудита кибербезопасности, оценка существующих методов аудита кибербезопасности

1. ПОСТАНОВКА ЗАДАЧИ

Из-за экспоненциального роста информатизации широкой области деятельности, особенно в сферах здравоохранения, науки, транспорта, связи, энергетики, в банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, в оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, растет потребность в обеспечении кибербезопасности. Соответственно в каждой из этих сфер критической информационной инфраструктуры (КИИ) функционируют информационные системы (далее – ИС), в том числе государственные информационные системы (ГИС), обрабатывающие информацию ограниченного доступа, которые нуждаются в обеспечении конфиденциальности, целостности и доступности. Федеральные органы исполнительной власти, уполномоченные в сфере обеспечения информационной безопасности (далее – ИБ), каждый год совершенствуют соответствующую нормативную правовую базу. На сегодняшний день для организаций, предприятий, органов государственной власти и органов местного самоуправления субъектов Российской Федерации актуальными являются Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», вступивший в силу с 1 января 2018 года, Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» с редакцией от 28 мая 2019 года, Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», Приказ ФСТЭК

России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

Особо важным с точки зрения органов исполнительной власти и органов местного самоуправления субъектов РФ при осуществлении защиты ГИС, относящихся к объектам КИИ, является построение системы кибербезопасности. Для этого в каждой подобной системе необходимо провести аудит ИБ. В данном случае рассматриваются ГИС, относящиеся к объектам КИИ. Аудит кибербезопасности – это форма государственного (межведомственного) контроля, который включает анализ рисков, связанных с возможностью осуществления угроз безопасности, особенно в отношении информационных ресурсов, оценку текущего уровня защищенности ГИС, оценку соответствия ГИС требованиям нормативно-правовых документов и существующим стандартам в области ИБ и выработку рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ГИС. Федеральная служба по техническому и экспортному контролю осуществляет межведомственный контроль в соответствии с приказом ФСТЭК России от 11 февраля 2013 г. № 17. В области КИИ межведомственный контроль будет осуществляться с 2021 года в соответствии с Постановлением Правительства РФ от 17 февраля 2018 года № 162 «Об утверждение правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» и Приказом ФСТЭК России от 25 декабря 2017 г. № 239.

В результате аудита кибербезопасности ожидается проведение оценки уровня безопасности ГИС, относящихся к объектам КИИ организации для управления ею в целом с учетом перспектив его развития. В современных условиях ГИС проникают во все сферы деятельности системы государственной власти и органов местного самоуправления, а с учетом необходимости их связи с интернет-сетью они оказываются открытыми для реализации угроз внутренними и внешними нарушителями разного потенциала. Проблема ИБ становится не менее важной, чем экономическая или физическая безопасность. Несмотря на важность рассматриваемой проблемы, в настоящее время не уделяется достаточного внимания выполнению работ, связанных с аудитом кибербезопасности ГИС, относящихся к объектам КИИ региональных органов исполнительной власти и органов местного самоуправления. Это связано прежде всего с отсутствием необходимой нормативной правовой базы и методик, с неподготовленностью специалистов и недостаточным практическим опытом в области проведения аудита кибербезопасности.

В настоящей статье понятия «защита информации», «информационная безопасность» и «кибербезопасность» считаются тождественными.

2. МЕТОДЫ И РЕЗУЛЬТАТЫ

Для решения проблемы, описанной в настоящей статье, необходимо разработать и апробировать методику аудита кибербезопасности ГИС, относящихся к объектам КИИ.

Для реализации цели необходимо решить следующие задачи:

1) провести анализ требований к системе кибербезопасности ГИС, относящихся к объектам КИИ;

2) провести анализ существующего нормативно-методического аппарата аудита кибербезопасности ГИС;

3) разработать методику аудита кибербезопасности;

4) провести ее апробацию.

В настоящей статье предполагается что объектом исследования является система кибербезопасности ГИС, относящихся к объектам КИИ, а предметом исследования – процесс проведения ее аудита.

В результате выполнения поставленной цели и задач будет разработана методика аудита кибербезопасности ГИС, относящихся к объектам КИИ, и обоснованы критерии при проведении аудита кибербезопасности, на основе которых будет оцениваться защищенность свойств ИБ.

Основной особенностью аудита является включение его в состав процедуры государственного контроля, что накладывает на него жесткие требования по неукоснительному соблюдению всех требований и положений следующих видов документов:

– законодательных актов РФ;

– нормативных правовых актов РФ и федеральных органов государственной власти;

– методических документов;

– международных и национальных стандартов, признанных обязательными в данной сфере.

Кроме того, необходимо уточнить требования к инструментарию, применяемому при проведении аудита. Помимо применения сертифицированных систем анализа защищенности (уязвимостей) необходимо использовать дополнительное программное обеспечение, позволяющее интерпретировать результаты с высокой достоверностью и оперативностью.

Если требования к средствам анализа защищенности (уязвимостей) достаточно понятны и определены в Приказе № 239 ФСТЭК России, то дополнительные инструменты необходимо рассмотреть более подробно.

В действительности такое программное обеспечение будет представлять базу данных, содержащую следующую информацию:

– данные по существующим уязвимостям в форме и объеме, позволяющих максимально быстро их интерпретировать вне зависимости от применяемых сканеров уязвимостей;

– оценивать уровень уязвимости и актуальность возможных угроз безопасности с учетом особенности каждого проверяемого объекта;

– сравнивать полученные результаты с результатами контроля на других подобных объектах.

Если рассматривать существующие методы, то в общем случае аудит ИБ включает в себя следующее:

– проведение оценки рисков, связанных с вероятностью реализации угроз безопасности в отношении активов;

– оценку текущего состояния защищенности информационной системы;

– оценку соответствия информационной системы существующим стандартам в области ИБ.

– выработку рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ИС;

– получение максимальной отдачи от средств, инвестируемых в создание (совершенствование, модернизацию) комплексной системы ИБ.

Аудит ИБ можно разделить на следующие категории:

– экспертный аудит безопасности, в ходе которого выявляются уязвимости в системе мер защиты информации (ЗИ) на основе опыта экспертов, участвующих в процедуре обследования;

– оценка соответствия рекомендациям нормативных правовых документов (международным и российским стандартам и др.);

– инструментальный анализ состояния защищенности ИС, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечения системы;

– комплексный аудит, включающий в себя все вышеперечисленные формы проведения обследования.

Для проведения аудита ИБ можно использовать следующий алгоритм:

1) выбор объекта аудита (организация, отдельные здания и помещения, отдельные системы или их компоненты);

2) составление команды аудиторов-экспертов;

3) определение цели, объема, масштаба аудита и установление конкретных сроков работы;

4) общая оценка состояния защищенности объекта аудита;

5) регистрация, сбор и проверка статистических данных;

6) оценка результатов технического контроля;

7) составление отчета о результатах проверки по частям;

8) составление итогового отчета;

9) разработка плана мероприятий по устранению уязвимостей и недостатков в обеспечении безопасности предприятия.

Все известные методы проведения аудита основаны на серии стандартов ГОСТ Р ИСО/МЭК 27000. Соответственно, требования законодательных и нормативно-правовых актов, МД по ЗИ в отношении ГИС, относящихся к объектам КИИ, не выполняются [1–6].

ЗАКЛЮЧЕНИЕ

В работе была рассмотрена проблема разработки методики аудита кибербезопасности ГИС, относящихся к объектам КИИ.

Обозначена важность данной проблемы и описаны причины ее возникновения, рассмотрены и обобщены существующие методики, а также сформулированы и поставлены цели и задачи для решения данной проблемы.

В дальнейшем будет разработана методика аудита кибербезопасности ГИС, относящихся к объектам КИИ РФ, и рекомендации по использованию модели, а также критерии при проведении аудита кибербезопасности, на основе которых будет оцениваться защищенность свойств ИБ.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.

2. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (в редакции от 28 мая 2019 года).

3. Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

4. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

5. Методический документ. Меры защиты в государственных информационных системах: утвержден ФСТЭК России 11 февраля 2014 г.

6. Методический документ. Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении: утверждена ФСТЭК России 11 февраля 2019 г.

7. О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: Указ Президента Российской Федерации от 22 декабря 2017 года № 620 // КонсультантПлюс: web-сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_285915/ (дата обращения: 18.11.2019).

8. О Национальном координационном центре по компьютерным инцидентам (вместе с Положением о Национальном координационном центре по компьютерным инцидентам): Приказ ФСБ России от 24 июля 2018 года № 366 // КонсультантПлюс: web-сайт. – URL: http://www.consultant.ru/document/cons_doc_LAW_306334/ (дата обращения: 18.11.2019).

9. *Потапова Д.А.*, *Журавлев С.И.* Оценка ущерба от компьютерных инцидентов для критической информационной инфраструктуры // Материалы 45-й Международной научно-технической конференции молодых ученых, аспирантов и студентов: в 2 т. – Уфа, 2018. – Т. 1. – С. 447–454.

10. *Будовских И.А., Загинайлов Ю.Н.* Оценка применимости для аудита безопасности государственных ИС методики определения угроз безопасности информации, разработанной ФСТЭК России // Измерение, контроль, информатизация: материалы XVII международной научно-технической конференции. – Барнаул, 2016. – С. 240–243.

11. *Гисматов А.Р., Байрушин Ф.Т.* Особенности специфики применения документов ФСТЭК России в области защиты государственных информационных систем // Актуальные проблемы социального, экономического и информационного развития современного общества: Всероссийская научно-практическая конференция, посвященная 100-летию со дня рождения первого ректора Башкирского государственного университета Чанбарисова Шайхуллы Хабибулловича. – Уфа, 2016. – Ч. 1. – С. 53–55.

12. *Сплюхин Д.В., Николаев Д.Б.* Анализ новейших требований ФСТЭК и общие решения существующих проблем защиты информационных систем // Математика и математическое моделирование: сборник материалов X Всероссийской молодежной научно-инновационной школы. – Саров, 2016. – С. 28–29.

13. *Портнова А.С.* Анализ современных нормативно-методических документов ФСТЭК России в области систем обнаружения вторжений // Безопасные информационные технологии: Восьмая Всероссийская научно-техническая конференция: сборник трудов конференции / под ред. М.А. Басараба. – М., 2017. – С. 340–346.

14. Подход к созданию центров обработки персональных данных в организациях, обеспечивающих защиту государственных информационных ресурсов / В.Н. Труфанов, Д.А. Щевелев, И.В. Демидов, С.В. Совалин // Информатизация и связь. – 2018. – № 1. – С. 56–62.

15. *Агеев В.О., Шилов А.К.* Обеспечение защиты ГИС в зарубежных и отечественных системах // Информационное противодействие угрозам терроризма. – 2015. – № 24. – С. 312–315.

16. *Горян Э.В.* Ведущая роль Сингапура в обеспечении кибербезопасности в АСЕАН: промежуточные результаты и перспективы дальнейшего расширения // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. – 2018. – Т. 10, № 3. – С. 101–116.

17. Вопросы Федеральной службы по техническому и экспортному контролю: Указ Президента РФ от 16.08.2004 № 1085 (ред. от 08.05.2018) // КонсультантПлюс: web-сайт. – URL: www.consultant.ru/document/cons_doc_LAW_14031/ (дата обращения: 18.11.2019).

Ан Владимир Робертович, магистрант кафедры вычислительной техники Новосибирского государственного технического университета. E-mail: vovan2011nsk@mail.ru

Табакаева Валерия Александровна, магистрант кафедры фотоники и приборостроения Сибирского государственного университета геосистем и технологий. E-mail: tabakaeva1997@mail.ru

Селифанов Валентин Валерьевич, старший преподаватель кафедры защиты информации Новосибирского государственного технического университета. E-mail: sfo1@mail.ru

Буларга Сергей Андреевич, доцент кафедры интеллектуальных систем в управлении и автоматизации Московского технического университета связи и информатики. E-mail: s.bularga@gmail.ru

Ворожцов Анатолий Сергеевич, кандидат технических наук, доцент кафедры интеллектуальных систем в управлении и автоматизации Московского технического университета связи и информатики. E-mail: as.vorojcov@mail.ru

DOI: 10.17212/2307-6879-2019-3-4-84-95

Development of a GIS cybersecurity audit methodology related to critical information infrastructure facilities of the Russian Federation*

V.R. An[1], V.V. Selifanov[2], V.A. Tabakaeva[3], S.A. Bularga[4], A.S. Vorozhtsov[5]

[1] *630073, Russian Federation, Novosibirsk, Karl Marx Prospekt 20, Novosibirsk State Technical University, Master of the Department Information Security. E-mail: vovan2011nsk@mail.ru*
[2] *630073, Russian Federation, Novosibirsk, Karl Marx Prospekt 20, Novosibirsk State Technical University, Senior Lecturer at the Department of Information Security. E-mail: sfo1@mail.ru*
[3] *630108, Russian Federation, Novosibirsk, ul. Plahotnogo 10, Siberian State University of Geosystems and Technologies, Master of the Department of Photonics and Instrument Engineering. E-mail: tabakaeva1997@mail.ru*
[4] *111024, Russian Federation, Moscow, ul. Aviamotornaya, 8a, Moscow Technical University of Communications and Informatics, assistant professor of intelligent systems in management and automation. E-mail: s.bularga@gmail.ru*
[5] *111024, Russian Federation, Moscow, ul. Aviamotornaya, 8a, Moscow Technical University of Communications and Informatics, Ph.D., associate professor of the Department of Intelligent Systems in Management and Automation. E-mail: as.vorojcov@mail.ru*

This article discusses the problem of developing a cybersecurity audit methodology for state information systems (hereinafter - GIS) related to the objects of critical information infrastructure (hereinafter - KII) of the Russian Federation. In accordance with the requirements of the legislation, state control in the field of ensuring the security of significant objects of critical information infrastructure will be carried out from 2021. However, at present, there is no approved and / or generally accepted methodology for the audit of GIS cybersecurity related to KII objects, the entrance of state (interdepartmental) control, and this raises the problem of interpreting its results. At the moment, there are many international and domestic recommendations and practices for conducting a cybersecurity audit of information systems, but they do not comply with existing and newly adopted documents in the field of cybersecurity of significant objects of critical information infrastructure of the Russian Federation and cannot be applied without significant revision. The authors consider the tasks that need to be solved to develop an audit methodology, including an analysis of existing legislative and regulatory legal acts of the Russian Federation and federal executive bodies authorized in this field, methodological documents and standards, as well as possible causes of the existing situation. As a result of the study, an algorithm is proposed for possible actions in conducting a cybersecurity audit during state control of significant objects of critical information infrastructure of the Russian Federation, obtained as a result of a compilation of international practices (standards) and requirements adopted in the Russian Federation, as well as requirements for the necessary tools – vulnerability analysis systems and supporting software (database management systems).

* *Received 29 November 2019.*

Keywords: information security, cybersecurity, significant object, critical information infrastructure, state information system, interagency control, cybersecurity audit methodology, assessment of existing methods of cybersecurity audit

REFERENCES

1. RF Federal Law “On the security of critical information infrastructure of the Russian Federation” of July 26, 2017 N 187-FZ. (In Russian).

2. Order of the FSTEC of Russia of February 11, 2013 N 17 “On approval of requirements for the protection of information not constituting state secrets contained in state information systems” with the edition of May 28, 2019. (In Russian).

3. Order of the FSTEC of Russia of December 21, 2017 N 235 “On approval of requirements for the creation of security systems for significant objects of critical information infrastructure of the Russian Federation and ensuring their functioning”. (In Russian).

4. Order of the FSTEC of Russia dated December 25, 2017 N 239 “On approval of requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation”. (In Russian).

5. Methodical document FSTEC of Russia. Security measures in state information systems. (In Russian).

6. Methodical document FSTEC of Russia. Methodology for identifying vulnerabilities and undeclared features in software. (In Russian).

7. On improving the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation. Decree of the President of the Russian Federation dated December 22, 2017 N 620. *Konsul'tantPlyus* [Consultant Plus]: website. (In Russian). Available at: http://www.consultant.ru/document/cons_doc_LAW_285915/ (accessed 18.11.2019).

8. About the National coordination center for computer incidents (together with the Regulation on the National coordination center for computer incidents). Order of the FSB of Russia of July 24, 2018 N 366. *Konsul'tantPlyus* [Consultant Plus]: website. (In Russian). Available at: http://www.consultant.ru/document/cons_doc_LAW_306334/ (accessed 18.11.2019).

9. Potapova D.A., Zhuravlev S.I. [Estimation of damage from computer incidents for critical information infrastructure]. *Materialy 45-i Mezhdunarodnoi nauchno-tekhnicheskoi konferentsii molodykh uchenykh, aspirantov i studentov* [Materials of the 45th International scientific and technical conference of young scientists, graduate students and students]. Ufa. 2018, vol. 1, pp. 447–454. (In Russian).

10. Budovskikh I.A., Zaginailov Yu.N. [Assessment of the applicability for the security audit of state IP methods of determining threats to the security of infor-

mation developed by the FSTEC of Russia]. *Izmerenie, kontrol', informatizatsiya*: *materialy XVII mezhdunarodnoi nauchno-tekhnicheskoi konferentsii* [Measurement, control, informatization: materials of the XVII International scientific and technical conference], Barnaul, 2016, pp. 240–243. (In Russian).

11. Gismatov A.R., Bairushin F.T. [Specific features of the application of documents of the FSTEC of Russia in the field of protection of state information systems]. *Aktual'nye problemy sotsial'nogo, ekonomicheskogo i informatsionnogo razvitiya sovremennogo obshchestva: Vserossiiskaya nauchno-prakticheskaya konferentsiya, posvyashchennaya 100-letiyu so dnya rozhdeniya pervogo rektora Bashkirskogo gosudarstvennogo universiteta Chanbarisova Shaikhully Khabibullovicha* [Actual problems of the social, economic and informational development of modern society: All-Russian scientific and practical conference dedicated to the 100th anniversary of the first rector of Bashkir State University Chanbarisov Shaikhulla Khabibullovich], Ufa, 2016, pt. 1, pp. 53–55. (In Russian).

12. Splyukhin D.V., Nikolaev D.B. [Analysis of the latest requirements of the FSTEC and general solutions to existing problems of protecting information systems]. *Matematika i matematicheskoe modelirovanie: sbornik materialov X Vserossiiskoi molodezhnoi nauchno-innovatsionnoi shkoly* [Mathematics and mathematical modeling: a collection of materials of the X All-Russian youth scientific and innovative school], Sarov, 2016, pp. 28–29. (In Russian).

13. Portnova A.S. [Analysis of modern regulatory and methodological documents of FSTEC of Russia in the field of intrusion detection systems]. *Bezopasnye informatsionnye tekhnologii: Vos'maya Vserossiiskaya nauchno-tekhnicheskaya konferentsiya* [Safe information technologies: proceedings of the Eighth All-Russian scientific and technical conference]. Moscow, 2017, pp. 340–346. (In Russian).

14. Trufanov V.N., Shchevelev D.A., Demidov I.V., Sovalin S.V. Podkhod k sozdaniyu tsentrov obrabotki personal'nykh dannykh v organizatsiyakh, obespechivayushchikh zashchitu gosudarstvennykh informatsionnykh resursov [Approach to the creation of personal data processing centers in organizations that ensure the protection of state information resources]. *Informatizatsiya i svyaz' – Informatization and Communication*, 2018, no. 1, pp. 56–62.

15. Ageev V.O., Shilov A.K. Obespechenie zashchity GIS v zarubezhnykh i otechestvennykh sistemakh [GIS protection in foreign and domestic systems]. *Informatsionnoe protivodeistvie ugrozam terrorizma – Information counteraction to threats of terrorism*, 2015, no. 24, pp. 312–315.

16. Goryan E.V. Vedushchaya rol' Singapura v obespechenii kiberbezopasnosti v ASEAN: promezhutochnye rezul'taty i perspektivy dal'neishego rasshireniya [The leading role of Singapore in ensuring cyber security in ASEAN: intermediate results and prospects for further expansion]. *Territoriya novykh vozmozhnostei. Vest-*

nik Vladivostokskogo gosudarstvennogo universiteta ekonomiki i servisa, 2018, vol. 10, no. 3, pp. 101–116.

17. Issues of the Federal Service for Technical and Export Control. Decree of the President of the Russian Federation of 08.16.2004 N 1085 (as amended on 05.08.2018). *Konsul'tantPlyus* [Consultant Plus]: website. (In Russian). Available at: www.consultant.ru/document/cons_doc_LAW_14031/ (accessed 18.11.2019).

Для цитирования:

Разработка методики аудита кибербезопасности ГИС, относящихся к объектам критической информационной инфраструктуры Российской Федерации / В.Р. Ан, В.В. Селифанов, В.А. Табакаева, С.А. Буларга, А.С. Ворожцов // Сборник научных трудов НГТУ. – 2019. – № 3–4 (96). – С. 84–95. – DOI: 10.17212/2307-6879-2019-3-4-84-95.

For citation:

An V.R., Selifanov V.V., Tabakaeva V.A., Bularga S.A., Vorozhtsov A.S. Razrabotka metodiki audita kiberbezopasnosti GIS, otnosyashchikhsya k ob"ektam kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii [Development of a GIS cybersecurity audit methodology related to critical information infrastructure facilities of the Russian Federation]. *Sbornik nauchnykh trudov Novosibirskogo gosudarstvennogo tekhnicheskogo universiteta – Transaction of scientific papers of the Novosibirsk state technical university*, 2019, no. 3–4 (96), pp. 84–95. DOI: 10.17212/2307-6879-2019-3-4-84-95.