УДК 004.056

БЕЗОПАСНОСТЬ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

1Гончаров И.В., 1Гончаров Н.И.,
1Кирсанов Ю.Г., 2Райков О.В.

1Акционерное общество «Научное производственное объединение «Инфобезопасность», 394018, Россия, г. Воронеж, ул. Куколкина,д. 9, оф. 402, e-mail: manager@infobez.org

2Федеральная служба по техническому и экспортному контролю

На основе практического опыта и с учетом совершенствования нормативно-методической базы по безопасности информации рассмотрены основные аспекты в государственных информационных системах с учетом того, что они могут являться информационными системами персональных данных и системами общего пользования, при защите информации, не составляющей государственную тайну.

Ключевые слова: государственная информационная система; информационная система персональных данных; государственная система общего пользования; информация, не составляющая государственную тайну; персональные данные; модель угроз; модель нарушителя; аттестация

SECURITY IN STATE INFORMATION SYSTEMS

1Goncharov I.V., 1Goncharov N.I.,
1Kirsanov Y.G., 2Raykov O.V.

1 Joint Stock Company "Scientific Production Association "Infobezopasnost", 394018, Russia, Voronezh, Kukolkina str. 9, Kukolkina str. 402, e-mail: manager@infobez.org

 2*Federal Service for Technical and Export Control*

Based on practical experience and taking into account the improvement of the regulatory and methodological framework for information security, the main aspects of state information systems have been considered, taking into account the fact that they may be information systems for personal data and public use, while protecting information that does not constitute state secrets.

Keywords: state information system; information system of personal data; information not constituting state secret; personal data; model of threat; model of violator; attestation.

За 2019 год число государственных информационных систем (ГИС) значительно возросло. В государственных информационных системах (далее – ГИС) [1] часто циркулируют персональные данные [2]. Такие ГИС обладают характеристиками информационных систем персональных данных (далее – ИСПДн) [3]. С ростом числа ГИС возрастает и число пользователей ГИС. В связи с этим в организациях, как государственных, так и коммерческих, возникает необходимость создания рабочих мест для работы с ГИС с разным уровнем доступа к ресурсам информационных систем. Сильному увеличению объема обрабатываемых ресурсов способствует соотнесение отдельных структур ГИС информационным системам общего пользования [4].

В соответствии с Требованиями по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (далее – Требования), лицо, обрабатывающее информацию, являющуюся государственным информационным ресурсом, по поручению обладателя информации (заказчика) или оператора и (или) предоставляющее им вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора, обеспечивает защиту информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации, и уполномоченное лицо должно обеспечивать защиту информации, являющейся государственным информационным ресурсом, в соответствии с Требованиями [1].

Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

1. Формирование требований по защите информации, содержащейся в информационной системе;

2. Разработка системы защиты информации информационной системы;

3. Внедрение системы защиты информации информационной системы;

4. Аттестация информационной системы по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие;

5. Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы [5, 6];

6. Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации [6].

В работе [3] был рассмотрен порядок системного подхода к соблюдению актуальных требований по защите персональных данных (ПДн) в рамках анализа состояния информационных систем персональных данных (ИСПДн) различного применения, алгоритм проведения анализа ИСПДн, были выделены важные аспекты для подготовки и создания таких систем и их систем защиты, а также принятия мер по защите ПДн [7, 8]. Классификация ИСПДн упразднена [9].

Для классификации государственных информационных систем (ГИС) используют три класса защищенности, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – третий, самый высокий – первый [4].

Существуют ГИС общего пользования, используемые в целях реализации полномочий федеральных органов исполнительной власти и содержащие сведения о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти, обязательные для размещения в информационно-телекоммуникационной сети Интернет, определяемые Правительством Российской Федерации (далее – информационные системы общего пользования), и являются обязательными для операторов информационных систем общего пользования при разработке и эксплуатации информационных систем общего пользования. Их ресурсы обязательно должны соответствовать характеристикам целостности и доступности определенного уровня. Данные системы классифицируются на два класса. Требования к защите информации, циркулирующей в них, определены в соответствующем совместном приказе Федеральных органов исполнительной власти [4].

В работе [10] предложено применение алгоритма [3] для проведения анализа защищенности ГИС.

В данном алгоритме обособлены следующие этапы:

1. Сбор и анализ исходных данных;

2. Определение перечня угроз безопасности в информационной системе (ИС) (в соответствии с [1, 8, 10, 11] и банком данных угроз безопасности информации (адрес: www.bdu.fstec.ru));

3. Формирование модели нарушителя (в соответствии с [1, 10]);

4. Определение актуальных угроз (в соответствии с [1, 10, 11]);

5. Определение уровня защищенности ИС (в соответствии с [12]).

6. Определение класса защищенности ИС (в соответствии с [1]).

7. Определение мер и средств по обеспечению безопасности ИС в соответствии с [1, 13, 14, 15]).

8. Формирование пакета документов.

Для понижения требуемого уровня защищенности могут использоваться методы и процедуры по обезличиванию персональных данных, обрабатываемых в ГИС, рассмотренные в [16,17].

В отличие от ИСПДн, ГИС в соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [1] требуют обязательной аттестации.

В качестве исходных данных, необходимых для аттестации информационной системы, используются следующие документы:

1. Модель угроз безопасности информации, которая должна содержать:

- описание информационной системы и ее структурно- функциональных характеристик;

- описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации [18].

2. Акт классификации информационной системы.

3. Техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, которые должны содержать:

- цель и задачи обеспечения защиты информации в информационной системе;

- класс защищенности информационной системы;

- перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система; перечень объектов защиты информационной системы;

- требования к мерам и средствам защиты информации, применяемым в информационной системе;

- стадии (этапы работ) создания системы защиты информационной системы [19, 20];

- требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;

- функции заказчика и оператора по обеспечению защиты информации в информационной системе;

- требования к защите средств и систем, обеспечивающих функционирование информационной системы (обеспечивающей инфраструктуре);

- требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

4. Проектная и эксплуатационная документация на систему защиты информации информационной системы.

5. Организационно-распорядительные документы по защите информации, которые должны определять правила и процедуры:

- управления (администрирования) системой защиты информации информационной системы;

- выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности информации (далее - инциденты), и реагирования на них;

- управления конфигурацией аттестованной информационной системы и системы защиты информации информационной системы;

- контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

- защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации.

6. Результаты анализа уязвимостей информационной системы, которые должны подтверждать, что в информационной системе отсутствуют уязвимости, содержащиеся в банке данных угроз безопасности информации ФСТЭК России [21], а также в иных источниках, или их использование (эксплуатация) нарушителем невозможно.

7. Материалы предварительных и приемочных испытаний системы защиты информации информационной системы.

8. Иные документы, разрабатываемые в соответствии с необходимыми Требованиями [1].

Аттестация информационной системы проводится в соответствии с программой и методиками аттестационных испытаний до начала обработки информации, подлежащей защите в информационной системе.

По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии информационной системы требованиям о защите информации и аттестат соответствия в случае положительных результатов аттестационных испытаний. Аттестат соответствия выдается на весь срок эксплуатации информационной системы. Оператор (обладатель информации) в ходе эксплуатации информационной системы должен обеспечивать поддержку соответствия системы защиты информации аттестату соответствия в рамках реализации мероприятий, предусмотренных пунктом 18 Требований [1].

Таким образом, в настоящей статье на основе практического опыта рассмотрены основные проблемы, возникающие при обеспечении безопасности информации в ГИС.

Список литературы

1. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2. Федеральный Закон РФ от 27 июля 2006 г. №152-ФЗ «О персональных данных».

3. Гончаров И.В., Райков О.В. и др. Порядок проведения анализа состояния информационной системы персональных данных различного применения. Вестник ВГУ, серия: системный анализ и информационные технологии, 2014, № 3.

4. Приказ Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю от 31 августа 2010г. № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования».

5. «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 года № 152.

6. Постановление Правительства Российской Федерации от 6 июля 2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

7. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн».

8. «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31 марта 2015 г.).

9. Приказ от 31 декабря 2013 г. № 151/786/461 «О признании утратившим силу приказа Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля 2008 года № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

10. Гончаров И.В., Райков О.В. и др. Порядок проведения анализа состояния информационной системы персональных данных различного применения в рамках выполнения требований по защите информации. ИТ-Стандарт. 2015. Т. 1. № 4-1 (5).

11. Методический документ «Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн», ФСТЭК России, 14 февраля 2008 г.

12. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите ПДн при их обработке в ИСПДн».

13. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

14. Методический документ «Меры защиты информации в государственных информационных системах», ФСТЭК России, 11 февраля 2014 г.

15. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите ПДн для каждого из уровней защищенности».

16. Гончаров И.В., Райков О.В. и др. Проблемы обеспечения безопасности информационных систем персональных данных и государственных информационных систем. ИТ-Стандарт. 2017.

17. Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными операторами, являющимися государственными или муниципальными органами».

18. Методический документ «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн», ФСТЭК России, 14 февраля 2008 г.

19. Информационное сообщение ФСБ России О нормативно- методических документах, действующих в области обеспечения безопасности персональных данных от 21.06.2016.

20. Приказ ФСБ России от 9 февраля 2005 года № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

21. Информационное сообщение о банке данных угроз безопасности информации ФСТЭК России от 6 марта 2015 г. № 240/22/879.

References

1. Order of the FSTEC of Russia No. 17 of 11 February 2013 "On Approval of Requirements for the Protection of Information Not constituting State Secrets contained in State Information Systems".

2. Federal Law of the Russian Federation dated July 27, 2006 No. 152-FZ "On Personal Data".

3. Goncharov I.V., Raikov O.V., etc. Procedure for analyzing the status of the information system of personal data of various applications. Vestnik VSU, series: System Analysis and Information Technologies, 2014, № 3.

4. Order of the Federal Security Service of the Russian Federation, Federal Service for Technical and Export Control of August 31, 2010 № 416/489 "On Approval of Requirements for the protection of information contained in public information systems".

5. "Instruction on the organisation and safety of storage, processing and transfer through communication channels with use of means of cryptographic protection of the information with the limited access, not containing the data making the state secret", confirmed by order FAPSI from June, 13th, 2001 № 152.

6. The governmental order of the Russian Federation from July 6, 2015 № 676 "About requirements to the order of creation, development, commissioning, operation and a conclusion out of operation of the state information systems and the further storage of the information containing in their databases".

7. Order of FSTEC of Russia No. 21 of February 18, 2013 "On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Safety of PDNs during their Processing in ISPDN".

8. 8. "Methodological recommendations for the development of regulatory legal acts that define the threats to the security of personal data relevant to the processing of personal data in the information systems of personal data used in the implementation of relevant activities", approved by the management of the 8th Center of the FSB of Russia (№ 149/7/2/6-432 of March 31, 2015).

9. Order of December 31, 2013 № 151/786/461 "On the invalidation of the order of the Federal Service for Technical and Export Control, the Federal Security Service of the Russian Federation and the Ministry of Information Technology and Communications of the Russian Federation dated February 13, 2008 № 55/86/20 "On approval of the procedure for classification of information systems of personal data.

10. 10. Goncharov I.V., Raikov O.V. et al. The order of carrying out of the analysis of a condition of information system of the personal data of various application within the limits of performance of requirements on information protection. IT-Standard. 2015. Т. 1. № 4-1 (5).

Methodological document "Methodology for Determining Actual Security Threats to Personal Data when Processing them in ISPDn", FSTEC, 14 February 2008.

12. Resolution of the Government of the Russian Federation No. 1119 dated 1 November 2012 "On Approval of Requirements for the Protection of Personal Data Protection during their Processing at ISPDn".

13. The order of the Ministry of Communications of Russia from September 05, 2013 № 996 "About the statement of requirements and methods on depersonalization of personal data".

14. Methodical document "Information protection measures in state information systems", FSTEC of Russia, 11 February 2014.

15. Order of the Federal Security Service of Russia No. 378 dated July 10, 2014 "On approval of the composition and content of organizational and technical measures to ensure the security of personal data during their processing in ISPDN using the means of cryptographic protection of information necessary to meet the requirements for the protection of personal data established by the Government of the Russian Federation for each level of security".

16. 16. Goncharov I.V., Raikov O.V. et al. Problems of Securing Information Systems of Personal Data and State Information Systems. IT-Standard. 2017.

17. Resolution of the Government of the Russian Federation dated March 21, 2012 No. 211 "On approval of the list of measures aimed at ensuring the fulfillment of obligations under the Federal Law "On Personal Data" and regulatory legal acts adopted in accordance with it, operators who are state or municipal operators who are state or municipal authorities".

18. Methodological document "Basic model of PDN security threats when processed at ISPDN", FSTEC of Russia, 14 February 2008.

19. Information message of FSB of Russia On normative and methodical documents acting in the field of personal data security from 21.06.2016.

20. Order of FSB of Russia dated February 9, 2005 № 66 "On approval of the development, production, implementation and operation of encryption (cryptographic) means of information protection (PKZ-2005 Regulations)".

21. Information message about the databank of threats to information security of FSTEC of Russia dated March 6, 2015 № 240/22/879.