# ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ И ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

**[1]Гончаров И.В., [1]Гончаров Н.И., [1]Кирсанов Ю.Г., [1]Паринов П.А., [2]Райков О.В.**

*[1]Закрытое акционерное общество «Научное производственное объединение «Инфобезопасность», 394018, Россия, г. Воронеж, ул. Куколкина, д. 9, оф. 402, e-mail: manager@infobez.org*
*[2]Федеральная служба по техническому и экспортному контролю*

**На основе практического опыта рассмотрены основные проблемы, изменения нормативно-методической документации по защите информации в информационных системах персональных данных и по защите информации, не составляющей государственную тайну в рамках анализа состояния государственных информационных системах.**

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

# PROBLEMS OF SECURITY OF INFORMATION SYSTEMS AND GOVERNMENT OF PERSONAL DATA INFORMATION SYSTEMS

**[1]Goncharov I.V., [1] Goncharov N.I., [1]Kirsanov Y.G., [1]Parinov P.A., [2]Raykov O.V.**

*[1]LJSC «IRC «Infosecurity», 394018, st. Kukolkina 9-402, e-mail: manager@infobez.org*
*[2]The Federal Service for Technical and Export Control*

**On the basis of practical experience of the main problems, legislative changes data protection in personal data information systems, regulatory and procedural documents and data protection, not constituting a state secret within the analysis of the state information systems.**

Keywords: personal data; information systems of personal data; state information system; Model threats; Model offender; information does not constitute a state secret, problems of protection of personal data, validation

В работе [1] 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, также принятия мер по защите ПДн. В работе [2] предложено применение алгоритма [1] для проведения анализа защищенности государственной информационной системы (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 [2, 3, 4] и банком данных угроз безопасности информации (адрес: www.bdu.fstec.ru));
3. Формирование модели нарушителя (в соответствии с [2, 4]);
4. Определение актуальных угроз (в соответствии с [2, 3, 4]);
5. Определение уровня защищенности ИС (в соответствии с [5]). Определение класса защищенности ИС (в соответствии с [6]).
6. Определение мер и средств по обеспечению безопасности ИС (в соответствии с [6, 7, 8]).
7. Формирование пакета документов.
Одним из основных этапов [1, 2] анализа системы является определение перечня актуальных угроз безопасности в информационной системе и формирование модели нарушителя, на основании которых происходит определение требуемого уровня защищенности ИС, класса защищенности ГИС и без которых невозможно определение корректных мер и средств по обеспечению безопасности ИС. В настоящее время определение угроз следует проводить в соответствии с «Базовой моделью угроз безопасности ПДн при их обработке в ИСПДн», ФСТЭК России [9] и «Методикой определения актуальных угроз безопасности ПДн при их обработке в ИСПДн», ФСТЭК России [4]. Данный документ [9] содержит положения, которые

требуют обновления. В 2015 году ФСТЭК России был опубликован проект новой Методики определения угроз безопасности информации в информационных системах [4], которая должна учитывать применение банка данных угроз безопасности информации, созданного ФСТЭК России в том же году [10]. Однако, документ так и остался проектом. К тому же, наполнение банка данных угроз безопасности происходит не так эффективно, как требует современное развитие информационных технологий.

Согласно приказу ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» требуется проведение аттестации ГИС [6]. В настоящее время не приняты соответствующие нормативно-методические документы по проведению аттестации ГИС. При этом зачастую аттестацию заказчик рассматривает как разовое мероприятие по обеспечению информационной безопасности. Закупаются средства защиты информации (СЗИ), разрабатываются организационно распорядительные документы (ОРД), но после аттестации про обеспечение информационной безопасности забывают. Однако обеспечение информационной безопасности - это непрерывный процесс, а не разовое мероприятие, в ходе которого требуется периодический пересмотр модели угроз, обновление СЗИ, устранение уязвимостей, актуализация ОРД, обучение, инструктирование пользователей и администраторов безопасности ИС.

Произошли изменения в нормативно-методических документах, ФСБ России, действующих в области обеспечения безопасности персональных данных. Согласно информационному сообщению ФСБ России от 21.06.2016 [11] в связи с завершением действия постановления Правительства Российской Федерации от 17 ноября 2007 года № 781 «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» и «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» утратили актуальность. Поэтому, в случае решения оператора использовать средства криптографической защиты информации (СКЗИ) следует руководствоваться следующими нормативно-методическими документами ФСБ России:

1) Приказ ФСБ от 10 июля 2014 года № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

2) 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)»;

3) «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;

4) «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 31.03.2015).

Таким образом, в настоящей статье на основе практического опыта рассмотрены основные проблемы, возникающие при обеспечении безопасности ИСПДн и ГИС, при аттестации ГИС, и изменения в нормативно-методических документах ФСБ России в части защиты персональных данных.

Список литературы

1. Гончаров И.В., Гончаров Н.И., Кирсанов Ю.Г., Паринов П.А., Райков О.В. Порядок проведения анализа состояния информационной системы персональных данных различного применения. Вестник ВГУ, серия: системный анализ и информационные технологии, 2014, № 3.
2. Гончаров И.В., Гончаров Н.И., Кирсанов Ю.Г., Паринов П.А., Райков О.В. 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).
3. Методический документ «Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн», ФСТЭК России, 14 февраля 2008 г.
4. Методический документ Методика определения угроз безопасности информации в информационных системах (проект) 2015.
5. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите ПДн при их обработке в ИСПДн».

6. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
7. Приказ Минкомсвязи России от 05 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»
8. Методический документ «Меры защиты информации в государственных информационных системах», ФСТЭК России, 11 февраля 2014 г.
9. Методический документ «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн», ФСТЭК России, 14 февраля 2008 г.
10. Информационное сообщение о банке данных угроз безопасности информации ФСТЭК России от 6 марта 2015 г. № 240/22/879.
11. Информационное сообщение ФСБ России О нормативно-методических документах, действующих в области обеспечения безопасности персональных данных от 21.06.2016.

Reference

1. Goncharov I.V., Goncharov N.I., Kirsanov Y.G., Parinov P.A., Raykov O.V. The procedure for conducting the analysis of the personal data information system for various applications. Vestnik VSU Series: System Analysis and Information Technology, 2014, number 3.
2. Goncharov I.V., Goncharov N.I., Kirsanov Y.G., Parinov P.A., Raykov O.V. The procedure for conducting the analysis of the personal data information systems for various applications in the framework of the requirements for data protection. IT standard. 2015. T. 1. № 4-1 (5).
3. Methodological document "Methodology for determining the PD current security threats as they are processed in ISPDn" FSTEC Russia, February 14, 2008
4. Methodical document Method for determining information security threats in information systems (project) in 2015.
5. Russian Federation Government Resolution dated November 1, 2012 № 1119 "On approval of requirements for the protection of PD as they are processed in the PDIS."
6. Order FSTEC Russia on February 11, 2013 № 17 "On approval of the requirements of the protection of information, not the state secret contained in the state information systems."
7. Order of the Ministry of Communications of Russia on September 5, 2013 № 996 "On Approval of the requirements and methods of personal data depersonalization"
8. Methodological document "Measures of information protection in state information systems", FSTEC Russia, February 11, 2014
9. Methodological document "Basic model of PD threats to security at their processing within ISPDn" FSTEC Russia, February 14, 2008
10. Announcement of a databank of information security threats FSTEC Russia on March 6, 2015 № 240/22/879.
11. Information report of the FSB Russia about regulatory and procedural instruments in force in the field of security of personal data from 21.06.2016.