ПОРЯДОК ПРОВЕДЕНИЯ АНАЛИЗА СОСТОЯНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ РАЗЛИЧНОГО ПРИМЕНЕНИЯ В РАМКАХ ВЫПОЛНЕНИЯ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

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

[1]ЗАО «НПО «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 опыта и с учетом актуальных требований описан алгоритм проведения анализа состояния информационных систем персональных данных различного применения, выделены аспекты, важные для подготовки и создания таких систем и их систем защиты

Ключевые слова: персональные данные, информационная система персональных данных, модель угроз, модель нарушителя

PROCEDURE analysis of the state personal data information systems for various applications in the framework of the requirements for information protection

On the basis of experience and taking into account the relevant requirements of the algorithm to analyze the state of personal data information systems for various applications, highlighted aspects that are important for the preparation and establishment of such systems and their protection systems

Keywords: personal data, personal data information systems, threat model, the model of the offender

Оператор, организующий и (или) осуществляющий обработку персональных данных (ПДн), в соответствии с Федеральным законом РФ от 27 июля 2006 года №152-ФЗ «О персональных данных» [1], обязан обеспечить безопасность ПДн при их обработке (статья 6 часть 3), а также соблюдать требования к защите обрабатываемых ПДн (статья 19), к основным из которых относятся:

определение угроз безопасности ПДн в соответствии с установленным порядком [1];

применение необходимых организационных и технических мер по обеспечению безопасности ПДн [1];

применение средств защиты информации в рамках реализации мер по обеспечению безопасности ПДн [1];

проведение оценки эффективности принимаемых мер по обеспечению безопасности ПДн в соответствии с установленным порядком [1].

Для решения поставленных задач оператор обязан провести комплексный анализ состояния информационной системы персональных данных (ИСПДн). Порядок действий оператора, связанный с данным анализом, отражен в нормативных правовых актах и методических документах ФСБ и ФСТЭК России [3,4].

Весь алгоритм можно условно разделить на 6 этапов [1-17] (рис. 1).

После проведения анализа состояния ИСПДн на этапе завершения реализации мер по защите ПДн в ИСПДн формируется пакет документов, определяющий порядок построения и эксплуатации защищенной ИСПДн.

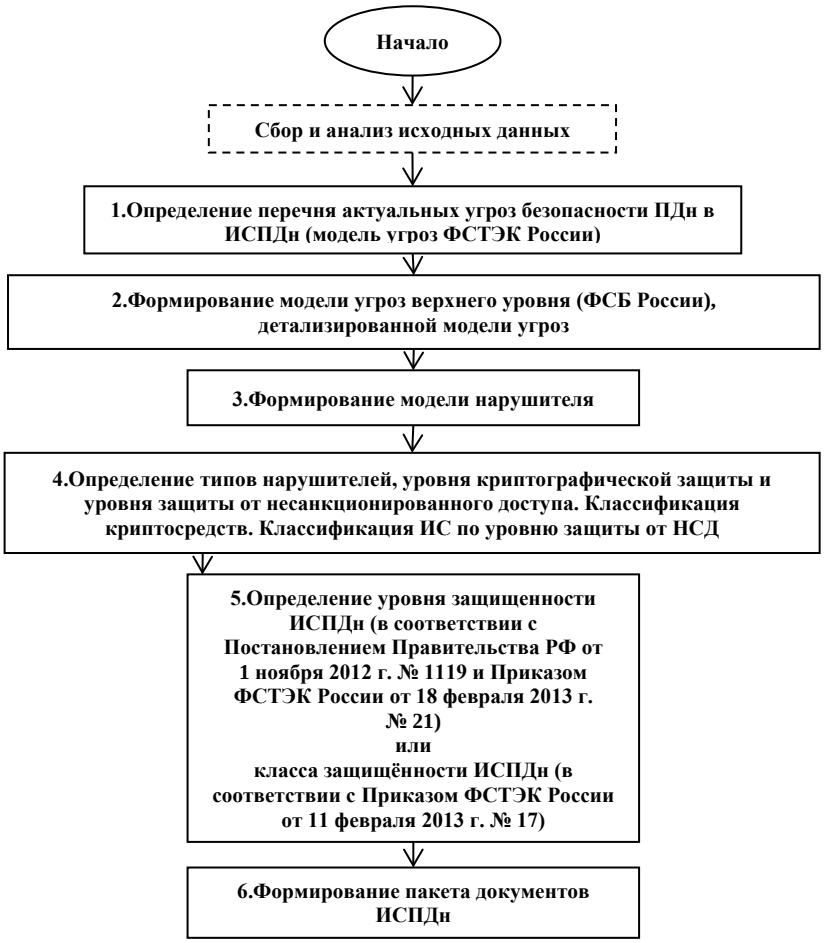

Рис.1 – Алгоритм проведения анализа состояния ИСПДн

Для всех операторов, являющихся государственным или муниципальным органом, в Постановлении Правительства РФ от 21 марта 2012 г. № 211 г. «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»[7] определен перечень требований, направленных на обеспечение безопасности ПДн, в том числе, разработка организационно-распорядительных документов, а также:

подтвержден порядок правил проведения работ, установлено действие законов, нормативно-методических документов;

установлено обязательное наличие должностной инструкции в составе общего перечня документов, что обуславливает введение должности.

В случае защиты информации, не составляющей государственную тайну, содержащейся в государственных информационных системах необходимо руководствоваться положениями приказа ФСТЭК России от 11 февраля 2013 г. № 17 [9].

Следует отметить, что организационно-распорядительные документы утверждаются актом руководителя оператора ПДн, являются внутренними, предшествующими обработке ПДн и содержат:

правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере ПДн, а также определяющие для каждой цели обработки ПДн содержание обрабатываемых ПДн, категории субъектов, ПДн которых обрабатываются, сроки их обработки или при наступлении иных законных оснований;

правила осуществление внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн;

правила работы с обезличенными данными;

перечень ИСПДн;

перечни ПДн, обрабатываемых в связи с реализацией трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций;

перечень должностей ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн;

перечень должностей, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн;

должностную инструкцию ответственного за организацию обработки ПДн в государственном или муниципальном органе;

обязательство лица, непосредственно осуществляющего обработку ПДн, в случае расторжения с ним контракта прекратить обработку ПДн, ставших известными ему в связи с исполнением должностных обязанностей;

согласие на обработку ПДн субъектов ПДн, а также разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн;

порядок доступа в помещения, в которых ведётся обработка ПДн.

Данные документы могут быть разработаны в дополнение и на основе предварительного анализа состояния ИСПДн, а так же по результатам классификации ИСПДн, разработки моделей угроз и нарушителя, определения уровня защищенности ИСПДн, формирования Политики безопасности ИСПДн и разрешительной системы доступа, которые в свою очередь содержат технологические характеристики и технологию функционирования ИСПДн и системы защиты ИСПДн.

Если организационно-распорядительные документы могут быть разработаны самим оператором ИСПДн, то для предварительного анализа состояния ИСПДн и сетевых характеристик, как правило, привлекают полномочных лицензиатов.

В целом анализ состояния ИСПДн может осуществляться на всех стадиях ее создания, в том числе и в ходе эксплуатации. В рамках проведения такого анализа, необходимо учитывать в надлежащем порядке требования и положения всех действующих нормативных документов, имеющих отношение к защите персональных данных [1-17].

Таким образом, практический опыт и актуальные требования действующих нормативных документов по безопасности ИСПДн позволили описать алгоритм проведения анализа состояния ИСПДн, выделить общие аспекты, позволяющие проводить подготовку и создание таких систем и их систем защиты, а также рекомендации для принятия решений по определению конкретных мер по защите 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. Федеральный Закон РФ от 27 июля 2006 г. №152-ФЗ «О персональных данных».
3. Методический документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 14 февраля 2008 г.
4. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных

данных с использованием средств автоматизации», утверждены ФСБ России от 21 февраля 2008 г.

5. Методический документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 14 февраля 2008 г.
6. Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 г. «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 органами».
7. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
8. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
9. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
10. Методический документ «Меры защиты информации в государственных информационных системах», ФСТЭК России, 11 февраля 2014 г.
11. Информационное сообщение по вопросам защиты информации и обеспечения безопасности персональных данных при их обработке в информационных системах в связи с изданием приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 июля 2013 г. № 240/22/2637.
12. Информационное сообщение о банке данных угроз безопасности информации ФСТЭК России от 6 марта 2015 г. № 240/22/879.
13. 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, 31 марта 2015 № 149/7/2/6-432.
14. Методический документ Методика определения угроз безопасности информации в информационных системах (проект) 2015.
15. 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».
16. Приказ ФСБ России от 10.07.2014 № 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».
17. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 31.12.2014) «Об информации, информационных технологиях и о защите информации».