# ПОРЯДОК ПРОВЕДЕНИЯ АНАЛИЗА СОСТОЯНИЯ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ И ОПРЕДЕЛЕНИЕ МЕР 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 практического опыта обоснован порядок общего системного подхода к соблюдению актуальных требований по защите информации, не составляющей государственную тайну в рамках анализа состояния государственных информационных системах, выделены аспекты, важные для подготовки и создания таких систем и их систем защиты, а также для принятия решений по определению конкретных мер по защите информации.**

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

# THE PROCEDURE OF CONDUCTING ANALYSIS OF THE GOVERNMENTAL INFORMATION SYSTEM AND DETERMINING THE MEASURES FOR PROTECTING INFORMATION

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

*[1]ZAO«NtC«Infobezopasnost», 394018, Russia, Voronezh, Kukolkina st., 9, of.. 402, e-mail: manager@infobez.org*
*[2]Federal service for technical and export control*

**On the basis of practical experience justified the order of a total system approach to compliance with relevant requirements for protection of information not constituting a secret of state in the framework of the analysis of condition state information systems, the aspects that are important for the preparation and development of such systems and their protection systems, but also for making decisions to identify specific measures to protect the information.**

Key words: personal data, informational system of personal data, governmental inforational system, threat model, violator model, information which is not presenting the government secret

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, так же принятия мер по защите ПДн.

Рассмотрим применение предложенного в [1] алгоритма для проведения анализа государственной информационной системе (ГИС).

Государственные информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов [16]. Требования к порядку создания развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации осуществляемых федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации определены в [12]. Согласно данному постановлению [12] основанием для создания ГИС является:

а) обязанность органа исполнительной власти по созданию системы, предусмотренная нормативными правовыми актами;

б) решение органа исполнительной власти о создании системы с целью обеспечения реализации возложенных на него полномочий.

Алгоритм можно условно разделить на следующие этапы:

1. Сбор и анализ исходных данных;

2. Определение перечня угроз безопасности в информационной системе (ИС) (в соответствии с [8, 9] и банком данных угроз безопасности информации (адрес: www.bdu.fstec.ru));

3. Формирование модели нарушителя (в соответствии с [8, 9]);

4. Определения актуальных угроз (в соответствии с [8, 9]);

5. Определение уровня защищенности ИС (в соответствии с [10]). Определение класса защищенности ИС (в соответствии с [14]);

6. Определение мер и средств по обеспечению безопасности ИС (в соответствии с [7, 10, 11, 12, 13, 14]);

7. Формирование пакета документов.

На первом этапе необходимо провести сбор и анализ исходных данных, которые используются для определения перечня актуальных угроз безопасности ИС.

В проекте Методического документа Методика определения угроз безопасности информации в информационных системах [9] устанавливается единый методический подход к определению угроз безопасности информации и разработке моделей угроз безопасности информации в государственных информационных системах, защита информации в которых обеспечивается в соответствии с [14]. Методика применяется совместно с банком данных угроз безопасности информации, сформированным ФСТЭК России (ubi.fstec.ru), а также базовыми и типовыми моделями угроз безопасности информации в информационных системах различных классов и типов, разрабатываемых ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085.

В данной методике предлагается следующий процесс определения угроз безопасности информации в информационной системе:

1. Идентификация источников угроз и угроз безопасности информации.

В качестве источников угроз безопасности информации могут выступать субъекты (физические лица, организации, государства) или явления (техногенные аварии, стихийные бедствия, иные природные явления).

Для идентификации угроз безопасности информации в информационной системе определяются:

- возможности (тип, вид, потенциал) нарушителей, необходимые им для реализации угроз безопасности информации;
- уязвимости, которые могут использоваться при реализации угроз безопасности информации (включая специально внедренные программные закладки);
- способы (методы) реализации угроз безопасности информации;
- объекты информационной системы, на которые направлена угроза безопасности информации (объекты воздействия);
- результат и последствия от реализации угроз безопасности информации.

Каждая угроза безопасности информации в информационной системе описывается (идентифицируется) следующим образом:

УБИj = [нарушитель (источник угрозы); уязвимости; способы реализации угрозы; объекты воздействия; последствия от реализации угрозы].

2. Оценка вероятности (возможности) реализации угроз безопасности информации и степени возможного ущерба

УБИj A = [вероятность (возможность) реализации угрозы (Pj); степень ущерба (Xj)].

Также по [9] разрабатывается модель нарушителя. Результаты оценки возможностей нарушителей включаются в модель нарушителя, которая является составной частью (разделом) модели угроз безопасности информации и содержит:

1. Типы, виды и потенциал нарушителей, которые могут обеспечить реализацию угроз безопасности информации. Типы нарушителей определяются по результатам анализа прав доступа субъектов к информации и (или) к компонентам информационной системы, а также анализа возможностей нарушителей по доступу к компонентам информационной системы исходя из структурно-функциональных характеристик и особенностей функционирования информационной системы.

В зависимости от потенциала, требуемого для реализации угроз безопасности информации, нарушители подразделяются на:

- нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз безопасности информации в информационной системе(внешние субъекты (физические лица), лица, обеспечивающие функционирование информационных систем или обслуживающих инфраструктуру оператора, пользователи информационной системы, бывшие работники, лица, привлекаемые для установки, наладки, монтажа, пуско-наладочных и иных работ);
- нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в информационной системе (террористические, экстремистские группировки, преступные группы (криминальные структуры), конкурирующие организации, разработчики, производители, поставщики программных, технических и программно-технических средств, администраторы информационной системы и администраторы безопасности;

- нарушителей, обладающих высоким потенциалом нападения при реализации угроз безопасности информации в информационной системе (специальные службы иностранных государств (блоков государств));

2. Цели, которые могут преследовать нарушители каждого вида при реализации угроз безопасности информации. Предположения о целях (мотивации) нарушителей делаются с учетом целей и задач информационной системы, вида обрабатываемой информации, а также с учетом результатов оценки степени возможных последствий (ущерба) от нарушения конфиденциальности, целостности или доступности информации;

3. Возможные способы реализации угроз безопасности информации. Возможные способы реализации угроз безопасности информации зависят от структурно-функциональных характеристик и особенностей функционирования информационной системы.

На основе определенных угроз безопасности информационной системе и модели нарушителя происходит определение актуальных угроз безопасности информации в информационной системе путем оценки:

- вероятности (возможности) реализации угрозы безопасности информации;
- степени возможного ущерба от реализации угрозы безопасности информации;

Решение об актуальности угрозы безопасности информации УБИj А для информационной системы с заданными структурно-функциональными характеристиками и условиями функционирования принимается в соответствии с таблицей 1.

Таблица 1 - Определение актуальности угрозы безопасности информации

| Вероятность (возможность) реализации угрозы (Yj) | Степень возможного ущерба (Xj) | | |
|---|---|---|---|
| | Низкая | Средняя | Высокая |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |

В случае решения оператора использовать средства криптографической защиты информации (СКЗИ) следует руководствоваться по разработке методическими рекомендациями 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 [5] при разработке частных моделей угроз. Использование СКЗИ для обеспечения безопасности персональных данных необходимо в следующих случаях [5]:

- если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации;
- если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ.

В случае, если угрозы, которые могут быть нейтрализованы только с помощью СКЗИ, актуальны или принято решение об использовании СКЗИ для обеспечения безопасности персональных данных вне зависимости от актуальности таких угроз, помимо исходных данных об информационных системах необходимо описать:

- объекты защиты (СКЗИ, среда функционирования СКЗИ, документы, носители с защищаемой информацией, каналы связи и т.д.) и актуальные характеристики безопасности объектов защиты угрозы;
- классификация и характеристики нарушителей, а также их возможностей по реализации атак;
- источники атак.

На основании исходных данных определяются обобщенные возможности источников атак. Актуальность использования возможностей источников атак определяет наличие соответствующих актуальных угроз.

В соответствии с частью 7 статьи 19 Закона [17] проекты нормативно правовых актов подлежат согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации. Согласно методическим рекомендациям [5] согласование с ФСБ России частных моделей угроз операторов, подготовленных в соответствии с настоящими методическими рекомендациями, не требуется.

В соответствии с Постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [10] необходимо определить уровни защищенности ПДн [1, 10]. На данном этапе необходимо определить категорию обрабатываемых ПДн (специальная категория ПДн,

биометрические ПДн, общедоступные ПДн, а также иные категории ПДн) и тип угроз, определение которого производится оператором с учетом совокупности условий и факторов, указанных в пункте 5, а также оценки вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 ФЗ «О персональных данных», и нормативных правовых актов, принятых во исполнение части 5 статьи 19 ФЗ «О персональных данных».

Определение уровня защищенности ПДн при их обработке в ИС проводится с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности ПДн [1].

В соответствии с приказом от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [14] определяется класс защищенности (КЗ) информационной системы. Оператору необходимо сначала определить уровень значимости (УЗ) информации и масштаб системы, и в результате сопоставления этих двух показателей определить класс (К) защищённости информационной системы. Средства обеспечения безопасности информации выбираются в соответствии с требованиями определенными в [14].

Для обеспечения безопасности информации при ее обработке в государственных информационных системах необходимо руководствоваться требованиями, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17, требованиями (в том числе в части определения уровня защищенности персональных данных), установленными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119. Согласно [3] в соответствии с пунктом 27 Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17, должно быть обеспечено соответствующее соотношение класса защищенности государственной информационной системы с уровнем защищенности персональных данных. В случае, если определенный в установленном порядке уровень защищенности персональных данных выше, чем установленный класс защищенности государственной информационной системы, то осуществляется повышение класса защищенности до значения, обеспечивающего выполнение пункта 27 Требований, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17.

СТР-К применяется в качестве методического документа при реализации мер по защите технических средств государственных информационных систем в целях нейтрализации угроз безопасности информации, связанных с защитой информации, представленной в виде информативных электрических сигналов и физических полей (защита от утечки по техническим каналам). Необходимость защиты ГИС от утечек по техническим каналам определяется наличием актуальной угрозы. Данный вид угроз связан с нарушителем с высоким потенциалом. Согласно проекту Методики [9] под нарушителем с высоким потенциалом понимаются специальные службы иностранных государств (блоков государств). Иные положения СТР-К могут применяться по решению обладателей информации, заказчиков и операторов государственных информационных систем в части, не противоречащей Требованиям, утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17 [3].

По результату анализа ИС должны быть сформированы следующие документы:

- акт определения требуемого уровня защищенности ИС;
- акт определения класса защищенности ИС;
- перечни обрабатываемых сведений в ИС;
- модель угроз безопасности информации в ИС;
- модель нарушителя безопасности информации в ИС;
- описание технологического процесса ИС;
- разрешительная система доступа ИС;
- технический паспорт ИС;
- комплект организационно распорядительной документации;
- перечень сотрудников, работающих в ИС.

Таким образом, в настоящей статье на основе практического опыта обоснован порядок общего системного подхода к соблюдению актуальных требования по защите информации, не составляющей государственную тайну в ГИС. Это позволяет обеспечить создание ГИС и ее системы защиты, а также обеспечить принятие решений по определению конкретных мер по защите информации.

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. «Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации», утверждены ФСБ России от 21 февраля 2008 г.

3. 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.
4. Информационное сообщение о банке данных угроз безопасности информации ФСТЭК России от 6 марта 2015 г. № 240/22/879.
5. 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.
6. Методический документ «Базовая модель угроз безопасности ПДн при их обработке в ИСПДн», ФСТЭК России, 14 февраля 2008 г.
7. Методический документ «Меры защиты информации в государственных информационных системах», ФСТЭК России, 11 февраля 2014 г.
8. Методический документ «Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн», ФСТЭК России, 14 февраля 2008 г.
9. Методический документ Методика определения угроз безопасности информации в информационных системах (проект) 2015.
10. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите ПДн при их обработке в ИСПДн».
11. Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 г. «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О ПДн» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
12. 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».
13. 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».
14. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о ЗИ, не составляющей ГТ, содержащейся в ГИС».
15. 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».
16. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 31.12.2014) «Об информации, информационных технологиях и о защите информации».
17. Федеральный Закон РФ от 27 июля 2006 г. №152-ФЗ «О персональных данных».