УДК 69

DOI 10.21661/r-530723

В.М. Бисюков

К ВОПРОСУ О МЕТОДИЧЕСКОМ ОБЕСПЕЧЕНИИ ПРОЦЕДУРЫ ВЫБОРА ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

***Аннотация**: актуальность темы обусловлена тем, что ст. 19 ФЗ №152 обязывает оператора персональных данных (ПДн) осуществлять защиту ПДн, обрабатываемых в информационных системах ПДн (ИСПДн) посредством построения системы защиты реализующей определённый набор организационных и технических мер защиты, а также оценки эффективности принимаемых мер. При выборе перечня организационных и технических мер защиты, а также методики оценки их эффективности, оператор ПДн сталкивается с проблемой учёта требований большого количества нормативно-методических документов, регламентирующих данный процесс. Целью исследования является разработка методического обеспечения процедуры выбора и оценки эффективности предложенных организационных и технических мер защиты ПДн в ИСПДн.*

***Ключевые слова**: информационная безопасность, риск информационной безопасности, персональные данные, оператор персональных данных, информационная система, технические меры защиты, организационные меры защиты, модель угроз информационной системы.*

V.M. Bisiukov

ON PROCEDURAL GUIDELINES ON THE PROCEDURE OF CHOOSING THE ORGANIZATIONAL AND TECHNICAL MEASURES FOR PERSONAL DATA PROTECTION IN THEIR PROCESSING IN PERSONAL DATA INFORMATION SYSTEMS

***Abstract**: the urgency of the issue treated in this paper is determined by the fact that the federal law requires personal data operators to guarantee the safety of*

processed personal data by developing security systems based on a number of organizational and technical security measures, as well as their evaluation. When choosing the organisational and technical security measures, the problem of having to consider a large number of normative and procedural documents which regulate this process arises. The aim of this study is to develop the procedural guidelines for choosing and assessing the effectiveness of suggested organizational and technical security measures for data protection in personal data information systems.

Keywords*: information security, information security risks, personal data, personal data operator, information system, technical security measures, organizational security measures, information system threats model.*

Технологию выбора организационных и технических мер по обеспечению безопасности персональных данных (ПДн), при их обработке в информационных системах ПДн (ИСПДн) можно представить в виде алгоритма [2, с. 9] (рис. 1).

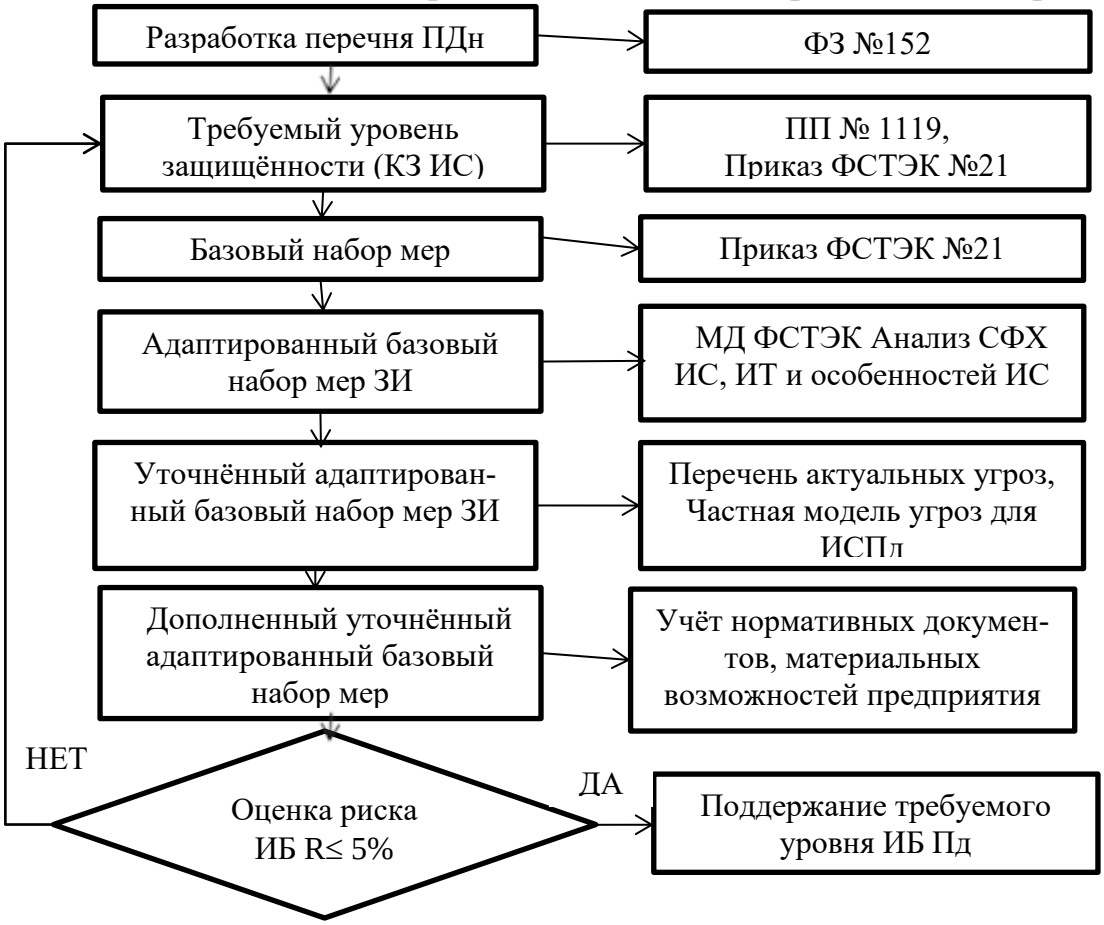

Рис. 1. Алгоритм выбора и оценки эффективности, организационных и технических мер по обеспечению безопасности ПДн, при их обработке в ИСПДн

Перечень ПДн является правовой основой построения системы защиты Пд в ИСПДн. Перечень ПДн оформляется отдельным разделом в перечне сведений, составляющих коммерческую тайну предприятия (таблица 1).

Таблица 1

Перечень сведений составляющих коммерческую тайну предприятия

№ п/п	Наименование сведений	Гриф конфиденциальности	Срок конфиденциальности	Перечень сотрудников допущенных к сведениям

Перечень подписывается всеми членами экспертной комиссии и утверждается первым руководителем предприятия.

Требуемый уровень защищённости ИСПДн определяется с учётом требований постановления правительства №1119 [3, с. 4–6]

Необходимость обеспечения того или иного уровня защищенности ПДн в ИСПДн устанавливается с учётом таблицы 2.

Таблица 2

Выбор уровня защищённости для ИСПДн

<table>
<tr><td rowspan="2">Категория ПДн</td><td colspan="5">Тип угроз</td></tr>
<tr><td>1</td><td colspan="2">2</td><td colspan="2">3</td></tr>
<tr><td>Специальные</td><td>УЗ-1</td><td>УЗ-1
При обработке ПДн >100 тыс. др. субъектов</td><td>УЗ-2
При обработке ПДн сотрудников оператора или < 100 тыс. др. субъектов</td><td>УЗ-2
При обработке ПДн>100 тыс. др. субъектов</td><td>УЗ-3
При обработке ПДн сотрудников оператора или < 100 тыс. др. субъектов</td></tr>
<tr><td>Биометрические</td><td>УЗ-1</td><td colspan="2">УЗ-2</td><td colspan="2">УЗ-3</td></tr>
<tr><td>Иные категории ПДн</td><td>УЗ-1</td><td>УЗ-2
При обработке ПДн>100 тыс. др. субъектов</td><td>УЗ-3
При обработке ПДн сотрудников оператора или < 100 тыс. др. субъектов</td><td>УЗ-3
При обработке ПДн>100 тыс. др. субъектов</td><td>УЗ-3
При обработке ПДн сотрудников оператора или < 100 тыс. др. субъектов</td></tr>
<tr><td>Общедоступные</td><td>УЗ-2</td><td>УЗ-2
При обработке ПДн>100 тыс. др. субъектов</td><td>УЗ-3
При обработке ПДн сотрудников оператора или < 100 тыс. др. субъектов</td><td colspan="2">УЗ-4</td></tr>
</table>

Базовый набор мер определяется на основе определённого уровня защищённости ИСПДн, с учётом требований приказа ФСТЭК №21 [2, с. 3].

Адаптация базового набора мер предполагает исключение мер, непосредственно связанных с информационными технологиями, не применяемыми в исследуемой ИСПДн, или структурно-функциональными характеристиками (СФХ) не свойственными данной ИСПДн.

Анализ применяемых технологий, программного обеспечения и СФХ ИСПДн предлагается проводить по следующим характеристикам (таблица 3).

Таблица 3

Анализируемые СФХ ИСПДн

Анализируемые СФК ИСПДн	Возможные варианты анализируемых характеристик
По структуре ИС	автономное автоматизированное рабочее место
	локальная ИС
	распределенная ИС
По используемым информационным технологиям	системы на основе виртуализации
	системы, реализующие «облачные вычисления»
	системы с мобильными устройствами
	системы с технологиями беспроводного доступа
	грид-системы
	суперкомпьютерные системы
По свойствам архитектуры	системы на основе «тонкого клиента»,
	системы на основе одно ранговой сети,
	файл-серверные системы
	центры обработки данных
	системы с удаленным доступом пользователей,
	использование разных типов операционных систем (гетерогенность среды)
	использование прикладных программ, независимых от операционных систем
	использование выделенных каналов связи
По наличию взаимосвязей с иными ИС	взаимодействующая с системами
	невзаимодействующая с системами

По наличию подключений к сетям связи общего пользования	подключенная
	подключенная через выделенную инфраструктуру (gov.ru или иную)
	неподключенная
По размещению технических средств	расположенные в пределах одной контролируемой зоны
	расположенные в пределах нескольких контролируемых зон
	расположенные вне КЗ
По режимам обработки информации в ИС	многопользовательский
	однопользовательский
По режимам разграничения прав доступа	без разграничения
	с разграничением
По режимам разделения функций по управлению ИС	без разделения
	выделение рабочих мест для администрирования в отдельный домен
	использование различных сетевых адресов,
	использование выделенных каналов для администрирования
По подходам к сегментированию ИС	без сегментирования,
	с сегментированием

Уточнение базового адаптированного набора мер производится в следующей последовательности:

1) построение базовой модели угроз для ИСПДн и определение на её основе потенциальных угроз безопасности ИСПДн [4, с. 63];

2) выявление актуальных угроз для ИСПДн [5, с. 7];

3) уточнение адаптированного базового набора мер.

На основании уточнённого адаптированного базового набора мер из перечня выбранных организационных и технических мер исключаются меры, не соответствующие актуальным угрозам и возможностям актуального нарушителя.

Дополнение уточнённого адаптированного базового набора мер производится с учётом ценности сведений и материальных возможностей предприятия.

Проведение оценки эффективности СЗПДн в ИСПДн предлагается проводить по критерию количественной оценке риска информационной безопасности

(ИБ) для ИСПДн [6, с. 2]. Этапы оценки эффективности СЗПДн для ИСПДн представлены в таблице 4.

Таблица 4

Этапы работы по оценке эффективности СЗПДн в ИСПДн

Этапы	Название этапов
Этап 1	Оценка степени учёта требований нормативно-методических документов при построении СЗПДн
Этап 2	Определение вероятностей реализации хотя бы одной из актуальных угроз
Этап 3	Определение степени использования организационных и технических мер защиты в СЗПДн
Этап 4	Определение количественного значения риска информационной безопасности

Числовое значение величины риска ИБ определяется по формуле [6, с. 4].

$$R = \text{Ругр} \cdot Rn \cdot C \frac{\text{Ко} + \text{К}t}{2} \cdot 100\%,$$

где R – величина риска реализации угроз ИБ для ИСПДн;

Р угр – вероятность реализации хотя бы одной угрозы из всего перечня актуальных угроз;

Rn – риск несоответствия требованиям законодательства;

С – ценность актива (0…1);

Ко – степень использования организационных мер;

Kt – степень использования технических мер.

Ели значение риска ИБ ≤ 5% то уровень защиты ПД и ИСПДн признаётся достаточным.

Список литературы

1. Закон РФ «О персональных данных» от 27.07.2006 №152 – ФЗ // Бюллетень нормативных актов министерств и ведомств. – №7. – 2006. – С. 15–32.

2. Приказ ФСТЭК №21 от 18.02.2013 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах ПДн».

3. Постановление правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении требований к защите ПДн при их обработке в информационных системах ПДн».

4. Базовая модель угроз безопасности ПДн при их обработке в информационных системах ПДн, утвержденная приказом ФСТЭК РФ 15.02.2008.

5. Методика определения актуальных угроз безопасности ПДн при их обработке в информационных системах ПДн, утверждена приказом ФСТЭК РФ 14.02.2008.

6. Белов В.М. Методика оценки рисков информационной безопасности / В.М. Белов, А.В. Плетнёв. – М.: Бизнес-школа «Интел-Синтез, 2016. – 126 с.

References

1. (2006). Zakon RF "O personal'nykh dannykh" ot 27.07.2006 152. Biulleten' normativnykh aktov ministerstv i vedomstv, 7, 15-32.

2. Prikaz FSTEK 21 ot 18.02.2013 "Ob utverzhdenii sostava i soderzhaniia organizatsionnykh i tekhnicheskikh mer po obespecheniiu bezopasnosti PDn pri ikh obrabotke v informatsionnykh sistemakh PDn".

3. Postanovlenie pravitel'stva RF ot 1 noiabria 2012 g. 1119 "Ob utverzhdenii trebovanii k zashchite PDn pri ikh obrabotke v informatsionnykh sistemakh PDn".

4. Bazovaia model' ugroz bezopasnosti PDn pri ikh obrabotke v informatsionnykh sistemakh PDn, utverzhdennaia prikazom FSTEK RF 15.02.2008.

5. Metodika opredeleniia aktual'nykh ugroz bezopasnosti PDn pri ikh obrabotke v informatsionnykh sistemakh PDn, utverzhdena prikazom FSTEK RF 14.02.2008.

6. Belov, V. M., & Pletniov, A. V. (2016). Metodika otsenki riskov informatsionnoi bezopasnosti., 126. M.: Biznes-shkola "Intel-Sintez.

Бисюков Виктор Михайлович – магистр техн. наук, доцент Института информационных технологий и телекоммуникаций ФГАОУ ВО «Северо-Кавказский федеральный университет», Ставрополь, Россия.

Bisiukov Viktor Mikhailovich – master of technical sciences, associate professor, Institute of IT and Telecommunications, FSBEI of HE “North-Caucasus Federal University”, Stavropol, Russia.
