



Код безопасности

Алгоритм действий оператора ПДн по созданию системы защиты ИСПДн



В данной статье рассматривается алгоритм действий оператора персональных данных по созданию системы защиты информационной системы персональных данных (ИСПДн). Данный алгоритм является авторским видением и пониманием действующих нормативных документов и может при-

меняться как при создании, так и при модернизации системы защиты ИСПДн. В статье не рассматривается процесс создания самой ИСПДн и такие базовые организационные меры, как заполнение и отправка уведомления об обработке ПДн, разработка и принятие организационных документов, указанных в требованиях к защите ПДн, принятых постановлением Правительства РФ от 1 ноября 2012 г. № 1119 (далее по тексту – ПП-1119), и другие, выполнение которых также необходимо при обработке персональных данных (ПДн).

Шаг 1. Разработка частной модели угроз

Защита ИСПДн начинается с составления **частной модели угроз** – формализованного перечня возможных угроз ПДн и оценки их актуальности, с учетом исходного состояния защищенности. Основанием для составления частной модели угроз могут являться следующие документы: «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)», утвержденная ФСТЭК России 15 февраля 2008 г., и «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная ФСТЭК России 14 февраля 2008 г.

Актуальность угроз определяется субъективно, но должна учитывать опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

В частной модели угроз обязательно должны быть отражены угрозы, связанные с наличием недокументированных (недекларированных) возможностей (НДВ) в системном и прикладном программном обеспечении, от выбора актуальности данных угроз зависит дальнейшая работа по защите ИСПДн.

Шаг 2. Оценка вреда и определение типа угроз

В соответствии с ПП-1119 устанавливается четыре уровня защищенности (УЗ) ПДн, оператор определяет УЗ обрабатываемых ПДн на основании типа актуальных угроз, категории, объема и типа обрабатываемых ПДн. Для начала необходимо определить тип актуальных угроз.

В ПП-1119 устанавливаются три типа актуальных угроз:

- 1-й – в случае актуальности угроз, связанных с наличием НДВ в системном программном обеспечении;
- 2-й – в случае актуальности угроз, связанных с наличием НДВ в прикладном программном обеспечении;
- 3-й – в случае, если угрозы, связанные с наличием НДВ, не актуальны.

Тип актуальных угроз определяется в соответствии с составленной частной моделью угроз. Дополнительно ПП-1119 предписывает определить тип угроз безопасности персональных данных с учетом оценки возможного вреда, ссылаясь на пункт 5 части 1 статьи 18.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» (далее по тексту – ФЗ-152), однако готовой методики по оценке данного параметра не существует.

Я предлагаю использовать субъективную оценку: оператор самостоятельно оценивает возможный вред субъектам ПДн в случае выбора конкретного типа угроз (на основании частной модели угроз). При этом определяется тип вреда и его размер. В соответствии с частью 1 статьи 1064 главы 59 Гражданского кодекса РФ, вред может быть материальным и личностным (т.е. моральным). Оценка материального вреда делается с помощью примерного расчета возможных материальных потерь субъекта в случае нарушения конфиденциальности его ПДн. Моральный вред в соответствии со статьей 1101 главы 59 Гражданского кодекса РФ компенсируется также в денежной форме. Для определения возможного ущерба можно провести анализ судебной практики по гражданским искам о присуждении выплат за нарушение порядка обработки ПДн, вследствие которых произошло нарушение конфиденциальности ПДн. По моим данным, средний размер моральной компенсации за нарушение конфиденциальности ПДн составляет порядка 3000 рублей, судебные решения по подтверждению материального вреда мне не известны.

Результаты оформляются в виде **акта оценки вреда, который может быть причинен субъектам ПДн**.

Шаг 3. Определение уровня защищенности ПДн

На втором шаге был установлен тип актуальных угроз, теперь необходимо на основании этой информации определить уровень защищенности. В пунктах 9–12

требований к защите ПДн, утвержденных ПП-1119, приводятся условия выбора УЗ.

Тип ИСПДн	Категория субъектов	Количество субъектов	Тип актуальных угроз				
			1	2	3		
ИСПДн-С	Не сотрудники	> 100 000	УЗ-1	УЗ-1	УЗ-2		
		< 100 000		УЗ-2	УЗ-3		
	Сотрудники	Любое					
ИСПДн-Б	Любая	Любое					
ИСПДн-И	Не сотрудники	> 100 000					
		< 100 000		УЗ-3	УЗ-4		
	Сотрудники	Любое					
ИСПДн-О	Не сотрудники	> 100 000		УЗ-2		УЗ-2	
		< 100 000				УЗ-3	
	Сотрудники	Любое					

Под типом ИСПДн подразумевается тип обрабатываемых в ИСПДн персональных данных в соответствии с пунктом 5 требований к защите ПДн, утвержденных ПП-1119:

ИСПДн-С – специальные категории ПДн – данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн;

- ИСПДн-Б – биометрические ПДн, без данных, относящихся к ИСПДн-С, – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных;
- ИСПДн-О – общедоступные ПДн в соответствии со статьей 8 ФЗ-152;
- ИСПДн-И – все остальные ИСПДн.

Отдельным столбцом в таблице указана категория субъектов: если в ИСПДн обрабатываются ПДн только сотрудников оператора, следует смотреть на строку «Сотрудники», если в ИСПДн есть ПДн других субъектов – «Не сотрудники».

Результат выбора уровня защищенности с указанием типа ИСПДн, категории и количества субъектов ПДн должен быть оформлен в виде **акта определения уровня защищенности ПДн при их обработке в ИСПДн**.

Шаг 4. Выбираем меры по защите

После определения уровня защищенности ПДн переходим к составлению модели защиты – выбора мер, закрывающих актуальные угрозы безопасности. В качестве основы для выбора мер необходимо использовать приложение к составу и содержанию организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, утвержденное приказом ФСТЭК России от 18 февраля 2013 г. № 21 (далее по тексту – П-21). Модель защиты, в соответствии с пунктом 9 П-21, составляется по следующему алгоритму:

- 1) определяется базовый набор мер, а именно составляется перечень тех мер, которые отмечены плюсами для соответствующего УЗ в приложении к П-21;
- 2) адаптация базового набора мер. На этом этапе из базового набора мер исключаются те, которые не актуальны из-за особенностей конкретной ИСПДн (например, исключаются меры по защите виртуализации, если виртуализация не используется);
- 3) уточнение адаптированного базового набора мер. На этом этапе добавляются ранее не выбранные меры, если в соответствии с частной моделью угроз какие-либо из актуальных угроз остались незакрытыми;
- 4) добавление уточненного адаптированного базового набора мер в соответствии с иными нормативными документами. На данный момент этот этап не актуален, скорее всего, он станет актуальным после выхода нормативных документов ФСБ.

Стоит отметить, что исключить какие-либо базовые меры по причине неактуальности угрозы, на закрытие которой направлена эта мера, нельзя. Поэтому на данном этапе рекомендуется еще раз пересмотреть актуальность угроз, сформулированную в частной модели угроз, в противном случае, у регуляторов могут возникнуть сомнения в правильности их выбора.

В случае затруднений в технической реализации какой-либо из мер или с учетом экономической целесообразности выполнения данных мер в полном объеме, можно воспользоваться пунктом 10 П-21 и внести соответствующие корректировки:

«При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных».

Итоговый документ с перечнем мер оформляется в виде модели защиты или иного документа с составом и содержанием мер по обеспечению безопасности ПДн.

Шаг 5. Реализация выбранных мер: выбираем и внедряем средства защиты

Последним шагом по созданию системы защиты ИСПДн является реализация выбранных на предыдущем этапе мер по защите. Меры по защите могут быть реализованы с помощью организационных мероприятий и, в соответствии с пунктом 4 П-21, посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия (например, сертифицированные во ФСТЭК России). Непосред-

ственный выбор средств защиты для закрытия тех или иных мер – достаточно большая тема, которую не раскроешь в рамках одной статьи.

Регуляторы прямо не обязывают оператора ПДн оформлять методы реализации мер по защите документально, но я рекомендую составить описание всех применяемых средств защиты и организационных мер с сопоставлением их модели защиты.

Заключение

Создание системы защиты ИСПДн начинается после подготовки следующих документов:

- 1) частная модель угроз;
- 2) акт оценки вреда, который может быть причинен субъектам ПДн;
- 3) акт определения уровня защищенности ПДн при их обработке в ИСПДн;
- 4) модель защиты или иной документ с составом и содержанием мер по обеспечению безопасности ПДн;
- 5) документ, содержащий в себе описание всех применяемых средств защиты и организационных мер (необязательно).



Код безопасности

Почтовый адрес: 127018, Россия, Москва, а/я 55.

Адрес офиса в Москве: ул. Большая Семеновская, д. 32, стр. 1.

Адрес офиса в Санкт-Петербурге: Свердловская наб., д. 44.

Тел.: +7 (495) 980-2345 (многоканальный).

Факс: +7 (495) 980-2345.

E-mail: info@securitycode.ru

Запрос дополнительной информации о продуктах: info@securitycode.ru

По вопросам стоимости и покупки продуктов buy@securitycode.ru

По вопросам партнерства и сотрудничества info@securitycode.ru

Вы можете узнать подробную информацию о продуктах на сайте
www.securitycode.ru

О компании «Код Безопасности»

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Кода Безопасности» применяются для защиты конфиденциальной информации, персональных данных, коммерческой и государственной тайны. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.