Русская Академия Ремёсел

Некоммерческое образовательное частное учреждение дополнительного профессионального образования

Свидетельство Министерства юстиции РФ 7714041778 от 13.11.2013 г. лицензия Департамента образования города Москвы № 037362 от 11.04.2016 г.

Исх.№ _____ от _____201___г.

«УТВЕРЖДАЮ»
Ректор

НОЧУ ДПО «РАР»
Просвирина Е.А.

«30» октября 2018 г.

МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Москва, 2017

Содержание

1. Общие положения

- Настоящий документ содержит методику моделирования угроз безопасности персональных данных при их обработке в информационных системах персональных данных в образовательных организациях, подведомственных Департаменту образования города Москвы.
- Разработка базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных и методики ее использования при определении актуальных угроз предусмотрена вторым этапом контракта от 25.07.2016 № 0У3/04-01-31/16 с НОЧУ ДПО "РАР" на оказание услуг по разработке системы документального обеспечения процессов внедрения и эксплуатации информационных систем персональных данных в образовательных организациях, подведомственных Департаменту образования города Москвы, с учетом выполнения требований нормативных правовых актов Российской Федерации в области обработки персональных данных.
- Настоящая Методика учитывает требования к организации порядка обработки персональных данных в соответствии с действующим законодательством Российской Федерации о персональных данных.

• Методические рекомендации

• Общие сведения о моделировании угроз

• *Введение*

В соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» каждый оператор обязан проводить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения требований закона, и определять угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.

К моделированию угроз целесообразно привлекать ответственных за обработку и защиту персональных данных, персонал, осуществляющий работу по администрированию и техническому сопровождению информационно технологической инфраструктуры организации, а также сторонние организации, имеющие лицензии на осуществление деятельности по технической защите конфиденциальной информации.

• *Методические документы*

Методическую базу для моделирования угроз безопасности персональных данных при их обработке в информационных системах персональных данных составляют следующие документы:

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная заместителем директора ФСТЭК России 15.02.2008;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная заместителем директора ФСТЭК России 14.02.2008.

• *Основные понятия, используемые в документе*

Угроза безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных;

Доступ к информации, в том числе к персональным данным - возможность получения информации и ее использования.

Доступ в информационную систему персональных данных - возможность запуска на выполнение штатных команд, функций, процедур системного и прикладного программного обеспечения.

Причиной возникновения угрозы безопасности информации могут являться человек, материальный или логический объект доступа, физическое явление, называемые источниками угрозы. Каждая угроза имеет вероятность реализации, зависящей от возможностей источников угроз, окружающих обстоятельств и обстановки.

- **Порядок определения границ информационных систем персональных данных**
  - ***Критерии определения границ***

Определение границ информационных систем персональных данных является основополагающим этапом при формальном описании информационнотехнологической инфраструктуры, поскольку от корректности определения границ зависят уровни защищенности компонентов инфраструктуры, сложность проектируемой системы защиты данных, целесообразность реализации различных мер.

В состав информационных систем персональных данных образовательной организации могут входить только те компоненты, которые расположены на территории организации, то есть серверы локальных информационных систем

и автоматизированные рабочие места, использующиеся в том числе для доступа к централизованным информационным системам Департамента образования города Москвы и Департамента информационных технологий города Москвы.

Для оценки необходимости разделения инфраструктуры на различные информационные системы персональных данных следует учитывать следующие критерии:

- назначение и функционал компонента;
- состав обрабатываемых данных;
- категории типов субъектов персональных данных, чьи данные обрабатываются в компоненте (работники или любые другие лица);
- количество субъектов персональных данных, чьи данных обрабатываются;
- типы субъектов доступа;
- территориальное расположение компонентов;
- логическое расположение компонентов;
- единство структуры компонентов;
- наличие подключения к сетям общего доступа.

- ***Порядок действий***

- 2.2.2.1. Из перечисленных в пункте 2.2.1 критериев три являются критичными для установления уровня защищенности, от которого зависит сложность системы защиты персональных данных: состав обрабатываемых данных, типы субъектов персональных данных и количество субъектов персональных данных. По этой причине целесообразно первоначально оценить общий объем обрабатываемых данных, и, если он не превышает 100 000 субъектов персональных данных, наличие в обрабатываемых персональных данных специальных категорий (о здоровье, интимной жизни, убеждениях и

др.), биометрических данных (физиологических данных, в том числе фотографий, используемых для идентификации субъекта), общедоступных данных.

Компоненты информационных систем, на которых ведется обработка специальных категорий и (или) биометрических персональных данных, должны быть выделены из общей инфраструктуры в одну или несколько отдельных информационных систем персональных данных, чтобы более высокие требования, предъявляемые к защите таких данных, не распространялись на остальные компоненты инфраструктуры и не усложняли (удорожали) общую систему защиты персональных данных.

Компоненты информационных систем, на которых ведется обработка только общедоступных данных и не ведется обработка иных данных, также могут быть выделены в отдельную информационную систему персональных данных.

Подробнее о влиянии критериев на определение уровня защищенности рассказывается в Методике определения уровня защищенности персональных данных в информационных системах персональных данных.

- 2.2.2.2. Следующий шаг – разделить компоненты по функционалу. Самый простой подход: разделить на автоматизированные рабочие места и серверы, поскольку рабочие места и серверы наиболее из всех компонентов различаются между собой по функциям, обрабатываемому одновременно объему данных, субъектам, имеющим к ним доступ, критичности выхода из строя.

В некоторых случаях, когда к серверу информационной системы относится несколько рабочих мест, с которых нет доступа к другим системам, целесообразно сервер вместе с относящимися к нему рабочими местами объединять в одну информационную систему персональных данных.

Если с автоматизированных рабочих мест есть доступ к многим информационным системам, обрабатывающим персональные данные одинаковой категории (или специальные, или биометрические, или общедоступные, или иные), целесообразно объединить все рабочие места в единую информационную систему персональных данных.

- Дальнейшее разделение инфраструктуры на отдельные информационные системы персональных данных с использованием критериев территориального и логического размещения, наличий подключений к сетям и других целесообразно только при высокодетализированном моделировании угроз и риск-ориентированном походе к управлению информационной безопасностью.

Для большинства образовательных организаций подход к разделению инфраструктуры на информационные системы персональных данных, приведенный в Базовой модели угроз безопасности персональных данных в информационных системах персональных данных государственных образовательных учреждений, подведомственных Департаменту образования города Москвы, является оптимальным.

- **Порядок адаптации базовой модели угроз**
- ***Порядок действий***

Базовые модели угроз для автоматизированных рабочих мест и серверов, расположенных в образовательных организациях, приведенные в документе «Базовая модель угроз безопасности персональных данных в информационных системах персональных данных государственных образовательных учреждений, подведомственных Департаменту образования города Москвы», учитывают наиболее распространенные варианты реализации информационно-технологической инфраструктуры в образовательных организациях, принятые меры защиты и имеющиеся предпосылки реализации угроз.

Структура частной модели угроз должна совпадать со структурой базовой модели и состоять из следующих разделов:

- общие положения;
- описание информационно-технологической структуры;
- основные виды угроз безопасности персональных данных в информационной системе персональных данных;
- источники угроз безопасности персональных данных в информационной системе персональных данных;
- описание методики определения угроз;
- модель угроз информационной системы;
- заключение (4-й подраздел базовой модели угроз следует выделить в отдельный раздел).

Разработка частной модели угроз состоит из следующих шагов:

- выбор типа информационной системы: автоматизированное рабочее место или сервер;
- корректировка базового описания информационно-технологической структуры с учетом специфики образовательной организации, в которой проводится разработка модели угроз (разделы «Общие сведения об информационнотехнологической инфраструктуре», «Меры физической защиты», «Технические средства и методы защиты информации») в соответствии с рекомендациями пункта 2.3.2;
- корректировка базового описания информационной системы, относящейся к выбранному типу (раздел «Группа информационных систем «Автоматизированные рабочие места» или «Группа информационных систем «Серверы образовательной организации») в соответствии с рекомендациями пункта 2.3.3;

- внесение в текст частной модели угроз разделов «Основные виды угроз безопасности персональных данных в информационной системе персональных данных», «Источники угроз безопасности персональных данных в информационной системе персональных данных», «Описание методики определения угроз» без изменений;
- внесение в текст частной модели угроз раздела с собственно моделью угроз выбранного типа («Базовая модель угроз информационных систем персональных данных группы «Автоматизированные рабочие места пользователей» или «Базовая модель угроз информационных систем персональных данных группы «Серверы образовательных систем») с используемым в образовательной организации названием информационной системы;
- корректировка разделов «Показатели исходной защищенности», «Вероятность реализации угроз», «Определение актуальности угроз» с учетом рекомендаций пунктов 2.3.5, 2.3.6, 2.3.7;
- составление заключения на основе заключения из базовой модели и рекомендаций пункта 2.3.8.
- ***Общее описание информационно-технологической структуры***

Раздел «Описание информационно-технологической структуры» подлежит адаптации и корректировке следующих положений, включая, но не ограничиваясь:

- распределенность инфраструктуры – одна или несколько площадок, имеющих свои локальные вычислительные сети;
- назначение используемых в организации серверов;
- логическое и (или) физическое разделение сегментов сети (в частности, преподавательской и ученической);
- наличие подключений к сетям общего доступа.

- Из предложенных вариантов схем информационно-технологической структуры образовательных организаций следует выбрать ту, которая наиболее полно отражает текущую ситуацию (наличие одного или нескольких отделений (корпусов), наличие серверов в одном или нескольких отделениях (корпусах).
- Раздел «Меры физической защиты» должен отражать существующую ситуацию в образовательной организации: количество площадок, точки контроля доступа (периметр территории, входы в здания), наличие камер видеонаблюдения.
- В разделе «Технические средства и методы защиты информации» следует указать:
- используемые типы средств защиты, их наименования, модели и версии;
- компоненты, на которых установлены средства защиты;
- сведения о парольной политике;
- сведения об осведомленности пользователей по вопросам информационной безопасности;
- иные применяемые методы защиты (журналирование событий, периодический анализ защищенности и другие).
- ***Описание информационных систем***

В соответствии с определенными границами информационных систем для каждой системы составляется описание информационной системы персональных данных.

В описание системы входят:

- назначение и функционал системы;
- состав обрабатываемых персональных данных;
- состав компонентов системы;

- наличие подключений к сетям общего доступа (сети Интернет, ведомственным сетям, Системе межведомственного электронного взаимодействия и др.);
- системы, с которыми осуществляется взаимодействие (к которым есть доступ из описываемой системы);
- территориальное расположение системы;
- сведения о включении в доменную структуру;
- способы получения доступа к системе, методы идентификации и аутентификации;
- используемые средства и методы защиты.
- ***Нарушитель безопасности персональных данных***

В базовой модели угроз приведена модель наиболее вероятного нарушителя безопасности персональных данных, действительная для всех информационных систем персональных данных в образовательной организации. Адаптация не требуется.

- ***Показатель исходной защищенности***

Рассчитанные в базовой модели угроз показатели исходной защищенности для автоматизированных рабочих мест и серверов образовательной организации подлежат актуализации в двух случаях:

- у образовательной организации только одна площадка, где расположены автоматизированные места, то есть системы, включающие автоматизированные рабочие места, будут локальными информационными системами, а не системами кампусного типа;
- серверы информационных систем расположены на нескольких площадках (например, сервер службы каталогов есть в каждом здании организации), то есть информационные системы будут кампусного типа, а не локальные.

В обоих случаях корректировке подлежит первый раздел («по территориальному размещению») таблицы характеристик уровня исходной защищенности информационной системы и соответственный пересчет общего количества решений уровня «высокий» и «средний». На вывод об общем среднем уровне защищенности информационной системы такие изменения не влияют, дальнейшие расчеты не затрагивают.

- ***Вероятность возникновения угроз***

Вероятности реализации угроз, оцененные в базовой модели, справедливы для усредненного варианта реализации информационно-технологической инфраструктуры в образовательной организации. При адаптации базовой модели угроз следует исключить из текста слово «базовый» в отношении модели угроз и изменить типовые названия информационных систем персональных данных на принятые в организации.

Дополнительные принятые меры обеспечения безопасности персональных данных (не учтенные в базовой модели) могут снизить вероятность реализации по ряду угроз. Поскольку оценка вероятности реализации осуществляется экспертным путем на основании анализа возможностей нарушителя, критичности существующих уязвимостей системы и достаточности принятых мер защиты, методика расчета вероятности слабо поддается формализации. Однако если выявлена необходимость учета дополнительных мер, следует воспользоваться упрощенной схемой учета влияния принятых мер на вероятность реализации угроз, приведенной в приложении (Приложение А).

В схеме учета символ «−» означает, что принятая мера никак не влияет на вероятность реализации угрозы, а символ «+» − влияет положительно. Если для нейтрализации угрозы используется не менее двух положительно влияющих мер дополнительно к указанным в базовой модели угроз (за исключением угрозы № 5, имеющей только одну эффективную меру противодействия), то

вероятность реализации угрозы может быть снижена со «средней» на «низкую».

- ***Определение актуальности угроз***

Не рекомендуется изменять определенные экспертным путем значения опасности угроз.

Для определения актуальности угроз, оценка вероятности которых изменена относительно базовой модели угроз, следует воспользоваться формулами из раздела «Описание методики определения угроз» базовой модели или следующей таблицей:

Вероятность и возможность реализации угрозы	**Показатель опасности угрозы**		
	низкая	**средняя**	**высокая**
• Маловероятная угроза – низкая возможность	• неактуальная	• неактуальная	• актуальная
• Низкая вероятность – средняя возможность	• неактуальная	• актуальная	• актуальная
• Средняя вероятность – средняя возможность	• актуальная	• актуальная	• актуальная
• Высокая вероятность – высокая возможность	• актуальная	• актуальная	• актуальная

- ***Заключение***

Перечень актуальных угроз в разделе «Заключение» должен соответствовать выявленному в результате определения актуальных угроз.

В заключении следует упомянуть, что модель угроз подлежит пересмотру и актуализации в случае изменения состава программных или технических средств, входящих в состав информационной системы персональных данных, функционального назначения информационной системы персональных данных, осуществления мероприятий по защите персональных данных, изменения законодательства Российской Федерации в области защиты персональных данных.

Упрощенная схема учета влияния реализованных мер по защите персональных данных на вероятность реализации угроз

• Мера	• Угроза (номер из базовой модели угроз)																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Проводится регулярное обновление системного и прикладного программного обеспечения	–	–	–	–	–	+	+	–	–	+	–	–	–	–	+	+	+	+	+	–	–
Установлены пароли на внесение изменений в базовую систему вводавывода	–	–	–	–	+	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Парольная политика предписывает длину паролей не менее 6 буквенно-числовых символов разного регистра, смена пароля не реже 1 раза в 3 месяца	–	–	–	–	–	+	+	+	+	–	–	+	–	–	–	–	–	–	+	–	–

Настроена регистрация событий безопасности и проводится периодический анализ журналов	–	–	–	–	–	+	–	+	–	–	–	–	–	–	–	–	–	–	–	–	–
Заблокированы порты подключения съемных устройств	–	–	–	–	–	–	–	+	+	–	–	–	–	–	–	–	–	–	+	–	–	–
Осуществляется контроль печати документов	–	–	–	–	–	–	–	+	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Проводится периодический инструментальный анализ защищенности	–	–	–	–	–	+	–	–	–	–	–	–	+	–	+	+	+	+	+	–	–
Преподавательская сеть физически или логически отделена от сети, куда имеют доступ обучающиеся	–	–	–	–	–	–	–	–	–	+	+	+	+	+	+	+	–	+	–	–	–