**Государственное образовательное учреждение
дополнительного профессионального образования
центр повышения квалификации специалистов Санкт-Петербурга
«Региональный центр оценки качества образования
и информационных технологий»**

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

**Санкт-Петербург
2010**

УДК 004.9
З 40

Защита персональных данных в информационных системах образовательного учреждения / Сост. М.Е. Крюкова. – СПб: ГОУ ДПО ЦПКС СПб «Региональный центр оценки качества образования и информационных технологий», 2010. – 68 с.

В сборнике представлены методические и справочные материалы по вопросу защиты персональных данных в информационных системах образовательного учреждения.

Методическое пособие адресовано руководителям образовательных учреждений.

ISBN 978-5-91454-041-5

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Сведения, хранящиеся в базах данных образовательных учреждений, электронных дневниках и журналах являются «персональными данными». Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативно-правовыми актами Российской Федерации в области защиты информации, трудовых отношений и образования, нормативными и распорядительными документами Министерства образования и науки Российской Федерации.

В соответствии с письмами Роскомнадзора от 23.06.2009 № 07-2/6639 и Рособразования от 03.09.2008 № 17-02-09/185, а также письмом ФАО от 29 июля 2009 г. № 17-110, информационные системы персональных данных, созданные после вступления в действие Федерального закона Российской Федерации от 26.07.2006 № 152-ФЗ «О персональных данных», должны соответствовать требованиям данного закона. Ранее созданные информационные системы должны быть приведены в соответствие с требованиями Закона, вступающими в силу с 1 января 2011 года.

Лица, виновные в нарушении требований Закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Во избежание негативных последствий руководители ОУ должны принять все меры по своевременному выполнению требований закона и организовать создание систем защиты персональных данных в подведомственных учреждениях.

В сборнике методических материалов рассматриваются требования нормативных документов по защите персональных данных, вопросы создания систем защиты персональных данных, на компакт-диске приведены нормативные документы, примеры организационно-распорядительных документов.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система	– система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций
Аутентификация отправителя данных	– подтверждение того, что отправитель данных соответствует заявленному
Безопасность информации	– состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы от внутренних и внешних угроз
Безопасность персональных данных	– состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных
Блокирование компьютерной информации	– искусственное затруднение доступа пользователей к защищаемой информации, не связанное с ее уничтожением
Блокирование персональных данных	– временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи
Вирус (компьютерный, программный)	– исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению

Вредоносная программа	– программа, предназначенная для осуществления несанкционированного доступа и/или воздействия на персональные данные или ресурсы информационной системы персональных данных
Вспомогательные технические средства и системы	– технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных
Доступ в операционную среду компьютера (информационной системы персональных данных)	– получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т. п.), исполняемых файлов прикладных программ
Доступ к информации	– ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации
Доступность	– свойство быть доступным и используемым по запросу со стороны уполномоченного логического объекта
Закладочное устройство	– элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации)
Защита информации	– деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию

Защищаемая информация	– информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации
Идентификация	– присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов
Информативный сигнал	– электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных
Информационная система	– совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
Информационная система персональных данных	– это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств
Информационные ресурсы	– отдельные документы, отдельные массивы документов, документы или массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)
Информационные технологии (ИТ)	– процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов

Информация	– сведения (сообщения, данные) независимо от формы их представления
Источник угрозы безопасности информации	– субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации
Источники угрозы	– потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности
ИТ-сервис	– услуга или комплекс услуг, предоставляемых ИТ-подразделениями конечному пользователю
Класс защищенности автоматизированной системы	– определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации
Контролируемая зона	– это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств
Конфиденциальность	– свойство, позволяющее не давать права на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам
Конфиденциальность информации	– обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
Конфиденциальность персональных данных	– обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания

Межсетевой экран	– локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и/или выходящей из информационной системы
Нарушитель безопасности персональных данных	– физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных
Недекларированные возможности	– функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации
Несанкционированный доступ (несанкционированные действия)	– доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и/или правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и своим техническим характеристикам
Носитель информации	– физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин

Обладатель информации	– лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам
Обработка персональных данных	– действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе, передачу), обезличивание, блокирование, уничтожение персональных данных
Объект защиты информации	– информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации
Объект информатизации	– средства и системы информатизации (СВТ, АС различного уровня и назначения на базе СВТ, в том числе информационно-вычислительные комплексы, сети и системы, средства и системы связи и передачи данных, технические средства приема, передачи и обработки информации, программные средства (ОС, СУБД, другое общесистемное и прикладное ПО), используемые для обработки информации, включая помещения, где они установлены
Оператор	– государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и/или осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных
Основные технические средства и системы	– технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи защищаемой информации

Перехват (информации)	– неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов
Персональные данные	– любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация
Побочные электромагнитные излучения и наводки	– электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания
Пользователь информационной системы персональных данных	– лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования
Правила разграничения доступа	– совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа
Программная закладка	– скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода

Программное (программно-математическое) воздействие	– несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ
Ресурс информационной системы	– именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы
Средства вычислительной техники	– совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем
Средства защиты информации	– технические, криптографические, программные и другие средства, предназначенные для защиты информационных ресурсов, а также средства контроля эффективности защиты информации
Субъект доступа (субъект)	– лицо или процесс, действия которого регламентируются правилами разграничения доступа
Технические средства информационной системы персональных данных	– средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т. п.), средства защиты информации

Технический канал утечки информации	– совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация
Угроза безопасности информации	– совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее
Угрозы 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
Уничтожение персональных данных	– действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных
Утечка (защищаемой) информации по техническим каналам	– неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации
Уязвимость	– некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации
Уязвимость (фактор)	– некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации

Целостность информации	– способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения), а также состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

СПИСОК ПРИНЯТЫХ СОКРАЩЕНИЙ

АРМ	автоматизированное рабочее место
АС	автоматизированная система
ВИ	видовая информация
ВТСС	вспомогательные технические средства и системы
ЗИ	защита информации
ИСПДн	информационная система персональных данных
ИТ	информационные технологии
КАИС КРО	Комплексная автоматизированная информационная система каталогизации ресурсов образования
КЗ	контролируемая зона
МЭ	межсетевой экран
НДВ	недекларированные возможности
НСД	несанкционированный доступ
ОБПДн	обеспечение безопасности персональных данных
ОС	операционная система
ПДн	персональные данные
ПМВ	программно-математическое воздействие
ПО	программное обеспечение
ПЭМИН	побочные электромагнитные излучения и наводки
РИ	речевая информация
СВТ	средство вычислительной техники
СЗИ	средство защиты информации
СПИ	стеганографическое преобразование информации
СТЗИ	система технической защиты информации
СЭУПИ	специальные электронные устройства перехвата информации
ТКУИ	технический канал утечки информации
ТСОИ	технические средства обработки информации
УБПДн	угрозы безопасности персональных данных

НОРМАТИВНО-ПРАВОВАЯ БАЗА[1]

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

2. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология – Практические правила управления информационной безопасностью»

3. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»

4. «Базовая Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.

5. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.

6. Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 г. Москва «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

7. Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

8. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России) Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»

9. Сборник руководящих документов по защите информации от несанкционированного доступа, Утвержден Председателем Гостехкомиссии России, 1997 г.

10. Письмо Федерального агентства по образованию от 29.07.2009 № 17-110 «Об обеспечении защиты персональных данных»

[1] Документы представлены на прилагаемом CD-диске.

11. Письмо Федерального агентства по образованию от 03.09.2009 № 17-02-09/185 «О представлении уведомлений об обработке персональных данных»

12. Письмо Федерального агентства по образованию от 22.10.2009 № 17-187 «Об обеспечении защиты персональных данных»

13. Методические рекомендации по организации технической защиты информации в аппаратах органов государственной власти субъектов Российской Федерации, органах исполнительной власти субъектов Российской Федерации, органов местного самоуправления и подведомственных им организациях, находящихся в пределах Северо-Западного Федерального округа, Санкт-Петербург, 2003 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ[2]

В.Е. Ильин,
к.т.н., доцент, методист
ГОУ ДПО ЦПКС СПб «РЦОКОиИТ»

КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ И ОПРЕДЕЛЕНИЕ АКТУАЛЬНЫХ УГРОЗ ИХ БЕЗОПАСНОСТИ

Для проведения классификации ИСПДн, определения категорий персональных данных и экспертной оценки угроз их безопасности целесообразно сформировать комиссию с привлечением специалистов в области информационной безопасности, в том числе по защите государственной тайны.

Перечень типовых ИСПДн определен приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных». Классификация ИСПДн осуществляется в зависимости от категории персональных данных (ПДн), не содержащих сведения, относящиеся к государственной тайне:

Категория 1 – ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

Категория 2 – ПДн, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории 1;

Категория 3 – ПДн, позволяющие идентифицировать субъекта персональных данных;

Категория 4 – обезличенные и/или общедоступные персональные данные.

Целесообразно отдельно определять категории ПДн, обрабатываемых в ИСПДн в электронном и в бумажном виде. В последнем случае следует руководствоваться постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

[2] Использованы материалы приложения 1 к письму Федерального агентства по образованию от 22.10.2009 № 17-187.

Типовые ИСПДн, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных, относятся к классу 1 (К1); к негативным последствиям – к классу 2 (К2); к незначительным негативным последствиям – к классу 3 (К3); не приводит к негативным последствиям для субъектов персональных данных – к классу 4 (К4).

Кроме того, при классификации учитываются объем и территория охвата субъектов персональных данных в порядке, приведенном в приказе ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

Классификация ИСПДн

Количество субъектов ПДн в системе / Категория ПДн, обрабатываемых в электронном виде	Более 100 тыс. ПДн	В объеме		От 1000 до 100 000 ПДн	В объеме				До 1000 ПДн
		РФ	субъекта РФ		отрасли	органа власти	муниципального образования	организации	
1. Расовая, национальная принадлежность, политические взгляды, религиозные и философские убеждения, состояние здоровья, интимная жизнь	1 класс (К1)			1 класс (К1)				1 класс (К1)	
2. Позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории 1	1 класс (К1)			2 класс (К2)				3 класс (К3)	
3. Позволяющие идентифицировать субъекта персональных данных	2 класс (К2)			3 класс (К3)				3 класс (К3)	
4. Обезличенные и/или общедоступные персональные данные	4 класс (К4)			4 класс (К4)				4 класс (К4)	

ИСПДн, обрабатывающие обезличенные или общедоступные персональные данные класса (категории 4) относятся к классу К4. В этом случае обязательные требования по защите ПДн не устанавливаются.

Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» определены необходимые мероприятия по защите персональных данных. В их число входят определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз; разработка на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем, и другие мероприятия.

При обработке персональных данных в информационной системе должно быть обеспечено:

а. проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и/или передачи их лицам, не имеющим права доступа к такой информации (прежде всего, регламентирование доступа сотрудников к обработке персональных данных, парольная и антивирусная защита);

б. своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в. недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д. постоянный контроль за обеспечением уровня защищенности персональных данных.

Определение угроз безопасности персональных данных осуществляется на основе утвержденной ФСТЭК России «Базовой модели угроз безопасности персональных данных». Полный перечень угроз определен ГОСТ Р 51275-2006.

Показатель опасности имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных, что соответствует классу К3;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных, что соответствует классу К2;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных, что соответствует классу К1.

Информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных соответствуют классу К4.

При использовании типовых моделей угроз и соответствующих им требований, приведенных в утвержденных ФСТЭК России «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» следует учитывать, что в ряде случаев возможности реализации отдельных угроз могут быть более высокими и потребовать дополнительных мер защиты персональных данных. Например, возможность реализации угроз увеличивается, если:

– помещения не запираются;

– при обработке персональных данных используются микрофон и динамики;

– монитор не отвернут от окна и посетителей;

– используются беспроводные устройства, в т. ч. клавиатура и мышь;

– отсутствует парольная защита BIOS;

– используются средства сетевого взаимодействия по электропроводке или беспроводные;

– запуск неразрешенных приложений не контролируется.

ОПРЕДЕЛЕНИЕ СПОСОБОВ ПОНИЖЕНИЯ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Существенно уменьшить обязательные требования и необходимые затраты на защиту персональных данных можно путем обезличивания и сегментирования ИСПДн, отключения сегментов ИСПДн от сетей общего пользования, организации выделенных АРМ и др.

Необходимо иметь ввиду, что объявить персональные данные общедоступными только внутри организации, даже с согласия субъектов ПДн, нельзя. В соответствии с Федеральным законом Российской Федерации от 27 июля 2007 г. № 152-ФЗ «О персональных данных», общедоступными являются персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности. Поэтому в информационных системах бухгалтерского и кадрового учета, учета контингента и успеваемости учащихся обязательно будут иметься персональные данные, которые необходимо защищать.

В этой связи наиболее эффективным является обезличивание ИСПДн путем замены ФИО субъектов ПДн на их личные коды (табельные номера), используемые для автоматизированного учета в данной организации.

Вторым по эффективности является полное исключение из ИСПДн сведений 1-й категории, касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни. При необходимости учет персональных данных 1-й категории следует осуществлять в форме анкет, справок, личных дел и иных документов только на бумажных носителях. Для формирования и ведения списков лиц с ограниченными возможностями здоровья конкретные данные о состоянии здоровья, как правило, не требуются.

Персональные данные 2-й категории, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию (за исключением ПДн, относящихся к категории 1), целесообразно вывести из интегрированных ИСПДн в отдельные локальные системы и отключить от Интернета.

Персональные данные 3-й категории, позволяющие только идентифицировать субъекта персональных данных, в зависимости от объема данных и класса ИСПДн можно обезличивать или обрабатывать в неизменном виде.

ИЗМЕНЕНИЕ КЛАССА ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ ПУТЕМ ОБЕЗЛИЧИВАНИЯ

Обезличивание ИСПДн позволяет сохранить действующий порядок доступа пользователей, включая удаленный. При этом нельзя ограничиться обезличиванием вновь вводимых персональных данных, а ранее накопленные оставить в той же базе данных без изменения. Неиспользуемые персональные данные за предшествующие годы целесообразно скопировать на съемные оптические носители и удалить из действующих ИСПДн.

Обезличивание является наиболее приемлемым способом приведения в соответствие требованиям законодательства интегрированных многофункциональных ИСПДн и распределенных ИСПДн, использующих для обмена данными сети общего пользования.

Наиболее просто обезличить ИСПДн, в которых ФИО использовались только в качестве логинов или паролей для доступа учащихся к информационным системам обеспечения учебного процесса. В этом случае достаточно изменить способ формирования идентификационных данных. Функциональность и порядок использования таких обезличенных информационных систем полностью сохраняются.

Возможен также универсальный способ обезличивания и последующей эксплуатации недоступных для самостоятельной модернизации ИСПДн, которые позволяют выводить предназначенные для распечатки бухгалтерские и иные документы в файл в формате MS Excel или MS Word для по-

следующего редактирования. Он заключается в разработке несложной программы или макроса для автоматической обратной замены личных кодов на ФИО в выгруженных из ИСПДн для распечатки документах. Файлы кодификатора (таблицы соответствия) ФИО и личных кодов могут быть легко сформированы путем выгрузки нужной формы из действующей ИСПДн и последующей ручной ее обработки, например, в Excel, с конвертированием в файлы требуемого формата.

Важными достоинствами указанного способа обезличивания ИСПДн, кроме универсальности, являются:

– сохранение функциональности и сервисного сопровождения обезличиваемых действующих ИСПДн без их программной модернизации;

– использование единого кодификатора ФИО, содержащего персональные данные 3 категории, для распечатки документов, выгружаемых из различных обезличиваемых ИСПДн;

– возможность децентрализованного использования кодификатора ФИО на отдельных АРМ;

– обеспечение надлежащего хранения и использования кодификатора ФИО на защищенном встроенном или отдельном внешнем носителе;

– возможность редактирования и дополнения кодификатора ФИО средствами MS Office.

Если численность учащихся превышает 1000 человек и класс ИСПДн соответствует К2, то кодификатор ФИО также может быть разбит на отдельно хранимые части (файлы), не превышающие 1000 человек (по годам зачисления, курсам, факультетам и др.). При этом база обезличенных данных может оставаться общей.

ПОНИЖЕНИЕ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПУТЕМ СЕГМЕНТИРОВАНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Сегментирование заключается в разделении сетевой ИСПДн на несколько сегментов для уменьшения требований и упрощения защиты персональных данных. Оно позволяет:

– децентрализовать обработку персональных данных 2-й категории и понизить класс сегментов ИСПДн до К3, если количество субъектов персональных данных превышает 1000 человек, или если они не принадлежат организации-оператору;

– уменьшить количество защищаемых АРМ в распределенных ИСПДн.

Данный способ на практике является одним из основных.

При сегментировании ИСПДн на взаимодействующие по сети подсистемы следует учитывать, что **класс системы в целом равен наиболее высокому классу ее подсистем** (сегментов). Поэтому простое разделение на

ИСПДн подсистемы без ограничения их взаимодействия не снижает требования по защите персональных данных.

Простейшим способом ограничения взаимодействия сегментов является их физическое изолирование друг от друга. Альтернативным способом сегментирования является использование сертифицированных ФСТЭК России межсетевых экранов. Однако на практике оба эти способа сопряжены с приобретением дополнительного серверного оборудования и программного обеспечения и повышенными затратами на администрирование и технологическое сопровождение сегментированной ИСПДн. Поэтому наиболее целесообразно сегментировать слабо взаимодействующие подсистемы ИСПДн, например, кадрового и бухгалтерского учета персонала и подсистемы обеспечения учебного процесса с обменом данными между ними с помощью съемных носителей.

Более эффективно осуществлять сегментирование до отдельных рабочих мест в сочетании с обезличиванием действующей ИСПДн. При этом затраты на эксплуатацию единой обезличенной ИСПДн не увеличиваются, а хранить кодификаторы ФИО (или их части) можно непосредственно на тех рабочих станциях, на которых персональные данные визуализируются. Если ИСПДн не является распределенной и не подключена к Интернету, то мероприятия по защите отдельных рабочих мест не потребуют больших затрат.

Наиболее сложной является защита персональных данных в распределенных ИСПДн. Поэтому пересылку персональных данных по сетям общего пользования целесообразно осуществлять только в обезличенном виде, а обмен кодификаторами ФИО – курьерским способом. Это позволит избежать классификации и защиты распределенных ИСПДн.

УМЕНЬШЕНИЕ ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИИ ПУТЕМ ОТКЛЮЧЕНИЯ ИСПДН ОТ СЕТЕЙ ОБЩЕГО ПОЛЬЗОВАНИЯ

Подключение ИСПДн к сетям общего пользования, в том числе к Интернету, требует дополнительных средств защиты даже в том случае, если передача персональных данных по ним не предусмотрена. Для уменьшения требований и затрат на защиту информации целесообразно изолировать от Интернета все локальные сетевые ИСПДн.

Если персоналу необходим доступ в Интернет, то наиболее просто предусмотреть для этого дополнительные компьютеры, не подключая их к ИСПДн.

При невозможности размещения дополнительных рабочих станций требуются дополнительные сертифицированные ФСТЭК России средства защиты подключенных к Интернету персональных компьютеров, если они обрабатывают персональные данные.

Средства защиты информации (сертифицированная операционная система или специализированные средства) не должны разрешать одному и

тому же зарегистрированному пользователю обрабатывать персональные данные и выходить в Интернет. Должны быть также разграничены разделы дисковой памяти и сменные носители информации. Выбор и настройка сертифицированных средств защиты информации могут осуществляться системными администраторами образовательных учреждений при консультировании со специалистами в области информационной безопасности. При этом один виртуальный пользователь (со своим логином и паролем) получает возможность выхода в Интернет, а другой – работать с персональными данными. Этими пользователями может быть одно и то же физическое лицо. По сравнению с выделенными АРМ, изолированными от Интернета, затраты на защиту персональных данных в нераспределенных ИСПДн 3 класса для многопользовательских АРМ с разными правами пользователей увеличиваются незначительно.

Для уменьшения требований к защите информации типовые ИСПДн рекомендуется изолировать от сети Интернет. При обработке персональных данных в пределах организации такие системы, как правило, будут соответствовать нераспределенным ИСПДн класса К3. При этом лицензий ФСТЭК России от оператора персональных данных не требуется, а защита данных осуществляется типовыми широко распространенными средствами.

Загрузку обновленных антивирусных баз данных, а также программ и форм персонифицированного учета и отчетности целесообразно осуществлять на других компьютерах, подключенных к сети Интернет. Безопасный перенос загруженных файлов в изолированные от Интернета локальные ИСПДн может осуществляться с использованием маркированных съемных носителей, в обязательном порядке проверяемых антивирусными средствами перед загрузкой в ИСПДн.

Официально распространяемые территориальными органами ФНС России и Пенсионного фонда России программы при соблюдении требований информационной безопасности в изолированных ИСПДн класса К3 могут использоваться при подготовке данных персонифицированного учета. При этом сформированные данные персонализированного учета должны выгружаться из ИСПДн на съемные маркированные носители. Незащищенная пересылка по сети Интернет данных, содержащих ФИО физических лиц, недопустима! Исключение могут составлять сведения, идентифицирующие работников только по ИНН, личному коду пенсионного страхования и другим кодам, без передачи ФИО физических лиц.

ОБЕСПЕЧЕНИЕ ОБМЕНА ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Обмен персональными данными с помощью маркированных съемных носителей не очень удобный, но менее затратный способ защищенного информационного взаимодействия.

Для обеспечения необходимого информационного взаимодействия по сети Интернет (в том числе пересылки электронных платежных документов, данных персонализированного налогового учета и др.) рекомендуется использовать выделенные автоматизированные рабочие места, которые не подключены к локальным сетевым ИСПДн. При этом повышенные требования и необходимость использования дополнительных сертифицированных средств защиты пересылаемых данных распространяются только на соответствующие АРМ.

Перенос персональных данных между взаимодействующими по сети Интернет выделенными АРМ и локальными ИСПДн целесообразно осуществлять с помощью маркированных съемных носителей. В противном случае, необходимо дополнительно использовать дорогостоящие сертифицированные межсетевые экраны.

С целью защиты персональных данных при передаче по каналам связи участниками информационного обмена применяются средства криптографической защиты информации (СКЗИ), сертифицированные в установленном порядке.

ОФОРМЛЕНИЕ АКТОВ КЛАССИФИКАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

После определения способов понижения класса ИСПДн уполномоченная руководителем учреждения комиссия оформляет акты классификации информационных систем персональных данных по форме, приведенной в приложении 1 к письму Федерального агентства по образованию от 22.10.2009 № 17-187, представленного на прилагаемом CD-диске.

ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ 3 И 4 КЛАССОВ

Проектирование и реализация систем защиты типовых ИСПДн, обычно сводится к выбору наименее затратного подходящего типового технического решения.

Стадия реализации типовых ИСПДн 3 класса сводится к приобретению и внедрению типовых технических средств защиты ПДн и адаптации типового комплекта нормативной и регламентирующей документации.

Стадия ввода в действие включает опытную эксплуатацию системы защиты ПДн, приемо-сдаточные испытания, аттестацию или декларирование соответствия требованиям по безопасности информации, обучение персонала.

На заключительном этапе работ осуществляется подготовка уведомления (или соответствующих изменений) в территориальное подразделение Роскомнадзора.

При реализации средств защиты необходимо иметь ввиду, что обязательные требования по защите ПДн для ИСПДн класса К4, обрабатывающих обезличенные или общедоступные персональные данные, не устанавливаются.

Обязательные мероприятия по защите персональных данных в типовых нераспределенных ИСПДн класса К3 могут быть осуществлены без привлечения специалистов в области информационной безопасности. Если в таких системах АРМ пользователей, работающих персональными данными, не подключены к сети (локальной или Интернет), а обмен данными осуществляется с помощью маркированных съемных носителей, то достаточно использовать средства защиты информации (СЗИ), встроенные в сертифицированные ФСТЭК России ОС Windows.

Совпадение программных кодов сертифицированных ФСТЭК России и обычных лицензионных ОС Windows, имеющихся практически в каждом учреждении, дает возможность осуществить самостоятельную апробацию и опытную эксплуатацию системы защиты ИСПДн до приобретения сертифицированных продуктов. Если в результате опытной эксплуатации возможностей СЗИ ОС Windows окажется недостаточно, то от приобретения сертифицированной версии продукта можно отказаться и приобрести специализированные СЗИ, устанавливаемые поверх обычной лицензионной ОС Windows.

В более сложных случаях, чем нераспределенные ИСПДн класса К3, для выполнения работ необходимо привлекать специалистов специализированных организаций.

ПОДГОТОВКА К ПРОВЕРКАМ ЗАКОННОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Роскомнадзор, ФСТЭК России и ФСБ России в рамках своей компетенции осуществляют плановые и внеплановые проверки законности обработки персональных данных. Это предусмотрено регламентом проведения проверок при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных.

Проверка осуществляется в отношении Операторов – государственных органов, муниципальных органов, юридических или физических лиц, организующих и/или осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных.

Проверка соответствия обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных завершается:

– составлением и вручением Оператору акта проверки;

– выдачей Оператору предписания об устранении выявленных нарушений требований законодательства Российской Федерации в области персональных данных;

– составлением протокола об административном правонарушении в отношении Оператора;

– подготовкой и направлением материалов проверки в органы прокуратуры, другие правоохранительные органы для решения вопроса о возбуждении дела об административном правонарушении, о возбуждении уголовного дела по признакам правонарушений (преступлений), связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью.

О проведении плановой проверки Оператор уведомляется не позднее, чем в течение трех рабочих дней до начала ее проведения посредством направления копии приказа руководителя, заместителя руководителя Роскомнадзора или ее территориального органа с уведомлением о вручении или иным доступным способом.

Внеплановые проверки проводятся по следующим основаниям:

– истечение срока исполнения Оператором ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства Российской Федерации в области персональных данных;

– поступление в Роскомнадзор или его территориальные органы обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации о следующих фактах:

– возникновение угрозы причинения вреда жизни, здоровью граждан;

– причинение вреда жизни, здоровью граждан;

– нарушение прав и законных интересов граждан действиями (бездействием) Операторов при обработке их персональных данных;

– нарушение Операторами требований настоящего Федерального закона и иных нормативных правовых актов в области персональных данных, а также о несоответствии сведений, содержащихся в уведомлении об обработке персональных данных, фактической деятельности.

О проведении внеплановой выездной проверки Оператор уведомляется Роскомнадзором или ее территориальным органом не менее чем за двадцать четыре часа до начала ее проведения любым доступным способом.

Должностные лица Роскомнадзора или его территориального органа, в качестве приглашенных специалистов, могут принимать участие в проверках ФСБ России, ФСТЭК России, правоохранительных органов и органов прокуратуры.

В ходе проведения проверки Роскомнадзор или его территориальный орган осуществляют следующие мероприятия по контролю документов Оператора, включающих сведения:

– содержащиеся в уведомлении об обработке персональных данных, поступивших от Оператора и фактической деятельности Оператора;

– о фактах, содержащих признаки нарушения законодательства Российской Федерации в области персональных данных, изложенных в обращениях граждан и информации, поступившей в Роскомнадзор или его территориальный орган;

– о выполнении Оператором предписаний об устранении ранее выявленных нарушений законодательства Российской Федерации в области персональных данных. Данная проверка проводится в виде внеплановой проверки;

– о наличии у Оператора письменного согласия субъекта персональных данных на обработку его персональных данных;

– о соблюдении требований законодательства Российской Федерации при обработке специальных категорий и биометрических персональных данных;

– о порядке и условиях трансграничной передачи персональных данных;

– о порядке обработки персональных данных, осуществляемой без использования средств автоматизации;

– о соблюдении требований конфиденциальности при обработке персональных данных;

– о фактах уничтожения Оператором персональных данных субъектов персональных данных по достижении цели обработки;

– о локальных актах Оператора, регламентирующих порядок и условия обработки персональных данных;

– об иной деятельности, связанной с обработкой персональных данных.

Должностные лица Роскомнадзора или его территориального органа при проведении проверок информационной системы персональных данных, в части касающейся персональных данных субъектов персональных данных, обрабатываемых в ней, вправе в пределах своей компетенции:

– выдавать обязательные для выполнения предписания об устранении выявленных нарушений в области персональных данных;

– составлять протоколы об административном правонарушении или направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении дел об административных правонарушениях, а также о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подследственностью;

– обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных и представлять интересы субъектов персональных данных в суде;

– использовать необходимую технику и оборудование, принадлежащие Роскомнадзору или его территориальному органу;

– запрашивать и получать необходимые документы (сведения) для достижения целей проведения мероприятия по контролю (надзору);

– получать доступ к информационным системам персональных данных;

– направлять заявление в орган, осуществляющий лицензирование деятельности Оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности предусмотрен запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;

– принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушениями требований законодательства Российской Федерации в области персональных данных;

– требовать от Оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных.

Примерный перечень запрашиваемых документов:

– учредительные документы Оператора;

– копия уведомления об обработке персональных данных;

– положение о порядке обработки персональных данных;

– положение о подразделении, осуществляющем функции по организации защиты персональных данных;

– должностные регламенты лиц, имеющих доступ и/или осуществляющих обработку персональных данных;

– план мероприятий по защите персональных данных;

– план внутренних проверок состояния защиты персональных данных;

– приказ о назначении ответственных лиц по работе с персональными данными;

– типовые формы документов, предполагающие или допускающие содержание персональных данных;

– журналы, реестры, книги, содержащие персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор, или в иных аналогичных целях;

– договоры с субъектами персональных данных, лицензии на виды деятельности, в рамках которых осуществляется обработка персональных данных;

– выписки из ЕГРЮЛ, содержащие актуальные данные на момент проведения проверки;

– приказы об утверждении мест хранения материальных носителей персональных данных;

– письменное согласие субъектов персональных данных на обработку их персональных данных (типовая форма);

– распечатки электронных шаблонов полей, содержащие персональные данные;

– справки о постановке на балансовый учет ПЭВМ, на которых осуществляется обработка персональных данных;

– заключения экспертизы ФСБ России, ФСТЭК России об оценке соответствия средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке (проверяется только наличие данных документов);

– приказ о создании комиссии и акты проведения классификации информационных систем персональных данных (проверяется только наличие данных документов);

– журналы (книги) учета обращений граждан (субъектов персональных данных);

– акт об уничтожении персональных данных субъекта(ов) персональных данных (в случае достижения цели обработки);

– иные документы, отражающие исполнение Оператором требований законодательства Российской Федерации в области персональных данных.

Акт по результатам проверки может содержать одно из следующих заключений:

– об отсутствии нарушений требований законодательства Российской Федерации в области персональных данных;

– о выявленных нарушениях требований законодательства Российской Федерации в области персональных данных, с указанием конкретных статей и/или пунктов нормативных правовых актов.

Наличие и соблюдение персоналом требуемых распорядительных документов и инструкций является необходимым условием обеспечения информационной безопасности персональных данных.

Такие важные вопросы обработки персональных данных, как:

– оформление согласия на обработку персональных данных;

– законодательство о защите персональных данных;

– порядок обработки персональных данных, осуществляемой без использования средств автоматизации;

– основные обязанности операторов информационных систем, обрабатывающих персональные данные;

– основные мероприятия по обеспечению безопасности персональных данных в учреждениях образования;

– порядок проведения аттестационных (сертификационных) испытаний;

– декларирование соответствия,

изложены в письме Федерального агентства по образованию от 29.07.2009 № 17-110 «Об обеспечении защиты персональных данных».

ПЕРЕЧЕНЬ ДОКУМЕНТОВ, РЕГЛАМЕНТИРУЮЩИХ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ В ПОДВЕДОМСТВЕННЫХ РОСОБРАЗОВАНИЮ УЧРЕЖДЕНИЯХ[3]

В.А. Стрельцов,
Генеральный директор
ООО «ТИЕРА ЦЕНТР»

А.В. Ушаков
Заместитель директора
ГОУ ДПО ЦПКС СПб «РЦОКОиИТ»

ПРИКАЗ О СОЗДАНИИ КОМИССИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ С НАДЕЛЕНИЕМ ЕЕ ПОЛНОМОЧИЯМИ ПО ПРОВЕДЕНИЮ МЕРОПРИЯТИЙ, КАСАЮЩИХСЯ ОРГАНИЗАЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

В комиссию рекомендуется включать руководителей или полномочных представителей всех структурных подразделений учреждения, обрабатывающих персональные данные. Председателем комиссии целесообразно назначить заместителя руководителя учреждения. При необходимости, вместо создания отдельной комиссии по защите персональных данных могут быть расширены состав и полномочия комиссии по защите сведений, составляющих государственную тайну.

ПРИКАЗ ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Общие положения, в том числе:

– предмет Положения – порядок получения, обработки, использования, хранения и гарантии конфиденциальности персональных данных физических лиц, необходимых для осуществления деятельности;

– цель и задачи учреждения в области защиты персональных данных (обеспечение в соответствии с законодательством Российской Федерации

[3] Использованные материалы представлены в приложении 2 к письму Федерального агентства по образованию от 22.10.2009 № 17-187, представленного на прилагаемом CD-диске. Формы документов, регламентирующих обработку персональных данных в подведомственных Рособразованию учреждениях, представлены в приложении 2 к письму Федерального агентства по образованию от 22.10.2009 № 17-187, представленного на прилагаемом CD-диске.

обработки, хранения и защиты персональных данных работников, учащихся и выпускников, а также персональных данных, содержащихся в документах, полученных из других организаций, в обращениях граждан и иных субъектов персональных данных);

– понятие и состав персональных данных;

– наименование учреждения (допускается привлекать для обработки персональных данных уполномоченные организации на основе соответствующих договоров и соглашений).

Порядок получения и обработки персональных данных:

– как происходит получение персональных данных (получение персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора, Положением об обработке и защите персональных данных и приказами учреждения на основе согласия субъектов на обработку их персональных данных. Оператор не вправе требовать от субъекта персональных данных предоставления информации о его национальности и расовой принадлежности, политических и религиозных убеждениях и о его частной жизни. Без согласия субъектов осуществляется обработка общедоступных персональных данных или содержащих только фамилии, имена и отчества, обращений и запросов организаций и физических лиц, регистрация и отправка корреспонденции почтовой связью, оформление разовых пропусков, обработка персональных данных для исполнения трудовых договоров или без использования средств автоматизации, и в иных случаях, предусмотренных законодательством Российской Федерации);

– как они обрабатываются и используются – обработка и использование персональных данных осуществляется в целях, указанных в соглашениях с субъектами персональных данных, а также в случаях, предусмотренных нормативно-правовыми актами Российской Федерации. Правила обработки и использования персональных данных устанавливаются отдельными регламентами и инструкциями Оператора;

– в каких структурных подразделениях и на каких носителях (бумажных, электронных) накапливаются и хранятся эти данные. Также целесообразно привести в приложении к приказу об утверждении Положения укрупненный перечень персональных данных и перечень структурных подразделений и/или отдельных должностей, имеющих право на их обработку*)*;

– на каком основании персональные данные защищаются от несанкционированного доступа.

Права, обязанности и ответственность субъекта персональных данных и Оператора при обработке персональных данных,
в том числе:

– права субъекта персональных данных в целях обеспечения защиты своих персональных данных (в целях обеспечения защиты своих персональных данных субъект персональных данных в соответствии с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ «О персональных данных» за исключением случаев, предусмотренных данным Федеральным законом, имеет право на получение сведений об Операторе, о месте его нахождения, о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными; требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав; на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных; на обжалование действий или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке; на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке);

– обязанности Оператора при сборе персональных данных (Оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы;

– в случае выявления неправомерных действий с персональными данными Оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий

с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя;

– в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Оператором и субъектом персональных данных. Об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных);

– права Оператора на передачу персональных данных третьим лицам (Оператор не вправе без письменного согласия субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации);

– ответственность Оператора за разглашение персональных данных (Оператор, а также должностные лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается в приказе об утверждении Положения и иных приказах на руководителей структурных подразделений и конкретных должностных лиц Оператора, обрабатывающих персональные данные).

ПИСЬМЕННОЕ СОГЛАСИЕ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ИХ ОБРАБОТКУ

Требования к оформлению согласия субъектов персональных данных на их обработку изложены в письме Федерального агентства по образованию от 29.07.2009 № 17-110 «Об обеспечении защиты персональных данных».

ПРИКАЗ О ВОЗЛОЖЕНИИ ПЕРСОНАЛЬНОЙ ОТВЕТСТВЕННОСТИ ЗА ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

В приказе рекомендуется привести список конкретных лиц, ответственных за защиту информационных систем и групп обрабатываемых в учреждении персональных данных.

РАЗРЕШИТЕЛЬНЫЕ ДОКУМЕНТЫ О ДОПУСКЕ КОНКРЕТНЫХ СОТРУДНИКОВ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Приказы или иные утвержденные руководством учреждения разрешительные документы должны включать списки сотрудников Оператора и временно привлекаемых лиц, допущенных к обработке укрупненных групп персональных данных. Работа с персональными данными лиц, не включенных в разрешительные документы, не допускается.

УВЕДОМЛЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

В соответствии со статьей 22 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», приказами Роскомнадзора и утвержденной формой уведомления, размещенными на его официальном сайте www.rsoc.ru, уведомление об обработке персональных данных должно быть направлено в соответствующее территориальное подразделение Роскомнадзора.

В соответствии с приведенными законодательными и нормативными актами уведомление должно содержать следующие сведения:

– наименование, адрес Оператора;

– цель обработки персональных данных;

– категории персональных данных;

– категории субъектов, персональные данные которых обрабатываются;

– правовое основание обработки персональных данных;

– перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных;

– описание мер, которые Оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке;

– дата начала обработки персональных данных;

– срок или условие прекращения обработки персональных данных.

Без уведомления Оператор вправе осуществлять обработку персональных данных:

– относящихся к субъектам персональных данных, которых связывают с Оператором трудовые отношения;

– полученных Оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются Оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

– относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующим общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

– являющихся общедоступными персональными данными;

– включающих в себя только фамилии, имена и отчества субъектов персональных данных;

– необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится Оператор, или в иных аналогичных целях;

– включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

– обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

ДОЛЖНОСТНЫЕ ИНСТРУКЦИИ СОТРУДНИКОВ, ИМЕЮЩИХ ОТНОШЕНИЕ К ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Должностные инструкции сотрудников учреждения, дополненные положениями о необходимости соблюдения утвержденного Положения об обработке и защите персональных данных и Инструкции о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные.

ЖУРНАЛ ОБРАЩЕНИЙ ПО ОЗНАКОМЛЕНИЮ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Журнал рекомендуется вести в каждом структурном подразделении в произвольной форме. В журнале необходимо фиксировать все обращения субъектов персональных данных (дата, ФИО, адрес) по ознакомлению с их персональными данными, дату направления запрашиваемых данных почтовой связью или предоставления лично заявителю. В случае отзыва данных субъектом персональных данных или выявления их несоответствия, в журна-

ле должны быть сделаны соответствующие записи. По каждому обращению необходимо указывать, когда и каким образом на него было отреагировано. Хранение журналов должно исключать несанкционированный доступ к ним.

ИНСТРУКЦИЯ О ПОРЯДКЕ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ ПРИ ОБРАЩЕНИИ С ИНФОРМАЦИЕЙ, СОДЕРЖАЩЕЙ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Общие положения, в том числе:

– предмет Инструкции (обязательные для всех структурных подразделений учреждения требования по обеспечению конфиденциальности документов, содержащих персональные данные);

– определение персональных данных (персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация);

– когда обеспечение конфиденциальности персональных данных не требуется (в случае обезличивания персональных данных или в отношении общедоступных персональных данных. В общедоступные источники персональных данных (в том числе справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных);

– необходимость согласия субъекта персональных данных или наличие иного законного основания на их обработку (конфиденциальность персональных данных предусматривает обязательное согласие субъекта персональных данных или наличие иного законного основания на их обработку). Согласие субъекта персональных данных не требуется на обработку:

- данных в целях исполнения обращения, запроса субъекта персональных данных, трудового или иного договора с ним;
- адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;
- данных, включающих в себя только фамилии, имена и отчества;
- данных в целях однократного пропуска на территорию, или в иных аналогичных целях;
- персональных данных, обрабатываемых без использования средств автоматизации;

– порядок ведения перечней персональных данных (в структурных подразделениях учреждения формируются и ведутся перечни конфиденциальных данных с указанием регламентирующих документов, мест хранения и ответственных за хранение и обработку данных. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается);

– нормативные документы, определяющие основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных и использования средств автоматизации (Основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных установлены постановлениями Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее);

– общие правила хранения и передачи персональных данных (запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении. Все сотрудники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных).

Сотрудникам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

Передача персональных данных допускается только в случаях, установленных Федеральными законами Российской Федерации «О персональных данных», «О порядке рассмотрения обращений граждан Российской Федерации», действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

Ответственность за защиту обрабатываемых персональных данных (например, сотрудники подразделений учреждения, сотрудники организаций-Операторов или лица, осуществляющие такую обработку по договору с Оператором, а также иные лица, осуществляющие обработку или хранение конфиденциальных данных в «учреждении», несут ответственность за обеспечение их информационной безопасности. Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами).

Порядок ознакомления с Инструкцией (сотрудники подразделений учреждения и лица, выполняющие работы по договорам и контрактам, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под расписку с настоящей Инструкцией).

Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой с использованием средств автоматизации, в том числе,

– правила доступа, хранения и пересылки персональных данных (например, безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии).

Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

Компьютеры и/или электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более симво-

лов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе по Интернету, запрещается.

Общие требования по защите персональных данных в автоматизированных системах (например, технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия).

При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

– использование предназначенных для этого раздела (каталога) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

– недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

– постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– недопущение несанкционированного выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

– обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

– учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

– контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– описание системы защиты персональных данных.

Специфические требования по защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации, в том числе:

– организация учета носителей персональных данных – все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

Учет и выдачу съемных носителей персональных данных осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Сотрудники учреждения получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

Правила использования съемных носителей персональных данных:

– запрещается хранить съемные носители с персональными данными вместе с носителями открытой информации на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

– запрещается выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т. д.

При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

Порядок действий при утрате или уничтожении съемных носителей персональных данных (например, о фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность начальник соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы персонального учета съемных носителей персональных данных).

Съемные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт.

При осуществлении обработки персональных данных с использованием средств автоматизации для каждой информационной системы персональных данных должен быть назначен администратор, а для системы высоких классов – также администратор системы безопасности. Инструкции для этого должностного лица составляются отдельно. Для технического обслуживания оборудования должен быть предусмотрен соответствующий обслуживающий персонал.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ОБЪЕКТАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Общие положения:

– предмет Инструкции (основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) учреждения);

– общие требования к пользователю (пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПЭВМ. Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ и несет персональную ответственность за соблюдение требований руководящих документов по защите информации).

Обязанности пользователя:

– выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции;

– при работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц, или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра, отображаемой на нем информации посторонними лицами;

– соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;

– после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня, произвести стирание остаточной информации с жесткого диска ПЭВМ;

– оповещать обслуживающий ПЭВМ персонал, а также непосредственного начальника о всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;

– не допускать «загрязнение» ПЭВМ посторонними программными средствами;

– знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий;

– знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий;

– помнить личные пароли, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе;

– знать штатные режимы работы программного обеспечения, знать пути проникновения и распространения компьютерных вирусов;

– при применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов;

– при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции;

– в случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

– приостановить работу;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника, администратора системы, а также смежные подразделения, использующие эти файлы в работе;

– оценить необходимость дальнейшего использования файлов, зараженных вирусом;

– провести лечение или уничтожение зараженных файлов (при необходимости, для выполнения требований данного пункта следует привлечь администратора системы).

Запрещаемые действия:

– записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации;

– удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;

– самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;

– самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;

– осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ;

– сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;

– отключать (блокировать) средства защиты информации;

– производить какие-либо изменения в подключении и размещении технических средств;

– производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями;

– оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.

Права пользователя ПЭВМ:

– обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий;

– обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

Ответственность пользователей ПЭВМ за:

– надлежащее выполнение требований настоящей инструкции;

– соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов;

– сохранность и работоспособное состояние средств вычислительной техники ПЭВМ;

– сохранность персональных данных.

Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

ИНСТРУКЦИЯ ПО ПРОВЕДЕНИЮ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И АНТИВИРУСНОГО КОНТРОЛЯ ПРИ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Общие положения, определяющие предмет Инструкции (порядок планирования и проведения мониторинга информационной безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации учреждения).

Мониторинг работоспособности аппаратных компонент автоматизированных систем, обрабатывающих персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование) должны контролироваться постоянно в рамках работы администраторов соответствующих систем.

Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

– установление сроков действия паролей (не более 3 месяцев);

– периодическую (не реже 1 раза в месяц) проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

Мониторинг целостности программного обеспечения включает следующие действия:

– проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;

– обнаружение дубликатов идентификаторов пользователей;

– восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

Мониторинг попыток несанкционированного доступа – предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы и специальных программных средств, и предусматривает:

– фиксацию неудачных попыток входа в систему в системном журнале;

– протоколирование работы сетевых сервисов;

– выявление фактов сканирования определенного диапазона сетевых портов, в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

Мониторинг производительности автоматизированных систем, обрабатывающих персональные данные, производится по обращениям пользователей, в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности систем.

Системный аудит производится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности, тестирование системы, контроль внесения изменений в системное программное обеспечение.

Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, тому уровню безопасности, который удовлетворяет требованиям политики безопасности. Обзоры безопасности имеют целью выявление всех несоответствий между текущим состоянием системы и состоянием, соответствующим специально составленному списку для проверки.

Обзоры безопасности должны включать:

– отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;

– проверку содержимого файлов конфигурации на соответствие списку для проверки;

– обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);

– проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);

– проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;

– проверку корректности конфигурации системных и активных сетевых устройств.

Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы. Информация об известных уязвимостях извлекается из документации и внешних источников. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то, с целью нейтрализации уязвимостей, необходимо, либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

Внесение изменений в системное программное обеспечение осуществляется администраторами систем, обрабатывающих персональные данные, с обязательным документированием изменений в соответствую-

щем журнале; уведомлением каждого сотрудника, кого касается изменение; выслушиванием претензий в случае, если это изменение причинило комунибудь вред; разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

Антивирусный контроль – для защиты серверов и рабочих станций необходимо использовать антивирусные программы:

– резидентные антивирусные мониторы, контролирующие подозрительные действия программ;

– утилиты для обнаружения и анализа новых вирусов.

К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.

При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения рабочей станции должна быть выполнена антивирусная проверка.

Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещении.

Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т. п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее:

– осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;

– проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

На серверах электронной почты необходимо применять антивирусное программное обеспечение, обеспечивающее проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна блокироваться. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

Необходимо организовать регулярное обновление антивирусных баз на всех рабочих станциях и серверах.

Администраторы систем должны проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которых распространяются вирусы. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

– отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;

– немедленно сообщить о факте обнаружения вирусов непосредственному начальнику с указанием предположительного источника (отправителя, владельца и т. д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

Анализ инцидентов

Если администратор системы, обрабатывающей персональные данные, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, то он должен установить:

– факт попытки несанкционированного доступа (НСД);

– продолжается ли НСД в настоящий момент;

– кто является источником НСД;

– что является объектом НСД;

– когда происходила попытка НСД;

– как и при каких обстоятельствах была предпринята попытка НСД;

– точку входа нарушителя в систему;

– была ли попытка НСД успешной;

– системные ресурсы, безопасность которых была нарушена;

– какова мотивация попытки НСД.

Для выявления попытки НСД необходимо установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях. Выявить подозрительную активность пользователей, проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго. Кроме того, необходимо проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

При анализе системных журналов администратору необходимо произвести следующие действия:

– проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;

– проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;

– просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;

– проверить наличие исходящих сообщений электронной почты, адресованных подозрительным хостам;

– проверить наличие мест в журналах, которые выглядят необычно;

– выявить попытки получить полномочия суперпользователя или другого привилегированного пользователя;

– выявить наличие неудачных попыток входа в систему.

В ходе анализа журналов активного сетевого оборудования необходимо:

– проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;

– проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;

– проверить наличие мест в журналах, которые выглядят необычно;

– выявить попытки изменения таблиц маршрутизации и адресных таблиц;

– проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

– составить базовую схему того, как обычно выглядит система;

– провести поиск подозрительных файлов, скрытые файлы, имена файлов и каталогов, которые обычно используются злоумышленниками;

– проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;

– проверить целостность системных программ;

– проверить систему аутентификации и авторизации.

В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

Особенности мониторинга информационной безопасности персональных данных в отдельных автоматизированных системах могут регулироваться дополнительными инструкциями.

БАЗОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ[4]

В.Ф. Шетка
к. в. н., профессор, Военная академия связи им. С.М. Буденного

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее – Модель угроз) содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Модель угроз содержит единые исходные данные по угрозам безопасности персональных данных, обрабатываемых в информационных системах персональных данных (ИСПДн), связанным:

– с перехватом (съемом) ПДн по техническим каналам с целью их копирования или неправомерного распространения;

– с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

С применением Модели угроз решаются следующие задачи:

– разработка частных моделей угроз безопасности ПДн в конкретных ИСПДн с учетом их назначения, условий и особенностей функционирования;

– анализ защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;

– разработка системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;

– проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и/или передачи их лицам, не имеющим права доступа к такой информации;

– недопущение воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;

[4] Извлечения из «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной Заместителем директора ФСТЭК России 15 февраля 2008 г.

– контроль обеспечения уровня защищенности персональных данных.

Угрозы безопасности ПДн, обрабатываемых в ИСПДн, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации УБПДн в ИСПДн. Внесение изменений в Модель угроз осуществляется ФСТЭК России в устанавливаемом порядке.

КЛАССИФИКАЦИЯ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Состав и содержание УБПДн определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн.

Совокупность таких условий и факторов формируется с учетом характеристик ИСПДн, свойств среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, и возможностей источников угрозы.

К характеристикам ИСПДн, обусловливающим возникновение УБПДн, можно отнести категорию и объем обрабатываемых в ИСПДн персональных данных, структуру ИСПДн, наличие подключений ИСПДн к сетям связи общего пользования и/или сетям международного информационного обмена, характеристики подсистемы безопасности ПДн, обрабатываемых в ИСПДн, режимы обработки персональных данных, режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.

Информационные системы ПДн представляют собой совокупность информационных и программно-аппаратных элементов, а также информационных технологий, применяемых при обработке ПДн.

Основными элементами ИСПДн являются:

– персональные данные, содержащиеся в базах данных, как совокупность информации и ее носителей, используемых в ИСПДн;

– информационные технологии, применяемые при обработке ПДн;

– технические средства, осуществляющие обработку ПДн;

– программные средства (операционные системы, системы управления базами данных и т. п.);

– средства защиты информации;

– вспомогательные технические средства и системы (ВТСС) – технические средства и системы, их коммуникации, не предназначенные для обработки ПДн, но размещенные в помещениях, в которых расположены ИСПДн, их технические средства, осуществляющие обработку ПДн.

Свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической

среды, в которой распространяются ПДн, и определяются при оценке возможности реализации УБПДн.

Возможности источников УБПДн обусловлены совокупностью способов несанкционированного и/или случайного доступа к ПДн, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПДн.

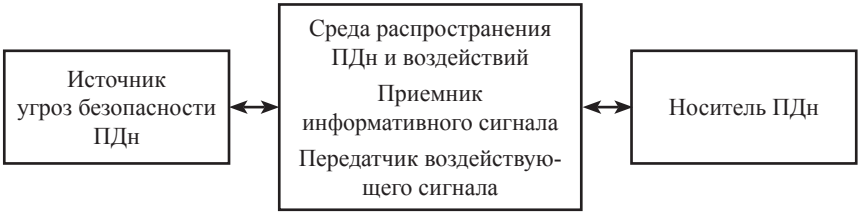
Угроза безопасности ПДн реализуется в результате образования канала реализации УБПДн между источником угрозы и носителем (источником) ПДн, что создает условия для нарушения безопасности ПДн (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПДн являются:

– источник УБПДн – субъект, материальный объект или физическое явление, создающие УБПДн;

– среда (путь) распространения ПДн или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПДн;

– носитель ПДн – физическое лицо или материальный объект, в том числе физическое поле, в котором ПДн находят свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.



Обобщенная схема канала реализации угроз безопасности персональных данных

Носители ПДн могут содержать информацию, представленную в следующих видах:

– акустическая (речевая) информация (РИ), содержащаяся непосредственно в произносимой речи пользователя ИСПДн при осуществлении им функции голосового ввода ПДн в ИСПДн, либо воспроизводимая акустическими средствами ИСПДн (если такие функции предусмотрены технологией обработки ПДн), а также содержащаяся в электромагнитных полях и электрических сигналах, которые возникают за счет преобразований акустической информации;

– видовая информация (ВИ), представленная в виде текста и изображений различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн;

– информация, обрабатываемая (циркулирующая) в ИСПДн, в виде электрических, электромагнитных, оптических сигналов;

– информация, обрабатываемая в ИСПДн, представленная в виде бит, байт, файлов и других логических структур.

В целях формирования систематизированного перечня УБПДн при их обработке в ИСПДн и разработке на их основе частных моделей применительно к конкретному виду ИСПДн угрозы классифицируются в соответствии со следующими признаками:

– по виду защищаемой от УБПДн информации, содержащей ПДн;

– по видам возможных источников УБПДн;

– по типу ИСПДн, на которые направлена реализация УБПДн;

– по способу реализации УБПДн;

– по виду нарушаемого свойства информации (виду несанкционированных действий, осуществляемых с ПДн);

– по используемой уязвимости;

– по объекту воздействия.

По видам возможных источников УБПДн выделяются следующие классы угроз:

– угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн (внутренний нарушитель);

– угрозы, связанные с преднамеренными или непреднамеренными действиями лиц, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и/или сетей международного информационного обмена (внешний нарушитель).

Кроме того, угрозы могут возникать в результате внедрения аппаратных закладок и вредоносных программ.

По типу ИСПДн, на которые направлена реализация УБПДн, выделяются следующие классы угроз:

– угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе автономного автоматизированного рабочего места (АРМ);

– угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе АРМ, подключенного к сети общего пользования (к сети международного информационного обмена);

– угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);

– угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена);

– угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем без подключения к сети общего пользования (к сети международного информационного обмена);

– угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе распределенных информационных систем с подключением к сети общего пользования (к сети международного информационного обмена).

По способам реализации УБПДн выделяются следующие классы угроз:

– угрозы, связанные с НСД к ПДн (в том числе угрозы внедрения вредоносных программ);

– угрозы утечки ПДн по техническим каналам утечки информации;

– угрозы специальных воздействий на ИСПДн.

По виду несанкционированных действий, осуществляемых с ПДн, выделяются следующие классы угроз:

– угрозы, приводящие к нарушению конфиденциальности ПДн (копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;

– угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на содержание информации, в результате которого осуществляется изменение ПДн или их уничтожение;

– угрозы, приводящие к несанкционированному, в том числе случайному, воздействию на программные или программно-аппаратные элементы ИСПДн, в результате которого осуществляется блокирование ПДн.

По используемой уязвимости выделяются следующие классы угроз:

– угрозы, реализуемые с использованием уязвимости системного ПО;

– угрозы, реализуемые с использованием уязвимости прикладного ПО;

– угрозы, возникающие в результате использования уязвимости, вызванной наличием в АС аппаратной закладки;

– угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;

– угрозы, возникающие в результате использования уязвимости, вызванной недостатками организации ТЗИ от НСД;

– угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации;

– угрозы, реализуемые с использованием уязвимостей СЗИ.

По объекту воздействия выделяются следующие классы угроз:

– угрозы безопасности ПДн, обрабатываемых на АРМ;

– угрозы безопасности ПДн, обрабатываемых в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т. п.);

– угрозы безопасности ПДн, передаваемых по сетям связи;

– угрозы прикладным программам, с помощью которых обрабатываются ПДн;

– угрозы системному ПО, обеспечивающему функционирование ИСПДн.

Реализация одной из УБПДн перечисленных классов или их совокупности может привести к следующим типам последствий для субъектов ПДн:

– значительным негативным последствиям для субъектов ПДн;

– негативным последствиям для субъектов ПДн;

– незначительным негативным последствиям для субъектов ПДн.

Угрозы утечки ПДн по техническим каналам однозначно описываются характеристиками источника информации, среды (пути) распространения и приемника информативного сигнала, то есть определяются характеристиками технического канала утечки ПДн.

Угрозы, связанные с несанкционированным доступом (НСД), представляются в виде совокупности обобщенных классов возможных источников угроз НСД, уязвимостей программного и аппаратного обеспечения ИСПДн, способов реализации угроз, объектов воздействия (носителей защищаемой информации, директориев, каталогов, файлов с ПДн или самих ПДн) и возможных деструктивных действий.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В РАБОТЕ СЕРВИСА «ЭЛЕКТРОННЫЙ ДНЕВНИК» КОМПЛЕКСНОЙ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ КАТАЛОГИЗАЦИИ РЕСУРСОВ ОБРАЗОВАНИЯ (КАИС КРО)

А.В. Скворцов
Менеджер проекта, ООО «Нетрика»

ОБЩАЯ ИНФОРМАЦИЯ О СИСТЕМЕ

Комплексная автоматизированная информационная система каталогизации ресурсов образования (КАИС КРО) предназначена для автоматизации информационного взаимодействия и информационного обеспечения участников образовательного процесса за счет реализации следующих функций:

– предоставление участникам образовательного процесса информации об образовательных учреждениях Санкт-Петербурга;

– предоставление информации о типах и объемах предоставляемых образовательных услуг, сгруппированной по географическому признаку в рамках городского района;

– взаимодействие с информационными системами «ПараГраф-ОУ» и «ПараГраф-Регион»;

– предоставление родителям и законным представителям доступа к индивидуальной информации об успеваемости конкретного ученика.

Система реализует принцип «единого окна», обеспечивающего доступ к широкому спектру ресурсов и данных через Интернет с единой точкой входа.

Разработка системы осуществляется на основании следующих документов:

– Постановление Правительства Санкт-Петербурга от 27 июля 2010 года № 932 «О плане мероприятий по развитию информационного общества и формированию электронного правительства в Санкт-Петербурге на 2010–2012 годы»;

– Постановление Правительства Санкт-Петербурга от 30.09.2008 года № 1202 «О плане мероприятий по информатизации системы образования Санкт-Петербурга на 2009–2010 годы».

Система упорядочивает и структурирует большое количество ценных ресурсов и данных и способствует повышению информированности жителей Санкт-Петербурга о возможностях, предоставляемых образовательными учреждениями города. Она является платформой для развития информационной образовательной среды города.

СЕРВИС «ЭЛЕКТРОННЫЙ ДНЕВНИК»

В рамках системы КАИС КРО реализован онлайн-сервис «Электронный дневник», который позволяет родителям и законным представителям учеников получать через Интернет сведения о различных аспектах образовательного процесса применительно к конкретному ученику.

В частности, сервис обеспечивает доступ к следующей информации:

– расписание;
– текущие и итоговые отметки;
– домашние задания;
– результаты ЕГЭ и ГИА;
– портфолио учащегося;
– посещаемость;
– переписка с педагогами;
– объявления.

Приоритетность внедрения сервисов подобного типа неоднократно подчеркивалась в выступлениях Президента РФ Д.А. Медведева, который, в частности, говорил на заседании президиума Госсовета о реализации Стратегии развития информационного общества о необходимости внедрения электронных версий дневника и классного журнала в дополнение к существующим бумажным.

Возможность прямого и оперативного доступа к сведениям об успеваемости, поведении и других аспектах учебной деятельности ученика для его родителей и законных представителей позволяет значительно улучшить взаимодействие семьи и педагогов, обеспечить регулярный контроль за образовательным процессом, повысить мотивацию учащихся.

В соответствии с п. 4 Распоряжения Комитета по образованию Правительства Санкт-Петербурга «О внедрении комплексной автоматизированной информационной системы каталогизации ресурсов образования» сервис «Электронный дневник» должен быть введен в штатный режим всеми государственными общеобразовательными учреждениями Санкт-Петербурга с 01.01.2011 г.». Высокие темпы внедрения сервиса и системы КАИС КРО, в целом, требуют от всех заинтересованных сторон, включая общеобразовательные учреждения, четких и согласованных действий, касающихся всех аспектов их функционирования.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: ОБЩИЕ ПОЛОЖЕНИЯ

Важной составляющей мероприятий по разработке и внедрению системы является соблюдение требований по защите персональных данных, которые зафиксированы в законодательстве Российской Федерации и соответствуют нормам международного права, в частности, Конвенции Совета

Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года.

Базовым в проблематике защиты персональных данных является принятый в 2006 году Федеральный закон Российской Федерации № 152-ФЗ «О персональных данных». На сегодняшний день существует целый ряд документов, которые фиксируют требования по защите персональных данных, в частности:

– Постановление Правительства Российской Федерации от 17.11.2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Эти документы предъявляют ряд требований как к информационным системам, оперирующим персональными данными, так и непосредственно к операторам персональных данных, под которыми могут подразумеваться юридические или физические лица, организующие и/или осуществляющие обработку персональных данных, а также определяющие цели и содержание такой обработки.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБРАЗОВАНИИ

Образование как важнейший социальный институт тесно связано с правом на неприкосновенность частной жизни, которое зафиксировано в Статье 23 Конституции Российской Федерации. Все участники образовательного процесса, начиная с контролирующих органов и заканчивая образовательными учреждениями, обязаны обеспечивать конфиденциальность данных об учениках и их семьях.

Проблеме защиты персональных данных было посвящено Письмо Федерального агентства по образованию от 29.07.2009 № 17-110 «Об обеспечении защиты персональных данных», адресованное руководителям госучреждений, подведомственных Рособразованию. Этот документ, ссылающийся на Федеральный закон № 152-ФЗ «О персональных данных» содержит, в частности, предупреждение руководителям образовательных учреждений о том, что «лица, виновные в нарушении требований закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность».

Также в Письме содержится рекомендация по применению личного кода (внутреннего идентификационного номера субъекта персональных данных, присваиваемого на весь период обучения или работы), что позволит

«обезличить базы данных, если в них не содержатся иные персональные данные, и существенно сократить затраты на защиту информации». О том, как эта рекомендация реализована при разработке системы КАИС КРО, будет подробно рассказано далее.

ПОРЯДОК ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Лица, осуществляющие обработку персональных данных, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами.

Должны быть определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ. Должно быть обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях, и соблюдены условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

Применительно к системе КАИС КРО операторы обязаны обеспечивать поддержку защиты персональных данных при вводе и обработке персональной информации с момента внедрения системы в эксплуатацию.

Учебные учреждения обязаны следовать соответствующим руководящим документам с оформлением соответствующего акта о декларировании полномочий по поддержке работоспособности комплекса мер по защите персональных данных, а также провести первичную оценку соответствия информационной системы требованиям внутренних документов объекта образования и составить акт ввода в эксплуатацию в форме аттестации.

Декларирование полномочий может осуществляться на основе собственных документов или на основании документов, полученных с участием привлеченных организаций.

Во избежание предоставления информации сторонним лицам оператор системы КАИС КРО должен ознакомиться с инструкцией об обработке персональных данных под роспись.

ОТВЕТСТВЕННОСТЬ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ И ИХ СОТРУДНИКОВ ПРИ РАБОТЕ С СИСТЕМОЙ КАИС КРО И СЕРВИСОМ «ЭЛЕКТРОННЫЙ ДНЕВНИК»

Образовательные учреждения несут ответственность за неисполнение инструкций по выполнению обработки персональной информации операторами, а также за невыполнение поддержания системы безопасности в работоспособном состоянии и доступа к АРМ сторонним лицам.

Сотрудники образовательных учреждений, осуществляющие работу с системой КАИС КРО, несут ответственность за невыполнение инструкции по работе с системой КАИС КРО и невыполнение требований безопасности при работе с персональной информацией.

Таким образом, полнота соответствия требованиям к защите персональных данных в используемой информационной системе имеет принципиальное значение для всех участников образовательного процесса. Руководство и коллектив образовательных учреждений как лица, вовлеченные в работу с персональными данными, вправе знать, каким образом внедряемая система гарантирует их защиту и исключает вероятность несанкционированного доступа.

РЕАЛИЗАЦИЯ МЕХАНИЗМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СИСТЕМЕ КАИС КРО И СЕРВИСЕ «ЭЛЕКТРОННЫЙ ДНЕВНИК»

Разработка системы КАИС КРО с точки зрения информационной и системной архитектуры изначально предусматривала соблюдение требований по защите персональных данных. Особое внимание этой проблеме было уделено при создании сервиса «Электронный дневник», так как именно этот компонент системы целиком и полностью предназначен для сбора, обработки и передачи сведений индивидуального характера об отдельных учащихся.

В системе используется внутренний идентификационный номер (личный код) субъекта персональных данных, присваиваемый на весь период обучения или работы. Соответственно, даже при потенциальной возможности утечки данных из канала связи, полученная недобросовестным образом информация не будет иметь привязки к конкретному субъекту или владельцу персональных данных. Это стало возможным благодаря тому, что уже на сервере образовательного учреждения данные обезличиваются и в центральное хранилище передаются в обезличенном и зашифрованном виде.

Система КАИС КРО предполагает работу пользователей и операторов в рамках строго определенных ролей, при которой доступ к данным ограничен просмотром исключительно той части, которая содержит сведения, предусмотренные для соответствующей роли.

Данные о конкретном обучающемся (его оценки, результаты экзаменов и т. д.) поступают в систему только после поступления заявки от родителя или законного представителя о его желании получить доступ в систему. В случае нежелания родителя или законного представителя использовать систему, сведения по данному конкретному обучающемуся в системе отсутствуют.

Для предотвращения доступа к персональным данным лиц, не имеющих соответствующих прав, предоставление доступа для родителей или законных представителей учащихся предусматривает несколько этапов. Сначала

родитель или законный представитель проходит онлайн-регистрацию в системе и формирует бланк-заявление, а затем лично передает заявление Ответственному за работу с системой в образовательном учреждении. При этом подпись на заявлении сверяется с подписью на документе, удостоверяющем личность.

Такая процедура позволяет гарантировать, что доступ к сведениям о конкретном обучаемом получил именно его законный представитель. Если есть необходимость предоставить такой доступ другим родственникам и близким обучаемого, это может сделать только сам родитель или законный представитель – такая роль в системе предусмотрена под названием «Заинтересованное лицо». При этом по умолчанию такое «заинтересованное лицо» имеет меньше прав, чем родитель или законный представитель – в частности, не может вести переписку с учителями.

Естественно, доступ к данным для родителей и законных представителей ограничен сведениями только об одном конкретном обучаемом. Если у родителя (законного представителя) два или более детей, то для каждого из них требуется отдельная регистрация и отдельная заявка на доступ в систему.

Работа педагогов с персональными данными обучаемых также строго регламентирована. В системе имеются две роли – «Классный руководитель» и «Преподаватель». Соответственно, один и тот же сотрудник образовательного учреждения выступает для разных классов либо в одной, либо в другой роли и получает доступ, в частности, либо ко всем данным об успеваемости, либо к данным только по своему предмету.

ТЕХНОЛОГИЧЕСКИЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ РАЗРАБОТКЕ И ВНЕДРЕНИИ СИСТЕМЫ КАИС КРО И СЕРВИСЕ «ЭЛЕКТРОННЫЙ ДНЕВНИК»

Ядром системы является централизованное защищенное хранилище. Данные передаются по безопасным каналам связи единой мультисервисной телекоммуникационной сети органов государственной власти Санкт-Петербурга. Ввод данных на стороне образовательных учреждений осуществляется через существующие информационно-аналитические системы планирования, учета и контроля. Сервис доступен для всех участников образовательного процесса на портале «Петербургское образование».

Для предупреждения перехвата данных, а также для установления постоянного устойчивого соединения в контролируемой сети рекомендуется к использованию создание туннеля на основе протокола SSH v.2, предусматривающего шифрование данных при их передаче. Само шифрование

реализуется с использованием криптографического алгоритма с открытым ключом RSA с длиной 1024 бит.

Основные преимущества протокола SSH для реализации внедрения системы:

– кроссплатформенность, т. е. совместимость с любой операционной системой (ОС) из имеющихся сейчас на рынке;

– возможность передавать по шифрованному каналу различные виды данных, включая звуковой поток или видео, что особенно актуально для таких сервисов системы, как видеоконференции и видеоуроки;

– устойчивость к атакам путем присоединения посредине – невозможно включиться в или перехватить уже установленную сессию;

– реализация защищенного соединения без обязательного прохождения процедуры авторизации при каждой сессии (пользователь может сохранить исходный ключ и не прибегать каждый раз к введению логина и пароля);

– возможность ношения исходного ключа на сменном носителе, что делает защиту соединения еще более безопасной.

Данные преимущества протокола SSH позволяют сохранить баланс между конфиденциальностью и доступность данных в соответствии с международными рекомендациями ITIL v3 по обеспечению информационной безопасности, а также определениям защищенной системы по нормативным документам Федеральной службы по техническому и экспортному контролю.

Дополнительным средством обеспечения безопасности может служить система обнаружения вторжений (IDS), которая позволяет:

– создавать правила для выявления нецелевого трафика и быстро переносить их на любую альтернативную станцию;

– создавать отчеты и отправлять их на неограниченное количество электронных адресов;

– получать бесплатно обновления для немедленной реакции в случае появления более новых систем вторжения;

– организовать совместную работу системы с существующими средствами безопасности как в самой ОС, так и сторонними производителями файрволов и антивирусов.

ЗАКЛЮЧЕНИЕ

Уровень соответствия требованиям защиты персональных данных, заложенный при концептуальном проектировании и технической реализации КАИС КРО и сервиса «Электронный дневник», позволяет образовательным учреждениям как операторам системы полностью находиться в правовом поле.

В случае, если заложенные в системе механизмы будут дополнены высокой дисциплиной и ответственностью при ее повседневном использовании, конфиденциальность сведений об учащихся будет обеспечена с высокой степенью вероятности.

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

Методическое пособие

Редактор – Кутепова Е.Г.
Компьютерная верстка, дизайн обложки – Розова М.В.

Подписано в печать 18.10.2010. Формат 60x90 1/16
Гарнитура Times. Усл.печ.л. 4,25. Тираж 1000 экз. Зак. 29.

Издано в ГОУ ДПО ЦПКС СПб "Региональный центр оценки качества образования и информационных технологий"

190068, Санкт-Петербург, Вознесенский пр., 34, лит. А
Тел. (812) 576-34-50, 576-34-81

Отпечатано в типографии Тиражи.RU
127055, Москва, Приютский пер., д. 3. Тел. (495) 585-08-95.