ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ «ШКОЛА № 887»
(ГБОУ Школа № 887)

Рассмотрено	Согласовано	Утверждаю
Управляющий совет	Председатель ППО	Директор ГБОУ Школа №887
ГБОУ Школа № 887	_____ Н.Ю. Меньшенина	_____ Ю.В. Плотникова
Протокол № 5 от 27.04.2021г.	11.05.2021г.	Приказ от 11.05.2021г. № 989

ПОЛОЖЕНИЕ ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ

Москва, 2021

Содержание

1 Введение 4

2 Общие положения 6

3 Роли персонала 7

4 Обязательные мероприятия по обеспечению безопасности информационных систем персональных данных 8

4.1 Общие требования 8

5 Обеспечение технической защиты персональных данных 11

5.1 Общие требования 11

5.2 Контроль выполнения требований по защите персональных данных 15

5.3 Учет съемных электронных носителей персональных данных 15

6 Обязанности персонала 17

6.1 Обязанности ответственного за организацию обработки персональных данных 17

6.2 Обязанности ответственного за обеспечение безопасности персональных данных 19

7 Организация внутреннего контроля обработки и обеспечения безопасности персональных данных 21

7.1 Цели организации внутреннего контроля 21

7.2 Проведение контрольных мероприятий 22

7.3 Порядок проведения разбирательств 23

Приложение А Дополнения в договоры и должностные инструкции 26

А.1 Должностная инструкция ответственного за организацию обработки персональных данных 26

А.2 Дополнения в разделы договоров, в соответствии с которыми образовательная организация поручает обработку персональных данных третьим лицам 28

А.3 Дополнения в разделы трудовых договоров об обеспечении безопасности персональных данных 30

Приложение Б Формы согласия субъекта на обработку его персональных данных 32

Б.1 Типовая форма согласия субъекта на обработку его персональных данных 32

Б.2 Форма согласия работника на обработку персональных данных 32

Приложение В Форма уведомления субъектов персональных данных об обработке его персональных данных 39

Приложение Г Формы бланков учета 41

Г.1 Форма журнала учета средств защиты информации 41

Г.2 Форма журнала учета съемных носителей персональных данных 42

Приложение Д Форма акта об уничтожении персональных данных 43

Приложение Е Формы перечней 44

Е.1 Форма перечня лиц, допущенных к обработке персональных данных 44

Е.2 Форма перечня персональных данных, обрабатываемых в образовательной организации 45

Е.3 Форма перечня информационных систем персональных данных, используемых в образовательной организации 46

Приложение Ж Требования к вводу или выводу информационных систем из эксплуатации 47

Ж.1 Требования к разработке и вводу в эксплуатацию информационных систем персональных данных 47

Ж.2 Требования к выводу информационной системы персональных данных из эксплуатации 49

1 Введение

1.1 Настоящее положение разработано в соответствии с законодательством Российской Федерации о персональных данных и нормативно-методическими документами исполнительных органов государственной власти по вопросам безопасности персональных данных, в том числе при их обработке в информационных системах персональных данных.

1.2 Основными нормативно-правовыми и методическими документами, на которых базируется настоящее положение, являются:

– Федеральный закон Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки персональных данных, права, обязанности и ответственность участников отношений, связанных с обработкой персональных данных;

– Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении Требований к защите 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».

1.3 Для осуществления мероприятий по обеспечению и контролю безопасности персональных данных, обработки обращений субъектов персональных данных и взаимодействия с уполномоченным органом по защите прав субъектов персональных данных приказом директора Государственного бюджетного общеобразовательного учреждения города Москвы «Школа № 887» (далее – образовательная организация) назначается работник, ответственный за организацию обработки персональных данных, и работник, ответственный за обеспечение безопасности персональных данных.

1.4 Настоящее положение подлежит пересмотру и при необходимости актуализации в случае изменений в законодательстве Российской Федерации о персональных данных, при изменении организационной структуры образовательной организации.

2 Общие положения

2.1 Настоящее положение предназначено для организации в образовательной организации процесса обеспечения безопасности персональных данных согласно требованиям действующего федерального законодательства.

2.2 Действие настоящего положения распространяется на все процессы по сбору, систематизации, накоплению, хранению, уточнению, использованию, распространению (в том числе передаче), обезличиванию, блокированию, уничтожению персональных данных, осуществляемые с использованием средств автоматизации и без их использования.

2.3 Положение обязательно для ознакомления и исполнения работниками образовательной организации, являющимися ответственными за организацию обработки персональных данных и ответственными за обеспечение безопасности персональных данных, инженерами по телекоммуникации (техниками).

3 Роли персонала

3.1 Во исполнение положений настоящего документа и соответствия требованиям законодательства Российской Федерации о персональных данных в образовательной организации введены следующие роли персонала:

– ответственный за организацию обработки персональных данных;

– ответственный за обеспечение безопасности персональных данных.

3.2 Назначение работников на роли ответственного за организацию обработки персональных данных, ответственного за обеспечение безопасности персональных данных осуществляется приказом директора образовательной организации.

4 Обязательные мероприятия по обеспечению безопасности информационных систем персональных данных

4.1 Общие требования

4.1.1 В образовательной организации до начала проведения работ по обеспечению безопасности персональных данных должна быть проведена инвентаризация информационных систем персональных данных путем опроса владельцев информационных систем на предмет наличия обработки в них персональных данных.

4.1.2 После инвентаризации информационных систем выявляются информационные системы персональных данных, в которых осуществляется автоматизированная обработка персональных данных, и информационные системы персональных данных, в которых осуществляется неавтоматизированная обработка персональных данных.

4.1.3 Для всех эксплуатируемых информационных систем персональных данных с автоматизированной обработкой персональных данных должны быть определены уровни защищенности персональных данных в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных».

4.1.4 По согласованию с Департаментом образования и науки города Москвы в образовательных организациях могут использоваться собственные информационные системы персональных данных. Порядок ввода в эксплуатацию и вывода из эксплуатации таких информационных систем описаны в приложении (Приложение Ж).

4.1.5 В случае создания новых информационных систем персональных данных, расширения состава данных в существующих информационных системах персональных данных, модернизации информационных систем персональных данных определение уровня защищенности персональных

данных проводится в следующей последовательности:

1) На этапе создания информационных систем или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем) приказом директора образовательной организации создается комиссия по проведению определения уровней защищенности персональных данных в информационных системах персональных данных;

2) комиссия в определенный приказом срок устанавливает категории, принадлежность и объем обрабатываемых персональных данных в информационных системах персональных данных, а также определяет тип актуальных для информационных систем персональных данных угроз безопасности персональных данных, связанных с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении;

3) комиссия формирует акты определения уровней защищенности персональных данных для каждой информационной системы персональных данных, в которых указываются типы угроз безопасности персональных данных в информационных системах персональных данных, перечень обрабатываемых категорий персональных данных, их принадлежность и количество записей, содержащих персональных данных.

4.1.6 В образовательной организации должны быть разработаны модели угроз безопасности персональных данных для всех информационных систем персональных данных. Модель угроз разрабатывается на основе методических документов, утвержденных в соответствии с ч. 5 ст. 19 ФЗ «О персональных данных».

4.1.7 Выбор и реализация методов и способов защиты информации в информационных системах персональных данных осуществляются на основе модели угроз информационной безопасности и в зависимости от уровня защищенности персональных данных в информационных системах персональных данных.

4.1.8 Выбранные и реализованные методы и способы защиты персональных данных в информационных системах персональных данных должны обеспечивать нейтрализацию выявленных угроз безопасности персональных данных при их обработке в информационных системах персональных данных в составе системы защиты персональных данных.

4.1.9 Для проведения работ по выбору и реализации методов и способов защиты персональных данных (включая техническое проектирование системы защиты персональных данных, внедрение средств защиты персональных данных, сопровождение средств защиты персональных данных и т. д.) могут привлекаться подрядные организации, имеющие лицензию на осуществление деятельности по технической защите конфиденциальной информации.

4.1.10 Общие технические требования по защите персональных данных в информационных системах персональных данных образовательной организации приведены в разделе 5.

5 Обеспечение технической защиты персональных данных

5.1 Общие требования

5.1.1 Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных должно осуществляться на всех стадиях жизненного цикла информационных систем персональных данных и состоять из согласованных мероприятий, направленных на предотвращение (нейтрализацию) и устранение угроз безопасности персональных данных в информационных системах персональных данных, минимизацию возможного ущерба, а также мероприятий по восстановлению данных и нормального функционирования информационных систем персональных данных в случае реализации угроз.

5.1.2 В целях защиты персональных данных от несанкционированного доступа и иных неправомерных действий мероприятия по организации и техническому обеспечению безопасности персональных данных для каждой информационной системы персональных данных должны включать:

1) определение уровней защищенности персональных данных в информационной системе персональных данных на основании Постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденного;

2) выявление и закрытие технических каналов утечки персональных данных на основе анализа и актуализации модели угроз безопасности персональных данных;

3) выбор и реализацию организационных и технических методов и способов защиты информации в информационной системе в зависимости от уровня защищенности персональных данных в информационной системе персональных данных с учетом особенностей инфраструктуры и с учетом

актуальных угроз безопасности персональных данных в информационной системе персональных данных;

4) установку, настройку и применение соответствующих программных, аппаратных и программно-аппаратных средств защиты информации;

5) разработку дополнений к трудовым договорам (или должностным инструкциям) по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных для персонала, задействованного в эксплуатации данной информационной системе персональных данных (подразделы А.1 и А.2 Приложения А).

5.1.3 Предотвращение утечки персональных данных по техническим каналам за счет побочных электромагнитных излучений и наводок, а также за счет электроакустических преобразований реализуется в образовательной организации организационными мерами и не требует специальных технических решений.

5.1.4 Защита персональных данных при их обработке в информационной системе персональных данных от несанкционированного доступа и иных неправомерных действий должна осуществляться в образовательной организации следующими методами и способами:

– реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам (включая персональных данных), информационной системы персональных данных и связанным с ее использованием работам, документам (подраздел Е.1 Приложения Е);

– ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, содержащие персональных данных;

– разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам (включая персональных данных), программным средствам обработки (передачи) и защиты персональных данных;

– регистрация действий пользователей и обслуживающего персонала информационной системы персональных данных, мониторинг попыток несанкционированного доступа;

– учет и хранение съемных носителей информации с персональными данными и их обращение, исключающее хищение, подмену и уничтожение (подраздел 5.3);

– использование защищенных каналов связи, используемых для передачи персональных данных;

– размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах контролируемой территории;

– предотвращение внедрения в информационную систему персональных данных вредоносных программ (программ-вирусов) и программных закладок;

– регистрация событий и мониторинг процессов обработки информации;

– контроль целостности программных средств;

– регистрация запуска (остановки) программ обработки персональных данных;

– регистрация вывода персональных данных на печать.

5.1.5 При организации взаимодействия информационной системы персональных данных с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) наряду с указанными методами и способами должны применяться следующие дополнительные методы и способы защиты персональных данных от несанкционированного доступа:

– межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы персональных данных;

– защита персональных данных при их передаче по каналам связи;

– использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;

– использование средств антивирусной защиты.

5.1.6 Должна производиться периодическая проверка электронных журналов безопасности, в которых регистрируются события безопасности. К электронным журналам безопасности относятся:

– журналы безопасности операционных систем;

– журналы событий системы управления базами данных;

– журналы событий средств защиты информации;

– журналы событий системы контроля и управления физическим доступом;

– журналы событий прикладного программного обеспечения;

– журналы активных сетевых устройств.

5.1.7 К событиям безопасности в информационной системе персональных данных относятся следующие события:

– доступ (входа и выхода в систему и доступа к объектам, в том числе неудачные попытки доступа);

– создание и удаление пользователей;

– изменение прав доступа и привилегий;

– подключение и отключение внешних устройств;

– изменение настроек средств защиты;

– события, генерируемые средствами защиты.

5.1.8 В образовательной организации также могут разрабатываться и применяться другие методы защиты информации от несанкционированного доступа, обеспечивающие нейтрализацию угроз безопасности персональных данных.

5.1.9 Конкретные методы и средства защиты персональных данных в информационной системе персональных данных должны определяться на основании нормативно-методических документов ФСТЭК России и ФСБ России, исходя из уровней защищенности персональных данных в информационной системе персональных данных и актуальных угроз безопасности персональных данных.

5.1.10 Все технические средства защиты информации должны быть снабжены инструкциями по эксплуатации.

5.1.11 Должен вестись учет технических средств защиты информации, эксплуатационной и технической документации к ним. Форма журнала учета технических средств защиты информации приведена в приложении (подраздел Г.1 Приложения Г).

5.1.12 Ответственность за ведение и поддержание в актуальном состоянии журнала учета технических средств защиты информации возлагается на ответственного за обеспечение безопасности персональных данных.

5.2 Контроль выполнения требований по защите персональных данных

5.2.1 В соответствии с документом «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденным Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119, должен проводиться периодический контроль выполнения требований по обеспечению безопасности персональных данных (не реже одного раза в три года).

5.2.2 Контроль функций системы защиты производится в рамках мероприятий, описанных в подразделе 7.2 настоящего положения.

5.2.3 Ответственность за контроль функций системы защиты персональных данных возлагается на ответственного за обеспечение безопасности персональных данных.

5.3 Учет съемных электронных носителей персональных данных

5.3.1 В образовательной организации должен вестись учет защищаемых съемных носителей персональных данных. К защищаемым носителям персональных данных относятся следующие:

– носители информации серверов;

– носители информации автоматизированного рабочего места;

– внешние запоминающие устройства (флеш-накопители, карты памяти и т. п.), содержащие персональные данные.

5.3.2 Форма журнала учета защищаемых съемных электронных носителей приведена в приложении (подраздел Г.2 Приложения Г).

5.3.3 Ответственность за учет защищаемых электронных носителей персональных данных возлагается на ответственного за обеспечение безопасности персональных данных.

6 Обязанности персонала

Должностные инструкции ответственного за организацию обработки персональных данных и ответственного за обеспечение безопасности персональных данных расширены с учетом специфики обработки и защиты персональных данных (подразделы А.1 и А.2 Приложения А). Работники, назначаемые на данные роли, ознакомляются под подпись со своими должностными инструкциями.

6.1 Обязанности ответственного за организацию обработки персональных данных

6.1.1 В обязанности ответственного за организацию обработки персональных данных входит:

– осуществление внутреннего контроля за соблюдением образовательная организациям и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– доведение до сведения работников образовательной организации положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

– прием и обработка обращений субъектов персональных данных и их законных представителей (ведение журнала учета обращений субъектов персональных данных, анализ правомерности запросов, составление и отправка ответов);

– прием и обработка запросов уполномоченного органа по защите прав субъектов персональных данных (ведение журнала учета запросов уполномоченного органа по защите прав субъектов персональных данных, анализ правомерности запросов, составление и отправка ответов);

– ведение и хранение журнала учета проверок уполномоченным органом по защите прав субъектов персональных данных;

– уведомление уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных, об изменениях в реквизитах оператора персональных данных;

– уведомление уполномоченного органа по защите прав субъектов персональных данных по запросу этого органа с предоставлением необходимой информации в течение тридцати дней[1] с даты получения такого запроса.

6.1.2 Ответственный за организацию обработки персональных данных обладает следующими полномочиями:

– запрашивать необходимую информацию у руководства и работников образовательной организации, относящуюся к обработке персональных данных и необходимую для выполнения его обязанностей;

– контролировать выполнение обязанностей ответственным за обеспечение безопасности персональных данных, инженерами по телекоммуникации (техниками), а также выполнение требований законодательства и внутренних нормативных документов образовательной организации, регламентирующих обработку и обеспечение безопасности персональных данных;

– назначать ответственного за уничтожение персональных данных и контролировать выполнение процедуры уничтожения персональных данных. Для выполнения уничтожения персональных данных на бумажном носителе в качестве лица, ответственного за уничтожение персональных данных, назначается владелец бизнес-процесса, в случае с другими носителями персональных данных или если обработка персональных данных осуществляется в информационной системе персональных данных, в качестве лица, ответственного за уничтожение персональных данных, назначается владелец информационной системы персональных данных;

– согласовывать заявки временного или разового допуска работника к работе с персональными данными в связи со служебной необходимостью.

[1] Ст. 20 ч. 4 ФЗ «О персональных данных»

6.2 Обязанности ответственного за обеспечение безопасности персональных данных

6.2.1 В обязанности ответственного за обеспечение безопасности персональных данных входит:

– предоставление и прекращение доступа пользователей к персональным данным в информационных системах персональных данных в соответствии с утвержденным перечнем должностей работников, допущенных к работе с персональными данными, или с утвержденными заявками на доступ к персональным данным;

– управление учетными записями пользователей комплекса информационных систем персональных данных совместно с инженерами по телекоммуникации (техниками);

– проведение контрольных мероприятий (см. подраздел 5.2);

– предоставление сведений о персональных данных ответственному за организацию обработки персональных данных в рамках проведения учета защищаемых носителей и проведения инвентаризации (см. подраздел 5.3);

– установка, конфигурирование и администрирование аппаратных и программных средств защиты информации комплекса информационных систем персональных данных;

– поддержание штатной работы комплекса информационных систем персональных данных совместно с инженерами по телекоммуникации (техниками);

– учет защищаемых носителей персональных данных (см. подраздел 5.3);

– учет технических средств защиты информации (см. пункт 5.1.11 подраздела 5.1);

– периодические ежемесячные[2] проверки журналов безопасности (см. пункт 5.1.6 подраздела 5.1);

– анализ защищенности информационных систем персональных данных;

[2] Периодичность проверки зависит от срока хранения информации в журналах безопасности, например, если информация в журнале безопасности хранится одну неделю, то проверки необходимо проводить еженедельно

– организация процесса обучения работников по направлению обеспечения безопасности персональных данных;

– участие в проведении внутреннего контроля и служебных расследований фактов нарушения установленного порядка обработки и обеспечения безопасности персональных данных (см. подразделы 7.2 и 7.3).

6.2.2 Ответственный за обеспечение безопасности персональных данных обладает следующими полномочиями:

– проводит плановые и внеплановые контрольные мероприятия в целях контроля, изучения и оценки фактического состояния защищенности персональных данных;

– запрашивает необходимую информацию у очевидцев и подозреваемых лиц при проведении разбирательств по фактам нарушения установленного порядка обработки и обеспечения безопасности персональных данных.

7 Организация внутреннего контроля обработки и обеспечения безопасности персональных данных

7.1 Цели организации внутреннего контроля

7.1.1 Организация внутреннего контроля процесса обработки персональных данных в образовательной организации осуществляется в целях изучения и оценки фактического состояния защищенности персональных данных, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

7.1.2 Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности персональных данных направлены на решение следующих задач:

- обеспечение соблюдения работниками образовательной организации требований настоящего положения и нормативных правовых актов, регулирующих защиту персональных данных;
- оценка компетентности персонала, задействованного в обработке персональных данных;
- обеспечение работоспособности и эффективности технических средств информационных систем персональных данных и средств защиты персональных данных, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности персональных данных;
- выявление нарушений установленного порядка обработки персональных данных и своевременное предотвращение негативных последствий таких нарушений;
- принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки персональных данных, так и в работе технических средств информационных систем персональных данных;

– разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности персональных данных по результатам контрольных мероприятий;

– осуществление контроля исполнения рекомендаций и указаний по устранению нарушений.

7.2 Проведение контрольных мероприятий

7.2.1 Контрольные мероприятия (проверки) проводятся на плановой основе, а также при необходимости внепланово.

7.2.2 Решение о необходимости проведения внеплановых контрольных мероприятий принимает ответственный за обеспечение безопасности персональных данных. Данное решение должно быть обосновано возросшими рисками информационной безопасности для обрабатываемых персональных данных и при существенных изменениях в среде обработки персональных данных.

7.2.3 Контрольные мероприятия (проверки) организуются ответственным за обеспечение безопасности персональных данных.

7.2.4 Плановые проверки проводятся не реже одного раза в полугодие и включают в себя:

– проверку деятельности работников образовательной организации, допущенных к работе с персональными данными в информационных системах персональных данных, на соответствие порядку обработки и обеспечения безопасности персональных данных, установленному положением по работе с персональными данными и другими нормативными правовыми актами, принятыми в образовательной организации и обязательными для ознакомления и исполнения соответствующими категориями работников;

– проверку работоспособности и эффективности технических средств информационных систем персональных данных и средств защиты персональных данных;

– проверку ведения эталонных копий средств защиты;

– проверку соответствия предоставленных прав доступа пользователей к персональным данным утвержденной матрице доступа;

– проверку минимальной длины и сложности паролей;

– проверку периодичности смены паролей;

– проверку отсутствия на автоматизированных рабочих местах пользователей средств разработки;

– проверку отсутствия на автоматизированных рабочих местах пользователей нештатного программного обеспечения;

– мониторинг журналов протоколирования событий аутентификации.

7.2.5 Ответственный за обеспечение безопасности персональных данных составляет план контрольных мероприятий на полугодие, в котором определяет состав и периодичность проведения проверок на данный период времени.

7.2.6 Результаты проверок оформляются актами. Выявленные в ходе проверок нарушения, а также отметки об их устранении фиксируются в журнале учета выявленных нарушений в порядке обработки и обеспечения безопасности персональных данных.

7.2.7 Выявленные нарушения расследуются в соответствии с подразделом 7.3.

7.2.8 При необходимости должны быть предложены меры по минимизации последствий выявленных угроз информационной безопасности.

7.2.9 В случае передачи части функций в области информационных технологий сторонним организациям указанные контрольные мероприятия осуществляют эти сторонние организации. Требования по осуществлению контрольных мероприятий указываются в договорах с этими сторонними компаниями.

7.3 Порядок проведения разбирательств

7.3.1 Проведение разбирательств может быть инициировано в одном из следующих случаев:

– обращение субъекта персональных данных по поводу неправомерных действий с его персональных данных;

– выявление нарушений работниками образовательной организации в рамках выполнения своих должностных обязанностей, связанных с обработкой или защитой персональных данных;

– выявление нарушений, приводящих к снижению уровня защищенности персональных данных, в ходе проведения проверок состояния защищенности персональных данных.

7.3.2 В ходе проведения расследования ответственным за обеспечение безопасности персональных данных проводится опрос очевидцев и подозреваемых лиц, предположительно допустивших нарушение.

7.3.3 В ходе проведения опроса выясняется:

– дата и время совершения нарушения;

– обстоятельства, при которых были совершены действия, приведшие к возникновению нарушения;

– последствия, возникшие вследствие совершения нарушения.

7.3.4 Все опрашиваемые лица должны предоставить объяснительные записки (показания, изложенные на бумажном носителе с подписью опрашиваемого).

7.3.5 Ответственный за обеспечение безопасности персональных данных оценивает последствия, возникшие вследствие совершения нарушения.

7.3.6 По результатам разбирательства ответственный за обеспечение безопасности персональных данных в течение трех рабочих дней составляет заключение по результатам разбирательств.

7.3.7 В заключении должны быть приведены:

– краткая справка по нарушению, в отношении которого проводилось разбирательство;

– лицо(а), которое совершило(и) нарушение;

– предложения по привлечению виновника к юридической ответственности (дисциплинарной ответственности: замечание, выговор,

увольнение; или к гражданско-правовой ответственности (взыскание причиненного ущерба) и/или применении к нему мер дисциплинарного воздействия (депремирование, указание на недостатки и т. п.);

– план мероприятий по предотвращению подобных нарушений в будущем (если уместно).

7.3.8 Заключение предоставляется ответственному за организацию обработки персональных данных и согласовывается с директором образовательной организации.

7.3.9 Срок проведения расследования не должен превышать семи рабочих дней.

Приложение А
Дополнения в договоры и должностные инструкции

А.1 Должностная инструкция ответственного за организацию обработки персональных данных

Назначение работника на должность ответственного за организацию обработки персональных данных осуществляется приказом директора образовательной организации.

Ответственный за организацию обработки персональных данных подчиняется непосредственно директору образовательной организации.

В своей деятельности ответственный за организацию обработки персональных данных руководствуется:

– действующими нормами международного права и законодательством Российской Федерации;

– уставом образовательной организации;

– организационно-распорядительными документами образовательной организации по вопросам организации обработки и обеспечения безопасности персональных данных;

– приказами, распоряжениями директора образовательной организации;

– настоящей должностной инструкцией.

На время отсутствия ответственного за организацию обработки персональных данных его обязанности исполняет директор образовательной организации.

Основными задачами ответственного за организацию обработки персональных данных являются:

– осуществление внутреннего контроля за соблюдением образовательной организацией и ее работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

– доведение до сведения работников образовательной организации положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

– прием и обработка обращений субъектов персональных данных и их законных представителей (ведение журнала учета обращений субъектов персональных данных, анализ правомерности запросов, составление и отправка ответов);

– прием и обработка запросов уполномоченного органа по защите прав субъектов персональных данных (ведение журнала учета запросов уполномоченного органа по защите прав субъектов персональных данных, анализ правомерности запросов, составление и отправка ответов);

– ведение и хранение журнала учета проверок уполномоченным органом по защите прав субъектов персональных данных;

– уведомление уполномоченного органа по защите прав субъектов персональных данных об обработке персональных данных, об изменениях в реквизитах оператора персональных данных;

– уведомление уполномоченного органа по защите прав субъектов персональных данных по запросу этого органа с предоставлением необходимой информации.

Ответственный за организацию обработки персональных данных вправе:

– запрашивать необходимую информацию у руководства и работников образовательной организации, относящуюся к обработке персональных данных и необходимую для выполнения его обязанностей;

– контролировать выполнение обязанностей ответственным за обеспечение безопасности персональных данных, а также выполнение требований законодательства и внутренних нормативных документов образовательной организации, регламентирующих обработку и обеспечение безопасности персональных данных;

– назначать ответственного за уничтожение персональных данных и контролировать выполнение процедуры уничтожения персональных данных;

– согласовывать заявки временного или разового допуска работника к работе с персональными данными в связи со служебной необходимостью.

А.2 Дополнения в разделы договоров, в соответствии с которыми образовательная организация поручает обработку персональных данных третьим лицам

ТЕРМИНЫ

В настоящем договоре используются следующие термины, если иное не следует из контекста:

«Персональные данные» означают любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

«Обработка персональных данных» (обработка) означает любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

«Субдоговор» и «заключение субдоговора» означает процесс, когда стороны договариваются с третьей стороной о выполнении обязательств в соответствии с настоящим Договором, а «субконтрактор» означает сторону, с которой заключен «субдоговор».

«Технические и организационные меры обеспечения безопасности» означают меры, предпринимаемые для обеспечения безопасности персональных данных от случайного или незаконного уничтожения, или случайной утраты, неавторизованной модификации, неправомерного раскрытия или доступа, а также от всех иных незаконных форм обработки.

РАЗДЕЛ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Обязанности, связанные с безопасностью

1) Обработчик обязан совершать какие-либо свои действия в отношении персональных данных, которые он обрабатывает от имени оператора, исключительно в соответствии с указаниями оператора.

2) Обработчик обязан принимать надлежащие технические и организационные меры по обеспечению безопасности персональных данных в соответствии с требованиями законодательства Российской Федерации в области персональных данных.

Конфиденциальность

1) Обработчик соглашается с тем, что он обязан обрабатывать персональные данные от имени оператора, соблюдая конфиденциальность обработки. В частности, обработчик соглашается с тем, что, если он не получил письменного согласия от оператора, он не будет раскрывать персональные данные, переданные обработчику оператором/для оператора/от имени оператора третьим лицам.

2) Обработчик не должен использовать персональные данные, переданные ему оператором, кроме как в соответствии с существом услуг, оказываемых им оператору.

Заключение «субдоговора»

1) Обработчик не должен заключать «субдоговор» по исполнению своих обязательств, налагаемых настоящим договором, без предварительного письменного согласия оператора.

2) В том случае если обработчик с согласия оператора заключает «субдоговор», он обязан заключать этот договор в письменной форме, а сам договор должен содержать все те обязательства в отношении безопасности обработки, которые накладываются на обработчика в соответствии с настоящим договором.

3) Если «субконтрактор» не в состоянии выполнять свои обязательства, вытекающие из «субдоговора», обработчик несет полную ответственность перед

оператором за выполнение обязательств, накладываемых на него настоящим договором.

Порядок действий с персональными данными после прекращения действия договора

В течение 5[3] дней со дня окончания действия настоящего договора обработчик обязан по указанию оператора:

– вернуть все персональные данные, переданные для обработки обработчику оператором, или

– по указанию оператора уничтожить все персональные данные, если это не запрещено законодательством, или

– выполнить все дополнительные соглашения между сторонами в части возвращения или уничтожения данных.

А.3 Дополнения в разделы трудовых договоров об обеспечении безопасности персональных данных

В раздел трудовых договоров (должностных инструкций) персонала информационных, закрепляющий должностные обязанности, необходимо включить следующий пункт:

1) При работе с информационными системами персональных данных следует руководствоваться требованиями к порядку обработки и обеспечения безопасности персональных данных, закрепленными в положении по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных образовательной организации.

В раздел «Ответственность» трудовых договоров (должностных инструкций) работников образовательной организации, допущенных к обработке персональных данных для выполнения своих должностных обязанностей, необходимо включить следующие пункты:

1) работник образовательной организации несет ответственность за обеспечение конфиденциальности персональных данных, ставших ему известными в связи с выполнением должностных обязанностей;

[3] Максимальный срок для прекращения обработки – 30 дней (ч. 4 ст. 21), но следует учитывать, что Обработчик должен завершить обработку раньше, чем Оператор, чтобы Оператор также успел завершить обработку в течение 30 дней

2) работник образовательной организации несет персональную ответственность за соблюдение требований по обработке и обеспечению безопасности персональных данных, установленных в положении по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных образовательной организации;

3) в случае нарушения установленного порядка обработки и обеспечения безопасности персональных данных, несанкционированного доступа к персональным данным, раскрытия персональных данных и нанесения образовательной организации, его работникам или клиентам материального, или иного ущерба виновные лица несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение Б
Формы согласия субъекта на обработку его персональных данных

Б.1 Типовая форма согласия родителей (законных представителей) обучающихся на обработку персональных данных

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____(*ФИО*), проживающий по адресу _____, паспорт серия_____ № _____ выдан (*кем и когда*) _____, тел.:_____, адрес электронной почты:_____ являюсь законным представителем несовершеннолетнего _____ (ФИО) на основании ст. 64 п. 1 Семейного кодекса РФ[4].

Настоящим даю свое согласие на обработку в ГБОУ Школа № 887 персональных данных моего несовершеннолетнего ребенка (подопечного) _____ _____, относящихся **исключительно** к перечисленным ниже категориям персональных данных:

–**данные свидетельства о рождении/данные документа, удостоверяющего личность:** ФИО; пол; дата рождения; тип, серия, номер документа, удостоверяющего личность; гражданство.

–**медицинские сведения:** данные медицинской карты; сведения о состоянии здоровья; отнесение к категории лиц с ОВЗ, детей-инвалидов; сведения о прохождении медосмотров; сведения об освоении адаптированной образовательной программы; сведения о наличии заключения ЦПМПК;

–**СНИЛС;**

–**адрес проживания/пребывания ребенка**;

–**номер телефона и адрес электронной почты**;

–**учебные достижения ребенка:** сведения об успеваемости; учебные работы ребенка; форма обучения, номер класса (группы), наличие/отсутствие льгот, данные о получаемом дополнительном образовании, форма ГИА, наличие допуска и перечень предметов, выбранных

[4] Для родителей. Для усыновителей «ст. ст. 64 п. 1, 137 п. 1 Семейного Кодекса РФ», опекуны – «ст. 15 п. 2 Федерального закона «Об опеке и попечительстве», попечители – «ст. 15 п. 3. Федерального закона «Об опеке и попечительстве».

для сдачи ГИА, место сдачи ГИА, результаты ГИА (в том числе итогового сочинения, изложения), содержание поданной апелляции и результаты ее рассмотрения;

–**фото- и видео- изображение.**

Также даю согласие на обработку следующих моих персональных данных:

- **ФИО, фотоизображения** (при использования информационной системы проход и питание (ИСПП).

Я даю согласие на использование персональных данных моего ребенка **исключительно** в следующих целях:

- обеспечения защиты конституционных прав и свобод моего ребенка;

- обеспечения соблюдения нормативных правовых актов Российской Федерации и города Москвы;

- обеспечения безопасности обучающихся в период нахождения на территории образовательной организации;

- обеспечения организации учебного процесса для ребенка, в том числе актуализация оценок успеваемости в электронном дневнике;

- обеспечения организации внеурочной деятельности, экскурсий, олимпиад и спортивных соревнований, и иных знаковых мероприятий;

- ведения статистики;

- размещения фотоизображения на официальном сайте ГБОУ Школа № 887, Московском образовательном Интернет-телеканале и социальных сетях в рамках образовательного процесса, внеурочной деятельности, экскурсий, олимпиад и спортивных соревнований, и иных знаковых мероприятий на территории образовательной организации;

- видеосъемки и размещения видеоматериалов на официальном сайте ГБОУ Школа № 887, Московском образовательном Интернет-телеканале и социальных сетях в рамках внеурочной деятельности, экскурсий, олимпиад, спортивных соревнований, и иных знаковых мероприятий на территории образовательной организации;

- видеосъемки и размещения видеоматериалов на официальном сайте ГБОУ Школа № 887 и социальных сетях в рамках образовательного процесса *(в случае размещения видеонаблюдения в группах (классах) – в целях предоставления услуг видеонаблюдения родителям (законным представителям) обучающихся);*

- размещения на официальном сайте информации об успехах и достижениях обучающихся;

- передачи сведений в федеральные и региональные информационные системы в целях обеспечения проведения процедур оценки качества образования – независимых диагностик, мониторинговых исследований, государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования (в соответствии с правилами, утвержденными постановлением Правительства Российской

Федерации от 31 августа 2013 г. № 755), ведения федерального реестра сведений документов об образовании и(или) квалификации, документов об обучении (в соответствии с Постановление Правительства Российской Федерации от 26 августа 2013 года № 729);

- работы с подсистемами КИС ГУСОЭВ;
- контроля за посещением занятий;
- предоставления информации для оформления проездных документов.

Настоящее согласие предоставляется на осуществление сотрудниками ГБОУ Школа № 887 следующих действий в отношении персональных данных ребенка: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование (только в указанных выше целях), обезличивание, блокирование (не включает возможность ограничения моего доступа к персональным данным ребенка), а также осуществление любых иных действий, предусмотренных действующим законодательством Российской Федерации.

Я не даю согласия на какое-либо распространение персональных данных ребенка, в том числе на передачу персональных данных ребенка каким-либо третьим лицам, включая физических и юридических лиц, государственных органов и органов местного самоуправления, за исключением передачи персональных данных следующим организациям:

- Департаменту образования и науки города Москвы, в том числе подведомственным ему организациям;
- Департаменту информационных технологий города Москвы, в том числе подведомственным ему организациям;
- Федеральной службе по надзору в сфере образования и науки, в том числе подведомственным ему организациям.

Обработка персональных данных должна осуществляться с соблюдением требований, установленных законодательством Российской Федерации и только для целей, указанных выше. ГБОУ Школа № 887 обязана осуществлять защиту персональных данных ребенка, принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении данной информации.

Обработка персональных данных моего ребенка для любых иных целей и любым иным способом, включая распространение и передачу их иным лицам или иное их разглашение может осуществляться только с моего особого письменного согласия в каждом отдельном случае.

Защита внесенной информации осуществляется с соблюдением требований, установленных законодательством Российской Федерации. Хранение и обработка информации, а также обмен информацией осуществляются после принятия необходимых мер по защите указанной информации. В случае нарушения требований Федерального закона от 27.07.2006 №

152-ФЗ «О персональных данных» ГБОУ Школа № 887 несет ответственность, предусмотренную Кодексом об административных правонарушениях РФ, Трудовым кодексом РФ, Уголовным кодексом РФ.

Данное согласие действует до достижения целей обработки персональных данных в ГБОУ Школа № 887 или до истечения срока хранения информации данного согласия. Данное согласие может быть отозвано в любой момент по моему письменному заявлению.

Мне разъяснено, что отзыв настоящего согласия может затруднить или сделать невозможным возобновление обработки персональных данных и их подтверждение.

Я подтверждаю, что, давая настоящее согласие, я действую по своей воле и в интересах ребенка, законным представителем которого я являюсь.

Дата: __.__._____ г.

Подпись: _____ (_____)

Б.2 Форма согласия работника на обработку персональных данных

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я,_____ _____, *(фамилия, имя, отчество полностью)*, зарегистрированного по адресу_____, паспорт серия_____№_____, выдан *(кем)* _____*(когда)* даю свое согласие на обработку своих персональных данных в целях:

- обеспечения защиты моих конституционных прав и свобод;
- обеспечения соблюдения законов и иных нормативных правовых актов;
- заключения и регулирования трудовых отношений и иных непосредственно связанных с ними отношений;
- отражения информации в кадровых документах;
- начисления заработной платы;
- предоставления льгот, предусмотренных трудовым и налоговым законодательством;
- исчисления и уплаты, предусмотренных законодательством РФ налогов, сборов и взносов на обязательное социальное и пенсионное страхование;
- представления работодателем установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд РФ, сведений подоходного налога в ФНС России, сведений в ФСС РФ;

- перечисления заработной платы;

- оформления полиса ДМС;

- предоставления налоговых вычетов;

- обеспечения моей безопасности;

- оперативного доведения до меня информации со стороны ГБОУ Школа № 887;

- контроля количества и оценки качества выполняемой мной работы;

- размещения фото и видеоизображений на официальном сайте ГБОУ Школа № 887 для освещения образовательного процесса, внеурочной деятельности, экскурсий, олимпиад и спортивных соревнований, и иных знаковых мероприятий;

- передачи сведений в федеральные и региональные информационные системы в целях обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования (в соответствии с правилами, утвержденными Постановлением Правительства Российской Федерации от 31 августа 2013 г. № 755).

Перечень моих персональных данных, на обработку которых я даю согласие:

- фамилия, имя, отчество;

- пол, возраст;

- дата и место рождения, гражданство;

- паспортные данные (серия, номер, кем и когда выдан);

- фото-, видео- изображения;

- сведения о социальных льготах, о состоянии здоровья, о результатах медицинских осмотров и о профилактических прививках;

- сведения о временной нетрудоспособности, о характере полученных травм на работе;

- наличие (отсутствие) судимости и (или) факта уголовного преследования;

- сведения об условиях труда на рабочем месте;

- адрес регистрации по месту жительства и адрес фактического проживания;

- номер телефона (домашний, мобильный) и адрес электронной почты;

- сведения об образовании (квалификация, профессиональная подготовка, повышение квалификации);

- результаты прохождения аттестации;

- семейное положение, состав семьи;

- отношение к воинской обязанности;

- сведения о трудовом стаже, наличие наград, поощрений и почетных званий, предыдущих местах работы, доходах с предыдущих мест работы;

- должность;

- размер заработной платы;

- сведения об открытых банковских счетах, на которые перечисляется заработная плата в ГБОУ Школа № 887;

- сведения о налоговых отчислениях и сборах;

- номер СНИЛС;

- ИНН;

- информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в ГБОУ Школа № 887;

- сведения о доходах в ГБОУ Школа № 887;

- опыт в проведении ГИА в предыдущие годы

- сведения о деловых и иных личных качествах, носящих оценочный характер.

Я не даю согласия на какое-либо распространение моих персональных данных и их передачу третьим лицам, включая физических и юридических лиц государственных органов и органов местного самоуправления, за исключением передачи персональных данных следующим организациям:

- Департамент образования и науки города Москвы, в том числе подведомственные ему организации;

- Департамент информационных технологий города Москвы, в том числе подведомственные ему организации;

- Федеральная служба по надзору в сфере образования и науки, в том числе в том числе подведомственные ему организации;

- Федеральная служба по труду и занятости;

- Пенсионный фонд России;

- Федеральная налоговая служба России;

- Фонд социального страхования России;

- Московская городская организация Профсоюза работников народного образования и науки РФ.

Обработка персональных данных должна осуществляться с соблюдением требований, установленных законодательством Российской Федерации и только для целей, указанных выше. ГБОУ Школа № 887 обязано осуществлять защиту моих персональных данных, принимать необходимые организационные и технические меры для защиты моих персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, обезличивание, а также от иных неправомерных действий в отношении данной информации.

Обработка моих персональных данных для любых иных целей и любым иным способом, включая распространение и передачу их иным лицам, или иное их разглашение может осуществляться только с моего письменного согласия в каждом отдельном случае.

Защита внесенной информации должна осуществляться с соблюдением требований, установленных законодательством Российской Федерации. Хранение и обработка информации, а также обмен информацией должны осуществляться после принятия необходимых мер по защите указанной информации. В случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» ГБОУ Школа № 887 должна нести ответственность, предусмотренную Кодексом об административных правонарушениях РФ, Трудовым кодексом РФ, Уголовным кодексом РФ.

Данное согласие действует до достижения целей обработки персональных данных в ГБОУ Школа № 887 или в течение срока хранения информации. Данное согласие может быть отозвано в любой момент по моему письменному заявлению в его части или полном объеме.

Я подтверждаю, что, давая настоящее согласие, я действую по своей воле и в своих интересах.

Дата: __.__._____ г.

Подпись: _____ (_____)

Приложение В
Форма уведомления субъектов персональных данных об обработке его персональных данных

Субъекту персональных данных:
(Ф.И.О.)

Адрес:

УВЕДОМЛЕНИЕ
об обработке персональных данных

Оператор персональных данных: Государственное бюджетное общеобразовательное учреждение города Москвы «Школа № 887»,
находящийся по адресу: _____,
руководствуясь _____
(правовое основание обработки персональных данных)

с целью _____
(цель обработки персональных данных)

осуществляет обработку ваших персональных данных, включая:

_____

_____
(перечисление персональных данных, находящихся в обработке: Ф.И.О., адрес, телефон…)

полученных _____
(источник получения персональных данных)

Обработка вышеуказанных персональных данных осуществляется путем:

_____
(перечень действий с персональными данными,

_____
общее описание используемых оператором способов обработки персональных данных)

К персональным данным имеют или могут получить доступ следующие лица:

_____

_____
(перечень конкретных лиц или должностей)

Обработка указанных персональных данных будет являться основанием для

_____
(решения, принимаемые на основании обработки; возможные юридические последствия обработки)

Дата начала обработки персональных данных: _____

Срок или условие прекращения обработки персональных данных:

_____

_____

_____ _____ _____
(должность) (подпись) (Ф.И.О.)

«__» _____ 202_ г.

Приложение Г
Формы бланков учета

Г.1 Форма журнала учета средств защиты информации

Журнал учета средств защиты информации

№ п/п	Тип средства	Наименование средства защиты информации	Индекс или условное наименование* (для сертифицированных средств)	Регистрационный номер* (для сертифицированных средств)	Информационные системы, в которой(ых) применяется средства	Наличие и место хранения документации
1						
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						

* Перечень индексов, условных наименований и регистрационных номеров определяется ФСТЭК России и ФСБ России в пределах их полномочий

Г.2 Форма журнала учета съемных носителей персональных данных

Журнал учета съемных носителей персональных данных

№ п/п	Тип носителя	Наименование модели	Инвентарный номер	Владелец информации	Ответственное лицо	Дата поступления носителя
1						
2						
3						
4						
5						
6						

Приложение Д
Форма акта об уничтожении персональных данных

УТВЕРЖДАЮ

_____

«_____»_____201_ г.

Акт №_____

об уничтожении персональных данных

№ п/п	Дата	Место и форма хранения персональных данных	Тип носителя персональных данных и его регистрационный номер/уничтожаемые персональные данные

Всего уничтожено носителей (прописью): _____.

Уничтожение произведено путем _____

_____

_____.

Ответственный за уничтожение (Ф.И.О., должность):

_____.

Дата: _____.

Подпись: _____.

Приложение Е
Формы перечней

Е.1 Форма перечня лиц, допущенных к обработке персональных данных

Перечень должностей работников, допущенных к работе с персональными данными

№ п/п	Вид персональных данных (из перечня)	Должность	Цель доступа	Права доступа	Срок доступа	Примечание

Е.2 Форма перечня персональных данных, обрабатываемых в образовательной организации

Перечень персональных данных, обрабатываемых в образовательной организации

Категории субъектов персональных данных	Перечень персональных данных	Места и способы обработки персональных данных	Срок обработки персональных данных	Условия прекращения обработки персональных данных

Е.3 Форма перечня информационных систем персональных данных, используемых в образовательной организации

Перечень информационных систем персональных данных, используемых в образовательной организации

№ п/п	Наименование информационной системы	Владелец системы	Уровень защищенности персональных данных в системе

Приложение Ж
Требования к вводу или выводу информационных систем из эксплуатации

По согласованию с Департаментом образования и науки города Москвы в образовательных организациях могут использоваться собственные информационные системы персональных данных, требования по вводу в эксплуатацию и/или выводу из эксплуатации которых описаны ниже.

Ж.1 Требования к разработке и вводу в эксплуатацию информационных систем персональных данных

Ж.1.1 Разработка информационной системы персональных данных должна включать следующие стадии:

а) предпроектная стадия (включает предварительный анализ целей и условий функционирования информационной системы персональных данных, а также обрабатываемых в ней персональных данных, на основании которого определяется предварительный класс информационной системы персональных данных, степень участия должностных лиц, актуализируются угрозы безопасности);

б) стадия проектирования системы защиты персональных данных для информационной системы персональных данных;

в) стадия ввода в действие информационной системы персональных данных.

Ж.1.2 По результатам проведенного анализа и с учетом действующих требований законодательства Российской Федерации о персональных данных и регуляторов должны быть разработаны:

- модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных;
- акт об установлении уровня защищенности персональных данных в информационной системе персональных данных;
- требования к защите персональных данных при их обработке в информационной системе персональных данных;

– частное техническое задание на создание системы защиты персональных данных для информационной системы персональных данных.

Ж.1.3 При определении отсутствия недекларированных возможностей в системном и/или прикладном программном обеспечении выполняются следующие мероприятия для подтверждения типа угроз безопасности персональных данных в информационной системе персональных данных:

– проверка системного и/или прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и/или без использования таковых;

– тестирование информационной системы на проникновения;

– использование в информационной системе системного и/или прикладного программного обеспечения, разработанного с использованием методов защищенного программирования.

Ж.1.4 Проектирование системы защиты персональных данных для вводимой в эксплуатацию информационной системы персональных данных должно производиться с учетом уже построенной в образовательной организации системы защиты персональных данных, включающей комплекс организационных и технических мер.

Ж.1.5 На стадии ввода в эксплуатацию информационной системы персональных данных должны быть проведены как минимум следующие мероприятия:

– установка пакета прикладных программ информационной системы персональных данных совместно со средствами защиты информации (встроенными и наложенными);

– опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе информационной системы персональных данных;

– приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

Ж.1.6 В случае внедрения дополнительных средств защиты должны быть составлены акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний, подготавливаемые и подписываемые ответственным за обеспечение безопасности персональных данных.

Ж.1.7 Перед вводом новой информационной системы персональных данных в опытную эксплуатацию должен быть составлен акт о вводе в опытную эксплуатацию информационной системы персональных данных, подписываемый ответственным за обеспечение безопасности персональных данных, а также акт определения уровней защищенности персональных данных в информационной системе персональных данных, подготовленный и подписанный комиссией по определению уровней защищенности персональных данных в информационной системе персональных данных.

Ж.1.8 В случае успешного функционирования информационной системы персональных данных на стадии опытной эксплуатации и принятия решения о переводе ее в промышленную эксплуатацию составляется акт о вводе в промышленную эксплуатацию новой информационной системы персональных данных.

Ж.2 Требования к выводу информационной системы персональных данных из эксплуатации

Ж.2.1 В случае принятия решения о выводе информационной системы персональных данных из промышленной эксплуатации ответственным за обеспечение безопасности персональных данных и директором по технологиям и развитию бизнеса должен быть подписан акт о выводе информационной системы персональных данных из промышленной эксплуатации.

Ж.2.2 При выводе информационной системы персональных данных из промышленной эксплуатации с целью обеспечения справочной поддержки образовательной организации доступ к ней должен быть ограничен определенным составом лиц с правами только на чтение.

Ж.2.3 После подписания акта о выводе информационной системы персональных данных из промышленной эксплуатации информационной системы

персональных данных переводится в архивный фонд образовательной организации (в соответствии с ч. 2 ст. 13 № 125-ФЗ «Об архивном деле»), при этом должны быть выполнены следующие требования:

– доступ к архивной информационной системе персональных данных и хранимым в ней документам должен обеспечиваться на основании соответствующей заявки на имя руководства образовательной организации, по согласованию с ответственным за организацию обработки персональных данных и владельцем информационной системы персональных данных;

– персональные данные, хранящиеся в архиве, могут быть использованы и переданы третьим лицам только в целях исполнения законодательства Российской Федерации;

– должны быть обеспечены финансовые, материально-технические и иные условия, необходимые для комплектования, хранения, учета и использования информационной системы персональных данных, включая специальное помещение, отвечающее нормативным условиям труда работников архива;

– доступ в помещения, где предполагается хранение выводимой из эксплуатации информационной системы персональных данных, должен быть ограничен;

– должен быть регламентирован перечень лиц, допущенных к работе с информационной системой персональных данных, переданной в архив;

– все внешние запоминающие устройства (ленты с резервными копиями, дискеты, CD-диски, флеш-накопители и т. п.) должны храниться в сейфах;

– должно быть разработано описание информационной системы персональных данных, переведенной в архивный фонд образовательной организации. Описание информационной системы персональных данных разрабатывается ответственным за обеспечение безопасности либо сторонней компанией, имеющей лицензию ФСТЭК России на осуществление технической защиты информации.