

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ  
Государственное бюджетное профессиональное образовательное  
учреждение города Москвы  
**«Политехнический техникум № 47 имени В.Г. Федорова»**  
(ГБПОУ ПТ № 47)

СОГЛАСОВАНО

Первичная профсоюзная организация

председатель

Т.Б. Драгун

протокол №

112

« 19 » 10 2020 г.



УТВЕРЖДЕНО

Директор ГБПОУ ПТ № 47

Д.А. Сынгаевский

2020 г.



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

Москва, 2020

## Содержание

<b>1. Введение.....</b>	4
<b>2. Общие положения.....</b>	5
<b>3. Роли персонала.....</b>	6
<b>4. Обязательные мероприятия по обеспечению безопасности</b>	
<b>5. информационных систем персональных данных .....</b>	7
Общие требования .....	7
<b>6. Обеспечение технической защиты персональных данных.....</b>	10
Общие требования .....	10
Контроль выполнения требований по защите персональных данных .....	14
Учет съемных электронных носителей персональных данных .....	14
<b>7. Обязанности персонала .....</b>	15
Обязанности Ответственного за организацию обработки персональных данных .....	15
Обязанности Ответственного за обеспечение безопасности персональных данных .....	
<b>8. Организация внутреннего контроля обработки и обеспечения</b>	
<b>9. безопасности персональных данных .....</b>	19
Цели организации внутреннего контроля .....	19
Проведение контрольных мероприятий.....	20
Порядок проведения разбирательств.....	21
<b>10.Приложение А Дополнения в договоры и должностные инструкции.....</b>	23
А.1 Должностная инструкция ответственного за организацию обработки персональных данных .....	23
А.2 Дополнения в разделы договоров, в соответствии с которыми образовательная организация поручает обработку персональных данных третьим лицам .....	25
А.3 Дополнения в разделы трудовых договоров об обеспечении безопасности персональных данных .....	27
<b>11.Приложение Б Формы согласия субъекта на обработку его персональных</b>	
<b>данных .....</b>	29
Б.1 Типовая форма согласия родителей (законных представителей) обучающихся на обработку персональных данных .....	29
Б.2 Форма согласия работника на обработку персональных данных .....	29
<b>12.Приложение В Форма уведомления субъектов персональных данных об</b>	
<b>обработке его персональных данных.....</b>	34
<b>13.Приложение Г Формы бланков учета .....</b>	36
Г.1 Форма журнала учета средств защиты информации.....	36
Г.2 Форма журнала учета съемных носителей персональных данных.....	37
<b>14.Приложение Д Форма акта об уничтожении персональных данных .....</b>	38
<b>15.Приложение Е Формы перечней .....</b>	39
Е.1 Форма перечня лиц, допущенных к обработке персональных данных.....	39
Е.2 Форма перечня персональных данных, обрабатываемых в образовательной организации.....	40
Е.3 Форма перечня информационных систем персональных данных, используемых в	

образовательной организации .....	41
<b>16. Приложение Ж Требования к вводу или выводу информационных систем из эксплуатации .....</b>	<b>42</b>
Ж.1 Требования к разработке и вводу в эксплуатацию информационных систем персональных данных .....	42
Ж.2 Требования к выводу информационной системы персональных данных из эксплуатации .....	44

## **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 № 152-ФЗ

«О персональных данных» (далее - Закон 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 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляющейся 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 профессиональном образовательного учреждения города Москвы «Политехнический техникум № 47 имени В.Г. Федорова» (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 персональные данные.

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 Закона о персональных данных.

4.1.7 Выбор и реализация методов и способов защиты информации в информационных системах персональных данных осуществляются на основе Модели угроз 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 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
- 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 персональные данные), информационной системе, содержащей персональные данные и связанные с ее работой документами (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 персональные данные;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам (включая персональные данные), 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 ниже);
- 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 Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 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 безопасность 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 безопасность персональных данных.

## **6. Обязанности персонала**

Должностные инструкции Ответственного за организацию обработки персональных данных и Ответственного за обеспечение безопасность 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 образовательной организацией 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<sup>1</sup> 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.

## **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

---

<sup>1</sup> Ст. 20 ч. 4 ФЗ «О персональных данных»

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 (подраздел 5.2 выше);
- предоставление сведений о персональных данных Ответственному за организацию обработки персональных данных в рамках проведения учета защищаемых носителей и проведения инвентаризации (подраздел 5.3 выше);
- 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 (подраздел 5.3 выше);
- учет технических средств защиты информации (пункт 5.1.11 подраздела 5.1 выше);
- периодические ежемесячные<sup>2</sup> проверки журналов безопасности (пункт 5.1.6 подраздела 5.1 выше);
- анализ защищенности информационных систем персональных данных;
- 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 (подразделы 7.2 и 7.3 ниже).

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.

---

<sup>2</sup> Периодичность проверки зависит от срока хранения информации в журналах безопасности, например, если информация в журнале безопасности хранится одну неделю, то проверки необходимо проводить еженедельно

## **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 устраниению 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 устраниении 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 персональными данными;
- 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 разбирательства.

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**

#### **A.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.

## **A.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* - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

*обработка персональных данных* («обработка») - 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* - 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* - 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<sup>3</sup> 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.

### **A.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.

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

---

<sup>3</sup> 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

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 граждансскую, 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 РОДИТЕЛЯ (ЗАКОННОГО ПРЕДСТАВИТЕЛЯ) НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ НЕСОВЕРШЕННОЛЕТНЕГО**

Я,

проживающий по адресу \_\_\_\_\_ (ФИО),  
паспорт серия \_\_\_\_\_ № \_\_\_\_\_ выдан (кем и когда)

тел.: \_\_\_\_\_, адрес электронной почты: \_\_\_\_\_ являюсь  
законным представителем несовершеннолетнего \_\_\_\_\_ (ФИО)  
на основании ст. 64 п. 1 Семейного кодекса РФ<sup>4</sup>.

Настоящим даю свое согласие на обработку в ГБОУ \_\_\_\_\_ персональных данных  
моего несовершеннолетнего \_\_\_\_\_ ребенка (подопечного)  
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 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;**

а также моих персональных данных, а именно:

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

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

- обеспечения защиты конституционных прав и свобод моего ребенка (подопечного);
- 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

<sup>4</sup> 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».

соревнований, и иных знаковых мероприятий;

- ведения статистики;

- размещения фотоизображения на официальном сайте ГБОУ \_\_\_\_\_

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 \_\_\_\_\_

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 \_\_\_\_\_ 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;

- размещения приказа о зачислении обучающихся (*во исполнение требований Приказа Министерства образования № 36 от 6 марта 2014 года «Об утверждении Порядка приема на обучение по образовательным программам среднего профессионального образования» - для ГБОУ СПО*);

- передачи сведений в федеральные и региональные информационные системы в целях обеспечения проведения процедуры 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;

- начисления стипендии (*для обучающихся по программам среднего профессионального и высшего образования*) и иных выплат, в том числе социальных;

- контроля за посещением занятий;

- предоставления информации для оформления проездных документов.

Настоящее согласие предоставляется на осуществление ГБОУ \_\_\_\_\_ 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 (подопечного), 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 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;

- 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 \_\_\_\_\_ обязана осуществлять защиту персональных данных ребенка, принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, модификации, 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.

Захита внесенной информации осуществляется с соблюдением требований, установленных законодательством Российской Федерации. Хранение, обработка, 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 \_\_\_\_\_ несет ответственность, предусмотренную законодательством Российской Федерации.

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 моего ребенка (подопечного), законным представителем которого я являюсь.

Дата: \_\_\_\_\_. \_\_\_\_\_. \_\_\_\_ г.

Подпись: \_\_\_\_\_ (\_\_\_\_\_\_).

Я,

, (фамилия, имя, отчество полностью), зарегистрированного по адресу \_\_\_\_\_, паспорт \_\_\_\_\_, выдан (кем) \_\_\_\_\_, серия № \_\_\_\_\_, (когда) \_\_\_\_\_ даю свое согласие на обработку своих персональных данных в целях:

## **Б.2 Форма согласия работника на обработку персональных данных**

### **СОГЛАСИЕ**

### **НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКА**

- 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 ГБПОУ ПТ №47;
- контроля количества и оценки качества выполняемой мной работы;
- размещения фото и видеоизображений на официальном сайте ГБПОУ ПТ №47 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;

ГБОУ \_\_\_\_\_;

- сведения о налоговых отчислениях и сборах;
- номер СНИЛС;
- ИНН;
- информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в ГБПОУ ПТ №47;
- сведения о доходах в ГБПОУ ПТ №47;
- 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. ГБПОУ ПТ№47 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, модификации, 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.

Задача 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» ГБПОУ ПТ№47 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 ГБПОУ ПТ№47 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: *наименование организации*,  
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.*)

« » 201 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 <sup>5</sup> (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						

<sup>5</sup> 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  
Акт № \_\_\_\_\_

« \_\_\_\_\_ »  
об уничтожении персональных данных

201 г.

№ 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

## **E.2 Форма перечня персональных данных, обрабатываемых в образовательной организации**

Перечень персональных данных, обрабатываемых в образовательной организации

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

**Перечень информационных систем персональных данных, используемых в образовательной организации**

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

## **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 системе 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 организацией, имеющей лицензию ФСТЭК России на осуществление технической защиты информации.