ПРИНЯТО
На заседании Педагогического совета
Протокол № 30
от 13.12.2021 г.

Приложение № 5 к приказу
Директора АНО ОШ ЦПМ
От «13» декабря 2021г.
№141-ОД21

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

Подписано цифровой подписью:
Андросов Александр Александрович
DN: cn=Андросов Александр Александрович, o=АНО ОШ ЦПМ, ou=Первый заместитель директора, email=a.androsov@school-cpm.ru, c=RU
Дата: 2023.01.10 12:16:47 +03'00'

Москва, 2021

Содержание

1 Введение 4

2 Общие положения....5

3 Обязательные мероприятия по обеспечению безопасности информационных систем персональных данных....6

3.1 Общие требования 6

4 Обеспечение технической защиты персональных данных 9

4.1 Общие требования 9

4.2 Контроль выполнения требований по защите персональных данных 13

4.3 Учет съемных электронных носителей персональных данных 13

4.4 Парольная политика 13

5 Обязанности полномочия Ответственного за обеспечение безопасности персональных данных 15

5.1 В обязанности Ответственного за обеспечение безопасности персональных данных входит: 15

5.2 Ответственный за обеспечение безопасности персональных данных обладает следующими полномочиями: 16

6 Организация внутреннего контроля обработки и обеспечения безопасности персональных данных 17

6.2 Проведение контрольных мероприятий 18

6.3 Порядок проведения разбирательств 19

Приложение 1 Дополнения в договоры и должностные инструкции 22

1.1 Должностная инструкция Ответственного за организацию обработки персональных данных 22

1.2 Дополнения в разделы договоров, в соответствии с которыми Учреждение поручает обработку персональных данных третьим лицам 24

1.3 Дополнения в разделы трудовых договоров об обеспечении безопасности персональных данных 26

Приложение 2 Формы согласия субъекта на обработку его персональных данных 28

1.4 Форма согласия работника на обработку персональных данных....28

1.5 Форма согласия работника на обработку персональных данных разрешенных субъектом для распространения....31

Приложение 3 Формы бланков учета 32

1.6 Форма журнала учета средств защиты информации 32

1.7 Форма журнала учета съемных носителей персональных данных 33

Приложение 4 Форма акта об уничтожении персональных данных 34

Приложение 5 Формы перечней 35

1.8 Форма перечня лиц, допущенных к обработке персональных данных 35

1.9 Форма перечня персональных данных, обрабатываемых в Учреждении 36

1.10 Форма перечня информационных систем персональных данных, используемых в Учреждении.....37

Приложение 6 Требования к вводу или выводу информационных систем из эксплуатации.....38

1.11 Требования к разработке и вводу в эксплуатацию информационных систем персональных данных.....38

1.12 Требования к выводу информационной системы персональных данных из эксплуатации.....40

1 Введение

1.1 Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных), постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», иным законодательством Российской Федерации о персональных данных и правовыми актами федеральных органов исполнительной власти по вопросам безопасности персональных данных, в том числе при их обработке в информационных системах персональных данных.

1.2 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 Автономной некоммерческой организации «Общеобразовательная школа Центра педагогического мастерства» (АНО ОШ ЦПМ) (далее – Учреждение) назначается из числа работников Ответственный за организацию обработки персональных данных и Ответственный за обеспечение безопасности персональных данных.

1.3 Настоящее Положение подлежит актуализации в случае изменений законодательства Российской Федерации о персональных данных и/или при изменении организационной структуры Учреждении.

2 Общие положения

2.1 Настоящее Положение (далее – Положение) разработано в целях организации в Учреждении процесса обеспечения безопасности персональных данных согласно требованиям законодательства Российской Федерации.

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

2.3 Положение обязательно для ознакомления и исполнения всеми работниками Учреждения, работающими с персональными данными, Ответственным за организацию обработки персональных данных, Ответственным за обеспечение безопасности персональных данных, инженерами по телекоммуникации (техниками).

3 Обязательные мероприятия по обеспечению безопасности информационных систем персональных данных

3.1 Общие требования

3.1.1 В Учреждении 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.

3.1.2 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.

3.1.3 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 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3.1.4 По согласованию с Департаментом образования и науки города Москвы в Учреждении могут использоваться собственные информационные системы персональных данных. Порядок ввода в эксплуатацию и вывода из эксплуатации таких информационных систем описан в Приложение 6 к настоящему Положению.

3.1.5 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 Учреждения 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.

3.1.6 В Учреждении должны быть разработаны модели угроз безопасности персональных данных для всех информационных систем персональных данных. Модель угроз разрабатывается на основе методических документов, принятых в соответствии с п. 5 ст. 19 Закона о персональных данных.

3.1.7 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.

3.1.8 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.

3.1.9 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 Обеспечение технической защиты персональных данных

4.1 Общие требования

4.1.1 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.

4.1.2 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 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

2) Выявление и закрытие технических каналов утечки персональных данных на основе анализа и своевременной 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 работников, задействованных в эксплуатации данной информационной системы персональных данных.

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

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

реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам (включая персональные данные) информационной системы персональных данных и связанным с ее использованием работам, документам;

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

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;

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.

4.1.5 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.

4.1.6 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.

4.1.7 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.

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

4.1.9 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.

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

4.1.11 В Учреждении должен вестись учет технических средств защиты информации, эксплуатационной и технической документации к ним. Форма журнала учета технических средств защиты информации приведена в Приложении Г к Положению.

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

4.2 Контроль выполнения требований по защите персональных данных

4.2.1 В Учреждении должен проводиться периодический контроль выполнения требований по обеспечению безопасности персональных данных (не реже одного раза в три года).

4.2.2 Контроль функций системы защиты производится в рамках мероприятий, описанных в пункте 6.2 Положения.

4.2.3 Ответственность за контроль функций системы защиты персональных данных возлагается на Ответственного за обеспечение безопасности персональных данных.

4.3 Учет съемных электронных носителей персональных данных

4.3.1 В Учреждении 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.

4.3.2 Учет защищаемых съемных носителей персональных данных ведется в журнале учета защищаемых съемных электронных носителей (Приложение № 3 к Положению).

4.3.3 Ответственность за учет защищаемых электронных носителей персональных данных возлагается на Ответственного за обеспечение безопасности персональных данных.

4.4 Парольная политика

4.4.1 Индивидуальный пароль служит для аутентификации пользователя и должен сохраняться пользователем в тайне. Во избежание записи паролей на бумаге, пароль должен быть легко запоминаем, но в, тоже время, быть достаточно сложным.

4.4.2 Правила использования паролей изложены в Инструкции пользователя по обеспечению безопасности персональных данных при их обработке в информационной системе (пункт 3.4).

4.4.3 Доступ пользователя к учетной записи блокируется после 90 дней неиспользования учетной записи.

4.4.4 Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки составляет до 10 попыток.

4.4.5 Временные пароли (при первоначальной регистрации пользователя и взамен утерянных) назначаются администратором информационной системы.

5 Обязанности полномочия Ответственного за обеспечение безопасности персональных данных

5.1 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;
- предоставление сведений о персональных данных Ответственному за организацию обработки персональных данных в рамках проведения учета защищаемых носителей и проведения инвентаризации;
- 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;
- учет технических средств защиты информации ;
- периодические ежемесячные[1] проверки журналов безопасности ;
- анализ защищенности информационных систем персональных данных;
- организация процесса обучения работников по направлению обеспечения безопасности персональных данных;

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

- участие в проведении внутреннего контроля и служебных расследований фактов нарушения установленного порядка обработки и обеспечения безопасности персональных данных.

5.2 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.

6 Организация внутреннего контроля обработки и обеспечения безопасности персональных данных

6.1 Организация внутреннего контроля процесса обработки персональных данных в Учреждении 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.

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

- обеспечение соблюдения работниками Учреждения 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.

6.2 **Проведение контрольных мероприятий**

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

6.2.2 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.

6.2.3 Контрольные мероприятия (проверки) организуются Ответственным за обеспечение безопасности персональных данных.

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

- проверку деятельности работников Учреждения, допущенных к работе с персональными данными в информационных системах персональных данных, на соответствие порядку обработки и обеспечения безопасности персональных данных, установленному Положением об обработке персональных данных и другими локальными актами, принятыми в Учреждении 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.

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

6.2.6 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.

6.2.7 Выявленные нарушения расследуются в соответствии с пунктом 6.3 настоящего Положения.

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

6.2.9 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.

6.3 **Порядок проведения разбирательств**

6.3.1 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 Учреждения 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;

- в связи с запросом уполномоченного органа по защите прав субъектов персональных данных.

6.3.2 Срок проведения расследования не должен превышать семи рабочих дней. Проведение расследования в больший срок должно быть согласовано с директором Учреждения. В ходе проведения расследования Ответственным за обеспечение безопасности персональных данных проводится опрос очевидцев и подозреваемых лиц, предположительно допустивших нарушение.

6.3.3 В ходе проведения опроса выясняются:

- дата и время совершения нарушения;
- обстоятельства, при которых были совершены действия, приведшие к возникновению нарушения;
- последствия, возникшие вследствие совершения нарушения.

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

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

6.3.6 По результатам разбирательства Ответственный за обеспечение безопасности персональных данных в течение трех рабочих дней составляет заключение.

6.3.7 В заключении должны быть приведены:

- основания проведения разбирательства;
- краткая справка по нарушению, в отношении которого проводилось разбирательство;
- лицо(а), которое совершило(и) нарушение;
- предложения по принятию мер о привлечении виновных лиц к ответственности;
- план мероприятий по профилактике подобных нарушений.

6.3.8 Заключение представляется Ответственному за организацию обработки персональных данных на согласование и представляется директору Учреждения для принятия решения.

Приложение 1
Дополнения в договоры и должностные инструкции

1.1 Должностная инструкция Ответственного за организацию обработки персональных данных

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

Ответственный за организацию обработки персональных данных подчиняется непосредственно директору Учреждения.

В своей деятельности Ответственный за организацию обработки персональных данных руководствуется:

- действующими нормами международного права и законодательством Российской Федерации;
- уставом Учреждения;
- организационно-распорядительными документами Учреждения по вопросам организации обработки и обеспечения безопасности персональных данных;
- приказами, распоряжениями директора Учреждения;
- настоящей должностной инструкцией.

На время отсутствия ответственного за организацию обработки персональных данных его обязанности исполняет директор Учреждения или назначенный им работник.

Основными задачами Ответственного за организацию обработки персональных данных являются:

- осуществление внутреннего контроля за соблюдением Учреждением и ее работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения работников Учреждения 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 Учреждения, относящуюся к работе с персональными данными и необходимую для выполнения его обязанностей;

контролировать выполнение обязанностей Ответственным за обеспечение безопасности персональных данных, а также выполнение требований законодательства и локальных актов Учреждения, 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.

1.2 Дополнения в разделы договоров, в соответствии с которыми Учреждение 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), блокирование, удаление, уничтожение персональных данных.

«Субподряд» и «заключение договора субподряда» означает процесс, когда Стороны договариваются с третьей стороной о выполнении обязательств в соответствии с настоящим Договором, а «субподрядчик» означает сторону, с которой заключен «договор субподряда».

«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

Действия с персональными данными, разрешенные обработчику

Персональные данные передаются обработчику для совершения следующих действий (операций):

Действие	Цель
Например, использование	*Например, участие в городском конкурсе*
Например, систематизация	*Например, подведение итогов конкурса*

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 «договора субподряда»

1) Обработчик не должен заключать «договор субподряда» по исполнению своих обязательств, налагаемых настоящим Договором, без предварительного письменного согласия Оператора.

2) В том случае если Обработчик с согласия Оператора заключает «договор субподряда», 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 «субподрядчик» не в состоянии выполнять свои обязательства, вытекающие из «договора субподряда», 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[2] 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.

1.3 Дополнения в разделы трудовых договоров об обеспечении безопасности персональных данных

В раздел трудовых договоров (должностных инструкций) персонала информационных систем, 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 Учреждения.

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

[2] 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

1) Работник Учреждения несет ответственность за обеспечение конфиденциальности персональных данных, ставших ему известными в связи с выполнением должностных обязанностей.

2) Работник Учреждения 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 Учреждения.

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

Приложение 2
Формы согласия субъекта на обработку его персональных данных

1.4 Форма согласия работника на обработку персональных данных

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____ (*ФИО),* проживающий по адресу _____, паспорт серия _____ № _____ выдан (*дата, орган, выдавший его, код подразделения*) _____ _____, даю (***наименование образовательного учреждения, его адрес, указанный в Едином государственном реестре юридических лиц, ИНН, ОГРН***) свое согласие *АНО ОШ ЦПМ* (далее – Учреждение) 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 Учреждения;
- контроля количества и оценки качества выполняемой мной работы;

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 Учреждении;
- сведения о налоговых отчислениях и сборах;
- номер СНИЛС;
- ИНН;
- информация о приеме, переводе, увольнении и иных событиях, относящихся к моей трудовой деятельности в Учреждении;
- сведения о доходах в Учреждении;
- 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;

Обработка персональных данных должна осуществляться с соблюдением требований, установленных законодательством Российской Федерации и только для целей, указанных выше. Учреждение 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, 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» Учреждение должно нести ответственность, предусмотренную законодательством Российской Федерации.

Данное Согласие действует до окончания моей работы в Учреждении 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.

«____» _____ 20__ г. _____ _____
(Подпись) (ФИО)

1.5 Форма согласия работника на обработку персональных данных разрешенных субъектом для распространения

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ, РАЗРЕШЕННЫХ СУБЪЕКТОМ ДЛЯ РАСПРОСТРАНЕНИЯ

Я, _____ (*ФИО),*

тел.: _____, адрес электронной почты: _____, даю **(*наименование образовательного учреждения, его адрес, указанный в Едином государственном реестре юридических лиц, ИНН, ОГРН*)** свое согласие *Наименование организации* (далее – Учреждение) на публикацию следующих своих персональных данных `своих персональных данных в целях:`

Данные	Место публикации	Цель публикации

Информационный ресурс Учреждения, посредством которого будет осуществляться публикация и иные действия с моими персональными данными **— *адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы*.**

Категории и перечень персональных данных, для обработки которых я устанавливаю условия и запреты (*заполняется по желанию*):

_____

_____

Условия, при которых мои персональные данные могут передаваться оператором, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных (*заполняется по желанию*):

_____

_____

_____

Данное Согласие действует до окончания моей работы в Учреждении 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.

«____» _____ 20__ г. _____ _____

Приложение 3
Формы бланков учета

1.6 Форма журнала учета средств защиты информации

Журнал учета средств защиты информации

№ п/п	Тип средства	Наименование средства защиты информации	Индекс или условное наименование[1] (для сертифицированных средств)	Регистрационный номер[1] (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						

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

1.7 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						
12						
13						
14						
15						
16						

Приложение 4
Форма акта об уничтожении персональных данных

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: _____.

При уничтожении присутствовал: _____

(должность, И.О.Фамилия)

Приложение 5
Формы перечней

1.8 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

1.9 Форма перечня персональных данных, обрабатываемых в Учреждении

Перечень персональных данных, обрабатываемых в Учреждении

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

1.10 Форма перечня информационных систем персональных данных, используемых в Учреждении

Перечень информационных систем персональных данных, используемых в Учреждении

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

Приложение 6
Требования к вводу или выводу информационных систем из эксплуатации

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

1.11 Требования к разработке и вводу в эксплуатацию информационных систем персональных данных

1.11.1 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 эксплуатацию информационной системы персональных данных.

1.11.2 По результатам проведенного анализа и с учетом 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.

1.11.3 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.

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

1.11.5 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.

1.11.6 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.

1.11.7 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.

1.11.8 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.

1.12 Требования к выводу информационной системы персональных данных из эксплуатации

1.12.1 В случае принятия решения о выводе информационной системы персональных данных из эксплуатации Ответственным за обеспечение безопасности персональных данных и иными уполномоченными лицами должен быть подписан Акт о выводе информационной системы персональных данных из эксплуатации.

1.12.2 При выводе информационной системы персональных данных из эксплуатации с целью обеспечения справочной поддержки Учреждения доступ к ней должен быть ограничен определенным составом лиц с правами только на чтение.

1.12.3 После подписания Акта о выводе информационной системы персональных данных из эксплуатации она переводится в архив Учреждения (в соответствии с ч. 2 ст. 13 Федерального закона № 125-ФЗ «Об архивном деле»), если иной способ ее использования (использования информации) не определен в

обосновании вывода информационной системы из эксплуатации. При этом должны быть выполнены следующие требования:

доступ к архивной информационной системе персональных данных и хранимым в ней документам (информации) должен обеспечиваться на основании соответствующей заявки на имя руководства Учреждения, 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 Учреждения. Описание информационной системы персональных данных разрабатывается Ответственным за обеспечение безопасности персональных данных либо сторонней компанией, имеющей лицензию ФСТЭК России на осуществление технической защиты информации.