МИНИСТЕРСТВО ФИЗИЧЕСКОЙ КУЛЬТУРЫ И СПОРТА
МОСКОВСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ МОСКОВСКОЙ ОБЛАСТИ
«УЧИЛИЩЕ (ТЕХНИКУМ) ОЛИМПИЙСКОГО РЕЗЕРВА № 2»
(ГБПОУ МО «УОР № 2»)

ПРИКАЗ

11 мая 2021 г. № 189

г. Звенигород

О защите информации и информационной безопасности
в ГБПОУ МО «УОР № 2»

В соответствии с требованиями Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных, Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и в целях организации защиты информации и обеспечения информационной безопасности в ГБПОУ МО «УОР № 2» (далее - Училище):

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие с 11 мая 2021 г. следующие организационно-распорядительные документы по защите информации и обеспечению информационной безопасности в ГБПОУ МО «УОР № 2»:

1.1. Положение о защите информации и обеспечении информационной безопасности в ГБПОУ МО «УОР № 2» (Приложение № 1);

1.2. Положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (Приложение № 2);

1.3. Состав комиссии по защите информации в ГБПОУ МО «УОР № 2» (Приложение № 3);

1.4. Положение о комиссии по защите информации ГБПОУ МО «УОР № 2» (Приложение № 4);

1.5. Типовые формы журналов по защите информации (Приложение № 5);

1.6. Типовую форму Протокола заседания комиссии ГБПОУ МО «УОР № 2» по защите информации (Приложение № 6);

1.7. Типовую форму Акта определения уровня защищенности ПД при их обработке в ИСПД и класса защищенности ИС (Приложение № 7);

1.8. Типовую форму Акта об уничтожении персональных данных субъектов персональных данных (Приложение № 8);

1.9. Инструкцию по организации резервирования (Приложение № 9);

1.10. Инструкцию по организации парольной защиты в ГБПОУ МО «УОР № 2» (Приложение № 10);

1.11. Инструкцию по организации антивирусной защиты в ГБПОУ МО «УОР № 2» (Приложение № 11);

1.12. Инструкцию по проверке электронного журнала обращений к информационной системе персональных данных (Приложение № 12);

1.13. Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении законных оснований (Приложение № 13);

1.14. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (Приложение № 14);

1.15. Инструкцию по обращению с криптосредствами в ГБПОУ МО «УОР № 2» (Приложение № 15);

1.16. Инструкцию по обработке персональных данных без использования средств автоматизации (Приложение № 16);

1.17. Правила работы с обезличенными данными в ГБПОУ МО «УОР № 2» (Приложение № 17)

1.18. Инструкцию по работе с инцидентами информационной безопасности (Приложение № 18);

1.19. План мероприятий по защите информации в ГБПОУ МО «УОР № 2» на 2021 год (Приложение № 19).

2. Секретарю Маскаевой А.Е. довести требования приказа до лиц, ответственных за обеспечение информационной безопасности в информационных системах безопасных данных и ответственных за его исполнение.

3. Контроль за исполнением настоящего приказа оставляю за собой

Директор  Алексеенко А.А.

Приложение № 3
к приказу № 189 от 11 мая 2021 г.

«УТВЕРЖДАЮ»
Директор ГБПОУ МО «УОР № 2»
_____ Алексеенко А.А.
«11» мая 2021 г.

Состав комиссии по защите информации
в ГБПОУ МО «УОР № 2»

Председатель комиссии – заместитель директора Ушаков В.В.;

Заместитель председателя комиссии – заведующий спортивным сооружением Шуйский Д.В.;

Члены комиссии:

1. начальник отдела Киценко А.П.;
2. начальник отдела Мелентьева Ю.В.;
3. начальник отдела Гавриленко Р.А.;
4. ведущий программист Лапин М.Н.

Приложение 1
к Приказу ГБПОУ МО «УОР № 2»
от «11» мая 2021г. № 189

ПОЛОЖЕНИЕ
о защите информации и обеспечении информационной безопасности в ГБПОУ МО «УОР № 2»

I. Общие положения

1.1. Настоящее Положение о защите информации и обеспечении информационной безопасности определяет порядок получения, обработки, использования и защиты в ГБПОУ МО «УОР № 2» (далее - Училище), определенной в соответствии с законодательством Российской Федерации информации ограниченного пользования, а также общие требования к информационным системам, содержащим такую информацию в Училище.

1.2. Настоящее Положение разработано в соответствии с федеральными законами и иными правовыми актами Российской Федерации, законами и иными правовыми актами города Москвы.

1.3. В целях настоящего Положения под информацией ограниченного пользования понимается образующаяся в процессе деятельности Училища или поступившая в Училище информация (сведения, сообщения, данные и т.п.), доступ к которой ограничен законодательством Российской Федерации, в том числе:

1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

2) сведения, составляющие тайну следствия и судопроизводства;

3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

4) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

1.4. К информации ограниченного пользования не могут быть отнесены сведения, обязательные к раскрытию Училищем в соответствии с законодательством Российской Федерации.

1.5. Настоящее Положение не распространяется на обработку обезличенных персональных данных, а также персональных данных, сделанных общедоступными субъектом персональных данных.

1.6. Училище организует обеспечение безопасности хранения, обработки и передачи по каналам связи информации, указанной в пункте 1.3 настоящего Положения.

1.7. Мероприятия по защите информации, указанной в пункте 1.3 настоящего Положения (далее - информация ограниченного пользования), осуществляются Училищем во взаимосвязи с мерами по обеспечению установленной конфиденциальности проводимых работ.

1.8. Обработка персональных данных в Училище осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.9. Объектами защиты информации в Училище являются:

1) средства и системы информатизации и связи (средства вычислительной техники, локальная вычислительная сеть, средства и системы связи и передачи информации, средства звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления и тиражирования документов), используемые для обработки, хранения и передачи информации ограниченного пользования;

2) технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается информация ограниченного пользования;

3) помещения (служебные кабинеты и т.д.) специально предназначенные для проведения конфиденциальных мероприятий;

4) помещения, специально предназначенные для хранения информации ограниченного пользования.

1.10. Ответственность за выполнение требований настоящего Положения возлагается на должностное лицо, ответственное за защиту информации и обеспечение информационной безопасности в Училище (далее - ответственное должностное лицо), а также лиц, допущенных к обработке, передаче и хранению информации ограниченного пользования.

1.11. Непосредственное руководство мероприятиями по организации защиты информации ограниченного пользования в Училище осуществляет директор ГБПОУ МО «УОР № 2».

II.Обеспечение защиты информации ГБПОУ МО «УОР № 2»

2.1. Защита информации в Училище представляет собой комплекс организационных и технических мер и включает в себя обеспечение защиты информации ограниченного пользования от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

2.2. Для организации защиты информации ограниченного пользования директор Училища принимает следующие меры:

1) утверждает перечень информации, подлежащей защите в Училище;

2) назначает лицо, ответственное за организацию защиты информации

и обеспечение информационной безопасности в Училище;

3) утверждает списки работников в Училище, которые, в соответствии со своими должностными обязанностями, допускаются к работе с информацией ограниченного пользования;

4) определяет помещение, специально предназначенное для хранения информации ограниченного пользования, и обеспечивает его охрану.

5) обеспечивает знакомство под роспись при приеме на работу в Училище работников с перечнем информации, подлежащей защите в Училище;

6) осуществляет контроль за обеспечением защиты информации ограниченного пользования;

7) обеспечивает подключение к охранной сигнализации и передачу охранной организации на хранение помещения, с последующей записью в Журнале сдачи и приема под охрану помещений и ключей от них.

III. Требования к информационной безопасности в ГБПОУ МО «УОР № 2»

3.1. Находящиеся в ведении Училища информационные системы (ИС) и ресурсы, содержащие информация ограниченного пользования, подлежат **обязательной защите.**

3.2. Информация ограниченного пользования должна обрабатываться (передаваться) с использованием защищенных систем и средств информатизации и связи или с использованием технических и программных средств технической защиты информации ограниченного пользования.

3.3. Уровень технической защиты информации ограниченного пользования, а также перечень необходимых мер защиты определяется в соответствии с требованиями законодательства РФ.

3.4. В целях обеспечения защиты информации ограниченного пользования работники Училища **обязаны**:

1) хранить в тайне пароль (пароли), позволяющие получить доступ к информации ограниченного пользования;

2) при служебной переписке использовать исключительно электронную почту в домене mfks_uor_2@mosreg.ru;

3) поддерживать в актуальном состоянии антивирусное программное обеспечение, регулярно проводить его обновление;

4) исключить физический доступ посторонних лиц к закрепленным за ним средствам обработки информации ограниченного пользования;

5) неукоснительно выполнять предписания на эксплуатацию средств связи, вычислительной техники, оргтехники, бытовых приборов и другого оборудования, установленного в помещении;

6) немедленно вызывать ответственное должностное лицо и ставить в известность руководителя Училища в случае утери ключевого носителя электронно-цифровой подписи или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или

несоответствии номеров печатей при их наличии) на аппаратных средствах или иных фактов совершения в его отсутствие попыток несанкционированного доступа к рабочей станции;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств рабочей станции;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов рабочей станции или периферийных устройств (дисководов, принтеров и т.п.), а также перебоев в системе электроснабжения;

- некорректного функционирования установленных на рабочей станции технических средств защиты;

- непредусмотренных формуляром рабочей станции отводов кабелей и подключенных устройств;

7) присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним рабочей станции в подразделении.

8) передать Училищу при прекращении или расторжении трудового договора имеющиеся в пользовании материальные носители информации, содержащие информацию ограниченного пользования.

3.5. Работникам Училища **запрещается**:

1) использовать компоненты программного и аппаратного обеспечения Училища в неслужебных целях;

2) самовольно вносить изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;

3) для предотвращения заражения компьютеров вредоносным программным обеспечением, в том числе с полной потерей данных, запрещается открывать вложенные файлы и переходить по ссылкам из писем, полученных из недостоверных источников;

4) осуществлять обработку информации ограниченного пользования в присутствии не допущенных к данной информации лиц;

5) записывать и хранить информацию ограниченного пользования на неучтенных носителях информации;

6) оставлять включенной без присмотра свою рабочую станцию, не активизировав средства защиты от несанкционированного допуска (временную блокировку экрана и клавиатуры);

7) передавать кому-либо свой персональный носитель электронно-цифровой подписи (кроме директора Училища, делать неучтенные копии носителя электронно-цифровой подписи (на любой другой носитель) и вносить какие-либо изменения в носитель электронно-цифровой подписи;

8) использовать свой персональный носитель электронно-цифровой подписи для формирования цифровой подписи любых электронных документов, кроме регламентированных технологическим процессом на его

рабочем месте;

9) оставлять без личного присмотра на рабочем месте или где бы то ни было свой персональный носитель электронно-цифровой подписи, машинные носители и распечатки, содержащие информацию ограниченного пользования;

10) умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок необходимо ставить в известность ответственное должностное лицо.

3.6. Допускается использование только учтенные носители информации ограниченного пользования, которые подвергаются регулярной ревизии и контролю.

3.7. При использовании работниками Училища носителей информации ограниченного пользования **необходимо**:

1) использовать носители информации ограниченного пользования исключительно для выполнения своих служебных обязанностей;

2) обеспечивать физическую безопасность носителей информации ограниченного пользования всеми разумными способами;

3) извещать ответственное должностное лицо и директора Училища о фактах утраты (кражи) носителей информации ограниченного пользования.

3.8. При использовании носителей информации ограниченного пользования **запрещено**:

1) использовать носители информации ограниченного пользования в личных целях;

2) передавать носители информации ограниченного пользования другим лицам (за исключением директора Училища и ответственного должностного лица);

3) хранить носители информации ограниченного пользования вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

4) выносить носители информации ограниченного пользования из служебных помещений для работы с ними без согласования директора Училища.

3.9. Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником Училища между информационной системой Училища, содержащей информацию ограниченного пользования и неучтенными (личными) носителями информации, рассматривается как **несанкционированное**.

3.10. В случае выявления фактов несанкционированного и/или нецелевого применения носителей информации ограниченного пользования инициализируется служебная проверка, проводимая комиссией, состав которой определяется директором Училища.

3.11. По факту выясненных обстоятельств составляется акт расследования инцидента и передается директору Училища для принятия мер

согласно локальным нормативным актам Училища и законодательству Российской Федерации.

3.12. Информация, хранящаяся на носителях информации ограниченного пользования, подлежит обязательной проверке на отсутствие вредоносного программного обеспечения.

3.13. В случае увольнения или перевода работника в другое структурное подразделение Училища, предоставленные носители информации ограниченного пользования **изымаются**.

IV. Заключительные положения

4.1. В целях обеспечения защиты информации и обеспечения информационной безопасности Училища имеет право привлекать к проведению работ по технической защите информации в установленном порядке организации, имеющие лицензии на соответствующие виды деятельности.

4.2. При проведении Училищем совместных работ с физическими лицами, юридическими лицами, органами государственной власти, органами местного самоуправления, связанных с информацией ограниченного пользования, должна быть обеспечена техническая защита информации ограниченного пользования независимо от места проведения работ.

4.3. Публикация на официальном сайте Училища в информационно-телекоммуникационной сети «Интернет» информации, содержащей персональные данные, осуществляется в соответствии с законодательством Российской Федерации.

4.4. Публикация на официальном сайте Училища в информационно-телекоммуникационной сети «Интернет» информации, содержащей сведения конфиденциального характера, а также информации ограниченного пользования **не допускается**.

4.5. Училище имеет право пройти добровольную аттестацию на соответствие требованиям по технической защите информации ограниченного пользования в порядке, установленном законодательством Российской Федерации.

4.6. Настоящее Положение обязательно для исполнения всеми работниками Училища, которые должны быть ознакомлены с ним под роспись.

4.7. Нарушение требований к работе с информацией ограниченного пользования, влечет материальную, дисциплинарную, гражданскую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации и локальными актами Училища

4.8. Настоящее Положение вступает в силу после его утверждения директором Училища.

Прошито, пронумеровано и скреплено

печатью (Шесть) листов

Должность Директор

ГБПОУ МО «УОР №2»

Подпись /А.А. Алексеенко /

Приложение 2
к Приказу ГБПОУ МО «УОР № 2»
от «11» мая 2021 № 189

Положение
об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

1. Общие положения

1.1. Положение об организации режима обеспечения безопасности помещений ГБПОУ МО «УОР № 2» (далее – Оператор), в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (далее – Положение) разработано 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», Приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.2. Защита от проникновения посторонних лиц в помещения Оператора обеспечивается организацией порядка доступа, а также соответствующей инженерно-технической защитой помещений, а именно охранной сигнализацией и системой контроля и управления доступом.

2. Границы контролируемой зоны

2.1. Контролируемая зона – границы пространства (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

2.2. План-схема контролируемой зоны помещений по адресу г. Звенигород, ул._____, д.___ приведена в приложении 1 к настоящему положению.

Приложение 1

План-схема границ контролируемой зоны

– – – – – Граница контролируемой зоны


Прошито, пронумеровано и скреплено
печатью ___ (Три) лист а
Должность Директор
ГБПОУ МО «УОР №2»
Подпись /А.А. Алексеенко /

Приложение 4
к Приказу ГБПОУ МО «УОР № 2»
от «11» мая 2021 № 189

ПОЛОЖЕНИЕ
о комиссии по защите информации ГБПОУ МО «УОР № 2»

1. Общие положения

1.1. Настоящее Положение определяет основные задачи, порядок формирования, полномочия и ответственность комиссии.

2. Основные задачи комиссии

2.1. Основными задачами комиссии являются:

2.1.1. Сбор и анализ исходных данных по информационным системам персональных данных ГБПОУ МО «УОР № 2».

2.1.2. Определение значений параметров для проведения классификации информационных систем в соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2.1.3. Определение значений параметров для установления уровня защищенности персональных данных в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.1.4. Определение класса защищенности информационных систем персональных данных ГБПОУ МО «УОР № 2» на основании собранных данных.

2.1.5. Определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных.

3. Порядок формирования комиссии

3.1. Комиссия формируется из числа штатных сотрудников ГБПОУ МО «УОР № 2», участвующих в процессе обработки персональных данных.

3.2. В состав Комиссии входит не менее четырех человек – членов Комиссии, в их числе – председатель Комиссии.

3.3. Члены комиссии назначаются приказом директора ГБПОУ МО «УОР № 2».

3.4. В случае изменения состава Комиссии, в приказ вносятся соответствующие изменения.

4. Полномочия комиссии

4.1. Для осуществления задач, указанных в разделе 2 настоящего Положения, Комиссия имеет право:

4.1.1. Получать необходимые сведения у всех работников ГБПОУ МО «УОР № 2», участвующих в обработке персональных данных.

4.1.2. Просматривать электронные базы данных и бумажные носители, содержащие персональные данные, с целью выявления состава обрабатываемых персональных данных.

4.1.3. Отслеживать технологический процесс обработки персональных данных.

4.1.4. Выявлять или получать готовые сведения о структуре локальной вычислительной сети ГБПОУ МО «УОР № 2».

4.1.5. Определять или получать готовые сведения о наличии и способах доступа к сетям общего пользования.

4.1.6. Определять или получать готовые сведения о технических и программных средствах обработки персональных данных.

4.1.7. Определять или получать готовые сведения об условиях, местах и способах передачи персональных данных в сторонние организации.

5. Организация деятельности Комиссии

5.1. Основной формой деятельности Комиссии является заседание.

5.2. Заседание Комиссии ведет председатель Комиссии или по его поручению заместитель председателя Комиссии. В отдельных случаях председатель Комиссии вправе поручить вести заседание Комиссии одному из членов Комиссии.

5.3. Заседания Комиссии проводятся в соответствии с планом ее работы, утверждаемым председателем Комиссии. Для решения оперативных вопросов сроки проведения внеочередного заседания согласовываются с председателем Комиссии. Проекты повестки дня заседания и решений Комиссии, а также необходимые материалы рассылаются членам Комиссии не позднее, чем за неделю до очередного заседания Комиссии.

5.4. Члены Комиссии лично участвуют в заседаниях Комиссии. Они не вправе делегировать свои полномочия другим лицам, в том числе другим членам Комиссии. В случае невозможности присутствия на заседании член Комиссии может сообщить свое мнение по рассматриваемым вопросам письменно.

5.5. Решения Комиссии принимаются большинством голосов присутствующих на заседании членов Комиссии и оформляются протоколами, которые подписывает председательствующий на заседании Комиссии.

5.6. Для предварительной подготовки вопросов, выносимых в повестку дня.

5.7. Члены Комиссии обладают равными правами при обсуждении вопросов, внесенных в повестку дня заседания Комиссии, и при голосовании.

5.8. Председатель Комиссии:

5.8.1. организует подготовку заседаний Комиссии, осуществляет контроль за деятельностью Комиссии;

5.8.2. организует подготовку информационных материалов о работе Комиссии.

5.9. Члены Комиссии имеют право:

5.9.1. участвовать в заседании Комиссии, в подготовке повестки дня заседаний и решений Комиссии;

5.9.2. вносить свои заключения, предложения и замечания по вопросам деятельности Комиссии;

5.9.3. ставить свои предложения на голосование ,а так же иные права, предусмотренные действующим законодательством РФ.

6. Отчетность комиссии

6.1. Комиссия при выполнении своих задач должна составить протокол заседания комиссии.

6.2. В результате своей деятельности Комиссия должна составить Акт(ы) определения уровня защищенности персональных данных и класса защищенности информационных систем персональных данных.

6.3. Решения Комиссии носят рекомендательный характер.

Пронито, пронумеровано и скреплено

печатью ( ) лист

Должность Директор

ГБПОУ МО «УОР №2»

Подпись /А.А. Алексеенко /

Приложение 5
к Приказу ГБПОУ МО «УОР № 2»
от «11» мая 2021 № 189

ЖУРНАЛ
учета машинных носителей персональных данных (стационарные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Дата и место установки (использования)	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета машинных носителей персональных данных (съемные носители)

№ п/п	Регистрационный номер	Тип и ёмкость	Получил (Ф.И.О, дата, подпись)	Сдал (Ф.И.О, дата, подпись)	Место хранения	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных

№ п/п	Сведения о допуске к персональным данным				Сведения о прекращении допуска к персональным данным	
	Наименование информационной системы персональных данных/способ обработки ПДн	ФИО, должность получившего допуск	Дата и номер приказа о допуске	Дата и подпись допускаемого лица	Дата и номер приказа о прекращении допуска	Номер приказа об увольнении или дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн

ЖУРНАЛ
учета средств защиты информации

№ п/п	Индекс и наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей СЗИ	Место установки	Примечание

ЖУРНАЛ
учета средств криптографической защиты информации

№ п/п	Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечания
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении	Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к кот-рым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие	Номер акта или расписка Об уничтожении	

ЖУРНАЛ
учета согласий субъектов персональных данных

№ п/п	Дата и номер согласия	Ф.И.О. субъекта персональных данных

ЖУРНАЛ
учета хранилищ

№ п/п	Регистрационный (учетный) номер хранилища	Вид хранилища	Дата постановки на учет	Фамилия и подпись принявшего (ответственного), дата	Место расположения (номер помещения)	Дата и номер акта о выводе из эксплуатаци	Примечание

ЖУРНАЛ
учета ЭП

№ п/п	Номера экземпляров ключевых документов	Номера криптографических ключей	Наименование СКЗИ	Отметка о получении		Отметка о выдаче		
				От кого получены (УУЦ)	Дата	ФИО пользователя	Дата	Подпись

ЖУРНАЛ
учета персональных идентификаторов и электронных ключей

№ п/п	Ф.И.О.	Получил	Дата	Время	Отметка о возврате (подпись администратора)

ЖУРНАЛ
учета выдачи персональных идентификаторов и электронных ключей (для администратора информационной безопасности)

№ п/п	Ф.И.О.	№ идентификатора	Получил	Дата	Сдал	Отметка о возврате

ЖУРНАЛ
учета выдачи паролей

№ п/п	Дата получения пароля	Ф.И.О. получателя	Подпись получателя

ЖУРНАЛ
учета обращений субъектов персональных данных по вопросам обработки персональных данных

№ п/п	Дата обращения	ФИО обратившегося	Цель обращения	Отметка о предоставлении информации или отказе в ее предоставлении / дата предоставления или отказа в предоставлении информации	Подпись ответственного	Примечание

ЖУРНАЛ
антивирусных проверок информационных систем

№ п/п	Дата и время проверки	Наименование ИСПДн (составной части ИСПДн)	Какими средствами проводилась проверка	Результаты проверки		Наименование инфицированных файлов, источника поступления (носитель, организация)	Примечание (принятые меры)	Фамилия и подпись лица, проводившего проверку
				кол-во проверенных файлов	кол-во инфицированных файлов			

ЖУРНАЛ
уничтожения носителей персональных данных

№ п/п	Наименование ИСПДн, в которой уничтожаются персональные данные	Ф.И.О. субъекта, персональные данные которого подлежат уничтожению	Обоснование уничтожения	Наименование файла, и его месторасположение	Дата уничтожения	Ф.И.О. и подпись Исполнителя	Ф.И.О. и подпись ответственного за обработку персональных данных

Прошито, пронумеровано и скреплено

печатью (Шесть) лист ов

Должность Директор

ГБПОУ МО «УОР №2»

Подпись /А.А. Алексеенко /

Приложение 6
к Приказу ГБПОУ МО «УОР № 2»
от «11» мая 2021 № 189

ПРОТОКОЛ №____
заседания комиссии ГБПОУ МО «УОР № 2» по защите информации

Дата и время проведения _____
Место проведения _____
Председатель комиссии _____ ФИО
Члены комиссии _____ ФИО
_____ ФИО
_____ ФИО

Повестка дня

Определение информационных систем персональных данных (далее - ИСПД), принадлежащих ГБПОУ МО «УОР № 2».

1. Слушали: _____
доложил(а) исходные данные об ИСПД ГБПОУ МО «УОР № 2»

Выступил(а): _____
предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПД ГБПОУ МО «УОР №2»

Постановили:

Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС «_____».

2. Слушали: _____
доложил(а) исходные данные об ИСПД «_____».

Выступил(а): _____
предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПД «_____».

Постановили:

Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПД «Наименование».

Председатель комиссии _____ ФИО
Члены комиссии _____ ФИО
_____ ФИО
_____ ФИО

Приложение 7
к Приказу ГБПОУ МО «УОР № 2»
от «11» мая 2021 № 189

АКТ

определения уровня защищенности ПД при их обработке в ИСПД «_____» и класса защищенности ИС «_____»

Председатель комиссии _____ ФИО
Члены комиссии _____ ФИО
_____ ФИО
_____ ФИО

Рассмотрев исходные данные об информационной системе персональных данных (далее - ИСПД), комиссия определила:

– Категории персональных данных обрабатываемых в ИСПД: в информационной системе обрабатываются специальные категории персональных данных;

– Категории субъектов: персональные данные субъектов персональных данных, не являющихся сотрудниками оператора;

– Объем обрабатываемых персональных данных: менее 100 000;

– Тип актуальных угроз: для информационной системы актуальны угрозы 3-го типа;

– Уровень значимости информации: информация имеет низкий уровень значимости УЗ 3;

– Масштаб информационной системы: информационная система имеет объектовый масштаб.

Комиссия решила, 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», а так же в соответствии с приказом ФСТЭК Российской Федерации от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и на основании анализа исходных данных, необходимо обеспечить третий уровень защищенности (УЗ 3) персональных данных и установить третий класс защищенности информационной системы (К3).

Результат оценки вреда:

Для информационной системы актуальны угрозы 3-го типа.

Уровень значимости информации определен степенью возможного ущерба для обладателя информации от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации, руководствуясь следующей формулой:

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)], где степень возможного ущерба определяется обладателем информации.

Комиссия утвердила следующее:

УЗ = [(конфиденциальность, низкая степень ущерба) (целостность, низкая степень ущерба) (доступность, низкая степень ущерба)] – таким образом, комиссия установила низкий уровень значимости (УЗ 3) (возможны незначительные негативные последствия).

Председатель комиссии _____ ФИО
Члены комиссии _____ ФИО
_____ ФИО
_____ ФИО

«__»_____2021 г.

Приложение 8
к Приказу ГБПОУ МО «УОР № 2»
от «11» мая 2021 № 189

АКТ
об уничтожении персональных данных субъектов персональных данных ГБПОУ МО «УОР № 2»

Комиссия в составе:

Роль	ФИО	Должность
Председатель		
Члены комиссии		

Установила, что на основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» гл. 2, ст. 5, пункт 7, подлежат уничтожению сведения, составляющие персональные данные:

№ п/п	Сведения, содержащие персональные данные	Место хранения	Кол-во ед. хранения	Примечание

Указанные персональные данные уничтожены путем_____ _____
(удаления с помощью средств гарантированного удаления информации, уничтожения носителя и т.п.)

Председатель комиссии: _____ _____
подпись расшифровка

Члены комиссии: _____ _____
подпись расшифровка

_____ _____
подпись расшифровка