Отдел организации образования
муниципального образования «Город Новодвинск»
муниципальное образовательное учреждение
«Средняя общеобразовательная школа № 2 им.В.И.Захарова»
(МОУ «СОШ №2 им.В.И.Захарова»)

ПРИКАЗ

26 декабря 2024 г. № 01-03/254

О назначении ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных«Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова»

Во исполнение требований Федерального закона 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»

ПРИКАЗЫВАЮ:

1. Назначить Харькова М.А., лаборант, технический специалист, ответственным за обеспечение безопасности персональных данных (администратором безопасности) в информационной системе персональных данных «Подключение к ЛК ППЭ».
2. Утвердить Инструкцию администратора безопасности информационной системы персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова» (Приложение).
3. Документоведу Мокеевой Л.В.:

- предусмотреть наличие в должностной инструкции Сверлову В.В., учитель, руководитель ППЭ-96, выполнение обязанностей ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных «Подключение к ЛК ППЭ»;
- организовать ознакомление с приказом ответственного за организацию обработки персональных данных Ковалеву О.А., заместитель директора по УВР, ответственного за организацию обработки персональных данных, администратора безопасности информационной системы персональных данных «Подключение к ЛК ППЭ» Харькова М.А. лаборант, технический специалист;
- довести содержание пункта 1 настоящего приказа до работников МОУ «СОШ №2 им.В.И.Захарова», осуществляющих обработку персональных данных в информационной системе персональных данных «Подключение к ЛК ППЭ» согласно перечню лиц, доступ которых к персональным данным, обрабатываемым в информационной системе персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова» необходим для выполнения ими служебных (трудовых) обязанностей.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор МОУ «СОШ № 2 им.В.И.Захарова» Т.А. Кривоногова

С приказом ознакомленны и согласнны:

Дата	Подпись	Расшифровка
		Харьков М.А.
		Мокеева Л.В.

Приложение
к приказу МОУ «СОШ №2 им.В.И.Захарова»
от 26 декабря 2024 г. № 01-03/254

Инструкция администратора безопасности информационной системы персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова»

1. Общие положения

1.1. Инструкция администратора безопасности информационной системы персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова» (далее - Инструкция) определяет в муниципальном образовательном учреждении «Средняя общеобразовательная школа №2 им.В.И.Захарова» (далее – МОУ «СОШ №2 им.В.И.Захарова») обязанности, права и ответственность работника, назначенного ответственным за обеспечение безопасности персональных данных (далее - администратор безопасности) в информационной системе персональных данных «Подключение к ЛК ППЭ».

1.2. В своей деятельности администратор безопасности информационной системы персональных данных (далее – ИСПДн) руководствуется законодательством Российской Федерации, иными нормативными правовыми актами Российской Федерации сфере обработки и защиты персональных данных, локальными актами МОУ «СОШ №2 им.В.И.Захарова»), а также настоящей Инструкцией.

1.3. Администратор безопасности ИСПДн «Подключение к ЛК ППЭ» назначается приказом МОУ «СОШ №2 им.В.И.Захарова» и обеспечивает в пределах своих функциональных обязанностей безопасность информации, обрабатываемой, передаваемой и хранимой в информационной системе персональных данных «Подключение к ЛК ППЭ».

2. Обязанности администратора безопасности

Администратор безопасности ИСПДн «Подключение к ЛК ППЭ» при эксплуатации ИСПДн обязан:

2.1 Соблюдать требования законодательных и нормативных документов по обеспечению безопасности персональных данных, обрабатываемой в ИСПДн.

2.2 Выполнять и принимать меры к выполнению требований организационно-распорядительной документации по организации обработки и защиты персональных данных в ИСПДн.

2.3 Осуществлять установку, настройку и сопровождение технических средств защиты ИСПДн;

2.4. Осуществлять организационное и техническое обеспечение процессов создания, использования, изменения и прекращения действия персональных идентификаторов и паролей доступа в ИСПДн, контроль действий пользователей ИСПДн при их работе с персональными идентификаторами и паролями доступа в соответствии с «Инструкцией по идентификации и аутентификации пользователей информационной системы персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова»;

– создавать, присваивать, уничтожать персональные идентификаторы и пароли доступа к техническим средствам и информационным ресурсам ИСПДн;

– хранить, выдавать, инициализировать, блокировать средства аутентификации (пароли, аппаратные идентификаторы) и принимать меры в случае утраты или компрометации средств аутентификации;

– вести, надежно хранить и в установленном порядке уничтожать Журнал учета выдачи первичных паролей информационной системы персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова»;

– надежно хранить и вести учет аппаратных средств аутентификации по Журналу учета аппаратных средств аутентификации МОУ «СОШ №2 им.В.И.Захарова»;

– надежно хранить и в установленном порядке уничтожать Журнал учета аппаратных средств аутентификации МОУ «СОШ №2 им.В.И.Захарова»;

– обеспечивать смену паролей пользователей с периодичностью не реже одного раза в 90 дней с момента очередной смены и изменять свой собственный пароль не реже 1 раза в месяц. Принимать меры по обеспечению внеплановой смены паролей в случае их компрометации или утере индивидуальных аппаратных идентификаторов;

– сообщать ответственному за организацию обработки ПДн о инцидентах, связанных с компрометацией или утерей паролей, аппаратных идентификаторов;

– выявлять и пресекать действия пользователей, которые могут привести к компрометации паролей и (или) утрате аппаратных идентификаторов.

2.5. Осуществлять и контролировать разграничение доступа пользователей к ресурсам и информации ИСПДн путем настройки программно-технических средств и средств защиты информации в соответствии с «Инструкцией по управлению доступом к информационной системе персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова»:

– управлять учетными записями (заведение, активацию, блокирование, уничтожение), в том числе осуществлять блокирование учетной записи при превышении времени неиспользования более 90 дней, в случае достижения установленного максимального количества неуспешных попыток аутентификации в течение не более 30 минут (максимальное количество неуспешных попыток аутентификации до блокировки до 5 попыток), блокирование сеанса доступа в ИСПДн после установленного времени бездействия (неактивности) пользователя 30 минут или по его запросу;

– обеспечивать актуальность, сохранность и конфиденциальность матрицы доступа к ресурсам ИСПДн, утвержденной приказом МОУ «СОШ №2 им.В.И.Захарова»;

– вести учет технических средств удаленного доступа (в случае использования удаленного доступа через сеть Интернет к ресурсам ИСПДн) с документальным оформлением в Журнале учета разрешенных средств удаленного доступа в МОУ «СОШ №2 им.В.И.Захарова», а также осуществлять выдачу, хранение технических средств удаленного доступа, установку и настройку программного обеспечения, его обновление, антивирусную защиту технических средств удаленного доступа и контролировать использование технических средств удаленного доступа к ИСПДн;

– вести учет мобильных технических средств (в случае использования мобильных технических средств для доступа к ресурсам ИСПДн) с документальным оформлением в Журнале учета разрешенных мобильных технических средств в МОУ «СОШ №2 им.В.И.Захарова» и контролировать использование мобильных технических средств для доступа к ИСПДн.

2.6. Вести учет, хранение и выдачу машинных носителей персональных данных в соответствии с «Инструкцией по защите машинных носителей персональных данных в МОУ «СОШ №2 им.В.И.Захарова», в том числе:

– организовывать и контролировать процедуру уничтожения (стирания) или обезличивания персональных данных при передаче между пользователями, в сторонние организации для ремонта или утилизации, а также факт уничтожения машинного носителя информации;

– участвовать в составе комиссии по проверке наличия и состояния машинных носителей информации;

– в случае выхода из строя, порчи или утраты машинного носителя персональных данных докладывать об инциденте ответственному за организацию обработки ПДн.

2.7. Контролировать проведение резервного копирования технических средств ИСПДн (при организации).

2.8. Осуществлять настройку журналов регистрации событий информационной безопасности в программном обеспечении ИСПДн и средств защиты информации в части касающейся, фиксировать информацию о событиях безопасности в ИСПДн, не подлежащую автоматической регистрации в Журнале событий информационной безопасности информационной системы персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова» в соответствии с «Инструкцией по управлению событиями информационной безопасности информационной системы персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова».

Вести, надежно хранить Журнал событий информационной безопасности информационной системы персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова».

2.9. Осуществлять установку, конфигурирование и управление средствами антивирусной защиты ИСПДн в соответствии с «Инструкцией по антивирусной защите информационной системы персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова», в том числе:

- установку и обновление лицензионных ключей средств антивирусной защиты, обновлений базы признаков вредоносных компьютерных программ (вирусов);

- принимать меры по локализации и удалению вредоносного ПО, выявлению источника и способа проникновения вредоносного ПО;

- восстановление работоспособности программных средств и информационных массивов программных средств, поврежденных вредоносным ПО;

- ограничение доступа пользователей на АРМ к настройкам установленных средств антивирусной защиты;

- контроль над работой пользователей ИСПДн по применению на непосредственных АРМ средств антивирусной защиты;

- немедленно оповещать ответственного за организацию обработки ПДн об обнаружении вредоносного ПО на серверном или телекоммуникационном оборудовании.

2.10. Осуществлять исполнение мероприятий по выявлению (поиску), анализу и устранению уязвимостей в ИСПДн (с разработкой Плана устранения выявленных уязвимостей) в соответствии с «Инструкцией по контролю (анализу) защищенности персональных данных информационной системы персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова»:

- осуществлять мониторинг наличия обновлений, выпускаемых разработчиками ПО используемого в ИСПДн и СЗИ в части касающейся;

- проводить обновление ПО средств защиты информации, ПО аппаратных средств в случае выявления уязвимостей, связанных с устаревшими версиями ПО;

- проводить оценку изменений в ПО на условия изменения конфигурации ИСПДн и СЗИ в соответствии с «Порядком по управлению изменениями в конфигурации информационной системы персональных данных «Подключение к ЛК ППЭ» и системы защиты персональных данных в МОУ «СОШ №2 им.В.И.Захарова» выполнять необходимые настройки, проводить тестирование работоспособности после установки обновлений ПО и вносить необходимые изменения в эксплуатационную документацию;

- проводить контроль установки обновлений ПО (проводить проверку соответствия версии общесистемного, прикладного и специального ПО, установленного в ИСПДн, а также ПО средств защиты информации и выпущенного разработчиком, наличия отметок в Техническом паспорте и в эксплуатационной документации);

- не реже 1 раза в полгода проводить контроль на соответствие Техническому паспорту ИСПДн состава технических средств, ПО и средств защиты информации.

- осуществлять проверку наличия и сроков действия лицензий на установленное ПО ИСПДн и ПО СИЗ, сертификатов соответствия на примененные в ИСПДн и СЗИ аппаратные средства;- ежемесячно проводить контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

- немедленно уведомлять ответственного за организацию обработки ПДн при получении информации о прекращении поддержки разработчиком используемого ПО в части выпуска обновлений безопасности, либо о планируемом прекращении такой поддержки;

- проводить проверку технического состояния аппаратных средств, журналов планово-профилактического обслуживания аппаратных средств ИСПДн за период контроля защищенности ИСПДн, перечня событий информационной безопасности за период контроля, связанных с отказами и неисправностями аппаратных средств, конфигурацию соединений и установки аппаратных средств, условия их эксплуатации;

- осуществлять контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ, в случае выявления сбоев, отказов или несоответствия настройкам, организовывать восстановление ПО и СЗИ;

- участвовать в организованной ответственным за организацию обработки ПДн проверке состояния и актуальности организационно-распорядительной документации по защите ПДн, обрабатываемых в ИСПДн

2.11. Контролировать выполнение требований к размещению устройств вывода информации в контролируемых зонах, расположение технических устройств и физический доступ к ним в соответствии с «Инструкцией по защите технических средств информационной системы персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова».

2.12.Проводить анализ планируемых изменений в конфигурацию ИСПДн и СЗПДн и принимать решение о необходимости внесения изменения в конфигурацию ИСПДн и СЗПДн, осуществлять проверку корректности изменения конфигурации и при необходимости совместно с ответственным за организацию обработки персональных данных организовать актуализацию документации по вопросам обеспечения безопасности ПДн, а также контроль эффективности обеспечения безопасности ПДн в ИСПДн.

2.13.Проводить анализ событий ИБ, подтверждать/опровергать является ли событие ИБ инцидентом ИБ, оформлять отчет об инциденте и предоставлять его

ответственному за организацию обработку ПДн и в случае необходимости пользователей ИСПДн в соответствии с «Порядком по выявлению инцидентов в информационной системе персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова» и реагированию на них».

Проводить в составе комиссии анализ выявленного инцидента ИБ.

Принимать меры по устранению последствий инцидента (проводить процедуру смены паролей пользователями, пересматривать и обновлять с учетом содержания инцидента матрицу доступа к ресурсам ИСПДн «Подключение к ЛК ППЭ» организовать переустановку ПО ИСПДн и СЗПДн с дистрибутивных носителей используемого ПО, удалять вредоносное ПО, организовать восстановление данных из резервных копий, организовать устранение уязвимостей, проверить состав конфигурации ИСПДн и СЗПДн и при необходимости восстановить конфигурацию в соответствии с эксплуатационной документацией)

Формировать Перечень мероприятий, направленных на предупреждение повторного возникновения инцидента, согласовать его с ответственным за организацию обработки ПДн.

3. Права администратора безопасности

Администратор безопасности ИСПД имеет право:

– привлекать к работам, связанным с обеспечением безопасности информации системных администраторов ИСПДн;

– требовать от пользователей ИСПДн выполнения установленной технологии обработки информации, инструкций по обеспечению информационной безопасности ИСПДн;

– докладывать ответственному за организацию обработки персональных данных о нарушениях или невыполнении пользователями требований обеспечению безопасности информации;

– вносить предложения по модернизации и совершенствованию системы защиты ПДн в МОУ «СОШ №2 им.В.И.Захарова» ответственному за организацию обработки персональных данных;

– останавливать обработку информации в ИСПДн в случаях подтвержденных нарушений установленной технологии обработки данных, приводящих к нарушению функционирования средств защиты информации.

4. Ответственность

Работники муниципального образовательного учреждения «Средняя общеобразовательная школа №2 имени В.И.Захарова» несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

ЛИСТ ОЗНАКОМЛЕНИЯ

с приказом МОУ «СОШ №2 им.В.И.Захарова» от 26 декабря 2024 г. № 01-03/254

«О назначении ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова»

№ п/п	ФИО	Должность	Дата	Подпись
1	Харьков Максим Александрович	Лаборант, технический специалист		
2	Мокеева Любовь Владимировна	Документовед		

ЛИСТ ОЗНАКОМЛЕНИЯ

с пунктом 1 приказа МОУ «СОШ №2 им.В.И.Захарова» от 26 декабря 2024 г. № 01-03/254 «О назначении ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных «Подключение к ЛК ППЭ» в МОУ «СОШ №2 им.В.И.Захарова»

№ п/п	ФИО	Должность	Дата	Подпись
1	Харьков Максим Александрович	Лаборант, технический специалист		
2	Мокеева Любовь Владимировна	Документовед		