ПРИЛОЖЕНИЕ 15
к приказу муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования - Рязанский муниципальный район Рязанской области
от «18» сентября 2020 г. № 39/1-од

ИНСТРУКЦИЯ
по работе администратора безопасности информации информационной системы персональных данных в муниципальном бюджетном общеобразовательном учреждении «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области

1. Общие положения

1.1 Администратор безопасности информации (далее - АБИ) - лицо, выполняющее функции по настройке и сопровождению всех программных и технических средств защиты информации информационной системы персональных данных, предназначенных для обработки информации, содержащей персональные данные (далее ИСПДн).

1.2 АБИ в пределах своих функциональных обязанностей обеспечивает безопасность информации, обрабатываемой, передаваемой и хранимой в ИСПДн.

1.3 АБИ назначается приказом муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области.

1.4 АБИ в своей работе руководствуется положениями нормативно - правовых актов РФ, руководящими документами по безопасности информации, актами муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области и положениями настоящей Инструкции.

2. Обязанности АБИ

Основными обязанностями АБИ являются:

- управление средствами и системами защиты информации (далее - СЗИ) информационных систем персональных данных (далее – ИСПДн) и поддержание их функционирования;
- восстановление функций программных и технических систем защиты информации (далее – СЗИ) от несанкционированного доступа (далее – НСД) к информации;
- генерация ключей, личных идентификаторов, а также паролей для пользователей автоматизированных систем (далее – АС);
- формирование и управление списком необходимых реквизитов и значением атрибутов объектов и субъектов доступа;
- обеспечение правильной эксплуатации технических и программных СЗИ в ИСПДн;
- контроль целостности эксплуатируемого в ИСПДн программного обеспечения, в том числе самих СЗИ, с целью недопущения и выявления несанкционированных модификаций;
- текущий, после сбоев и периодический (не реже 1 раза в год) контроль работоспособности средств и систем защиты информации от НСД;
- контроль соблюдения пользователями ИСПДн требований инструкций и порядка работы при обработке информации в ИСПДн, по вопросам защиты информации от НСД;
- выполнение резервного копирования машинных документов, содержащих персональные данные;
- организация антивирусной защиты информации и программных средств в ИСПДн.

3. Права АБИ

АБИ имеет право:

- Останавливать обработку информации в ИСПДн в случаях подтвержденных нарушений установленной обработки данных, приводящих к нарушению функционирования СЗИ.

4. Ответственность АБИ

4.1 На АБИ возлагается персональная ответственность за качество и полноту проводимых им работ по обеспечению защиты информации в соответствии с его функциональными обязанностями.

4.2 АБИ несет ответственность по законодательству РФ за нарушение требований нормативно - методических документов по защите информации и настоящей инструкции.

ПРИЛОЖЕНИЕ 16
к приказу муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования - Рязанский муниципальный район Рязанской области
от «18» сентября 2020 г. № 39/1-од

ИНСТРУКЦИЯ
по организации парольной защиты в информационных системах администрации муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области.

1. Общие положения

1.1. Данная инструкция по организации парольной защиты в автоматизированных рабочих местах и информационных системах (далее – ИС) муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области регламентирует процессы генерации, смены и прекращения действия паролей (удаления учётных записей пользователей) в ИС, а также контроль над действиями пользователей и обслуживающего персонала информационных систем при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей в ИС и контроль за действиями исполнителей и обслуживающего персонала информационной системы при работе с паролями возлагается на администратора информационной безопасности информационных систем и информационных систем персональных данных (далее – администратор безопасности ИС).

2. Термины и определения

2.1. Информация - сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.2. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 № 152-ФЗ «О персональных данных»).

2.3. Пароль - секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

2.4. Компрометация пароля – раскрытие, обнаружение или утеря пароля.

3. Правила формирования паролей

3.1. Личные пароли должны генерироваться и распределяться централизованно.

3.2. Ответственность за правильность формирования и распределения паролей в ИС возлагается на администратора безопасности ИС.

3.3. Ответственность за правильность формирования и распределения паролей для доступа на автоматизированные рабочие места гражданских служащих ИС возлагается на системного администратора ИС.

3.4. При ручном назначении пароля он должен соответствовать следующим параметрам:

3.5. Длина пароля должна быть не менее 6 символов.

3.6. Пароль должен содержать комбинацию букв в верхнем и нижнем регистре, а также цифры, знаки препинания и/или специальные символы (@,#, $, %, ^, &, * и т.п.).

3.7. Пароль не должен включать в себя слова, которые содержатся в словарях (русских или иностранных), имена, фамилии и отчества людей, клички животных, имена вымышленных персонажей, различные географические наименования, даты рождения, номера телефонов и другую личную информацию.

3.8. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях.

4. Порядок смены личных паролей

4.1. Смена паролей доступа в ИС должна проводиться регулярно, не реже одного раза в 60 дней, централизованно, администратором безопасности ИС.

4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетных записей доступа в ИС, а также учетные данные для доступа на автоматизированное рабочее место.

4.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за защиту персональных данных,

администратора безопасности информационных систем и других сотрудников Администрации, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

5. Хранение пароля.

5.1. Запрещается входить в ИС под учетной записью и паролем другого пользователя.

6. Действия в случае утери и компрометации пароля.

6.1. В случае подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

6.2. По факту компрометации пароля может быть проведено служебное расследование.

7. Ответственность при организации парольной защиты.

7.1. Каждый пользователь ИС несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учетной записи в ИС, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учетной записи.

7.2. Ответственность за контроль проведения мероприятий по организации парольной защиты в ИС возлагается на администратора безопасности ИС.

7.3. За разглашение информации ограниченного доступа и нарушение порядка работы с ИС, обрабатывающей информацию ограниченного доступа, сотрудники Администрации могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

ПРИЛОЖЕНИЕ 17
к приказу муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования - Рязанский муниципальный район Рязанской области
от «18» сентября 2020 г. № 39/1-од

ИНСТРУКЦИЯ

по управлению доступом к персональным данным в информационных системах персональных данных муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области

1. Введение

1.1. Настоящая инструкция предназначена для обеспечения защиты персональных данных (далее – ПДн), содержащихся в информационной системе персональных данных (далее – ИСПДн) муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области (далее - Администрация) при разграничении доступа пользователей к ресурсам и информации, содержащейся в ИСПДн.

1.2. Настоящая инструкция определяет порядок действий администратора безопасности и пользователей ИСПДн при разграничении доступа к ресурсам и информации ИСПДн.

2. Матрица доступа

2.1. Разграничение доступа к ресурсам и информации ИСПДн осуществляет и контролирует администратор безопасности путем настройки программно – технических средств и средств защиты информации (далее – СЗИ) ИСПДн на основании журнала учета выдачи паролей и матрицы доступа.

2.2. Матрица доступа к ресурсам ИСПДн Администрации утверждается распоряжением.

2.3. Сохранность, конфиденциальность и актуальность матрицы доступа обеспечивает администратор безопасности.

3. Порядок доступа без ввода пароля

3.1. Вход в ИСПДн и действия с ресурсами ИСПДн до процедур идентификации и аутентификации разрешен администратору безопасности для восстановления ИСПДн после сбоев и аварий технических средств ИСПДн. Срок действия разрешения заканчивается в момент запуска ИСПДн после восстановления.

3.2. Доступ к ресурсам ИСПДн до момента прохождения процедур идентификации и аутентификации остальным пользователям запрещен.

4. Порядок предоставления удаленного доступа

4.1. Удаленный доступ пользователей к информационным ресурсам ИСПДн возможен только с помощью технических средств (персональный компьютер, ноутбук, планшет, сотовый телефон) являющихся собственностью Администрации и внесенных в журнал разрешенных устройств удаленного доступа (приложение 1 к настоящей Инструкции).

4.2. Выдачу, учет, хранение, настройку программного обеспечения, установку программного обеспечения и его обновление, антивирусную защиту технических средств удаленного доступа осуществляет администратор безопасности. Все данные по конфигурации и настройкам должны быть записаны в журнал разрешенных устройств удаленного доступа.

4.3. При настройке средств удаленного доступа к ресурсам ИСПДн администратор безопасности осуществляет возможность удаленного доступа к ресурсам ИСПДн с автоматической аутентификацией средств удаленного доступа.

4.4. Указанные в пункте 4 требования подлежат исполнению только в случае, если предусмотрен доступ к ресурсам ИСПДн с использованием информационно-телекоммуникационной сети Интернет.

5. Порядок использования мобильных технических средств

5.1. К мобильным техническим средствам Администрации отнесены все переносные технические устройства, на которые может быть записана и с помощью которых может быть осуществлена обработка информации, содержащейся в ИСПДн.

5.2. Все мобильные технические средства Администрации должны быть учтены и идентифицированы. Учет мобильных технических средств осуществляет администратор безопасности в журнале учета разрешенных мобильных технических средств (приложение 2 к настоящей Инструкции).

5.3. При передаче мобильных технических средств на ремонт или техническое обслуживание администратор безопасности полностью очищает их от информации, имеющей отношение к ИСПДн.

5.4. Указанные в пункте 5 требования подлежат исполнению только в случае, если предусмотрен доступ к ресурсам ИСПДн с использованием мобильных технические средств.

6. Взаимодействие с внешними информационными системами (внешними пользователями)

6.1. Пользователям внешних информационных систем (внешним пользователям) доступ к ресурсам ИСПДн устанавливают в матрице доступа.

6.2. Администратор безопасности осуществляет процедуру доступа внешних пользователей к ресурсам ИСПДн в соответствии с пунктом 2 настоящей Инструкции.

7. Заключительные положения

7.1. Все пользователи ИСПДн должны быть предупреждены об ответственности за действия с получением доступа к ресурсам ИСПДн, нарушающие требования настоящей инструкции.

7.2. Пользователи ИСПДн должны быть ознакомлены с настоящей инструкцией до начала работы с ИСПДн. Обязанность ознакомления пользователей информационной системы с настоящей инструкцией лежит на администраторе безопасности.

7.3. Сотрудники Администрации несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

ПРИЛОЖЕНИЕ 1
к инструкции по управлению доступом к персональным данным в информационных системах персональных данных в муниципальном бюджетном общеобразовательном учреждении «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области

Муниципальное бюджетное общеобразовательное учреждение «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области

ЖУРНАЛ
учета разрешенных средств удаленного доступа

Учетный № _____
2_____ год. Листов (_____)

№	Наименование	Инв. №	Состояние	Пользователь	Дата выдачи/ роспись	Дата возврата/ роспись
1	2	3	4	5	6	7

ПРИЛОЖЕНИЕ 2
к инструкции по управлению доступом к персональным данным в информационных системах персональных данных муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области

Муниципальное бюджетное общеобразовательное учреждение «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области

ЖУРНАЛ
учета разрешенных мобильных технических средств

Учетный № _____
2_____ год. Листов (_____)

№	Наименование	Инв. №	Состояние	Пользователь	Дата выдачи/ роспись	Дата возврата/ роспись
1	2	3	4	5	6	7

№	Наименование	Инв. №	Состояние	Пользователь	Дата выдачи/ роспись	Дата возврата/ роспись

ПРИЛОЖЕНИЕ 18
к приказу муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования - Рязанский муниципальный район Рязанской области
от «18» сентября 2020 г. № 39/1-од

ИНСТРУКЦИЯ
по защите машинных носителей персональных данных, используемых в информационной системе персональных данных муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области

1. Введение

1.1. Настоящая инструкция определяет порядок учета, хранения, выдачи, уничтожения и ограничения использования машинных носителей информации в муниципальном бюджетном общеобразовательном учреждении «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области (далее – Администрация).

1.2. Машинный носитель информации (далее – МНИ) – это материальный носитель, используемый для передачи и хранения защищаемой информации в электронном виде, в том числе персональных данных (далее – ПДн). МНИ делятся на съемные и несъемные носители.

1.2.1. Несъемные МНИ являются частью автоматизированного рабочего места (далее – АРМ) или сервера и в процессе эксплуатации не предполагают демонтаж.

1.2.2. К съемным носителям относятся любые технические устройства, предназначенные для запоминания информации, оперативно подключаемые к АРМ или серверу в целях записи на них информации из памяти АРМ (или сервера) или считывания с них информации в память АРМ (или сервера).

2. Учет машинных носителей информации

2.1. Все используемые в информационной системе персональных данных Администрации (далее – ИСПДн) МНИ подлежат учёту.

2.2. Учет, хранение и выдачу носителей информации осуществляет администратор безопасности. При увольнении администратора безопасности составляется акт приема-сдачи учетных документов и носителей.

2.3. Учет всех видов и типов носителей информации производится в Журнале учета машинных носителей информации (Приложение №1 к настоящей Инструкции).

2.4. На несъемную часть носителей ИСПДн наносится уникальный в пределах Администрации учетный номер.

3. Выдача машинных носителей информации

3.1. Пользователи ИСПДн получают учтенный носитель от администратора безопасности, для выполнения работ на конкретный срок.

3.2. При получении пользователем носителя информации делается соответствующая запись в Журнале учета машинных носителей информации.

3.3. По окончании работ или установленного срока использования пользователь ИСПДн сдает носитель информации администратору безопасности, о чем делается соответствующая запись в Журнале учета машинных носителей информации.

4. Использование и передача машинных носителей информации

4.1. На МНИ записываются исключительно ПДн и программные средства обработки ПДн, содержащихся в ИСПДн.

4.2. Носители информации, допускающие повторную запись информации, проходят процедуру многократной перезаписи общедоступной информации перед повторным использованием или ремонтом с

целью гарантированного уничтожения остаточной информации. Процедуру перезаписи организует и контролирует администратор безопасности.

4.3. ПДн, используемые в различных целях, записываются на разные носители.

4.4. Вынос учтенных носителей информации за пределы установленных мест обработки ПДн допустим только с письменного разрешения ответственного за организацию обработки ПДн.

4.5. Передача носителей, содержащих ПДн, которые обрабатываются в ИСПДн сторонним организациям или третьим лицам производится через администратора безопасности. Администратор безопасности производит в этом случае необходимые отметки в Журнале учета машинных носителей информации.

5. Хранение машинных носителей информации

5.1. Хранение МНИ осуществляется в условиях, препятствующих несанкционированному ознакомлению с информацией, копированию, изменению или уничтожению информации, содержащейся на машинных носителях.

5.2. МНИ хранятся в служебных помещениях, в отведенных для этих целей хранилищах, исключающих несанкционированный доступ к ним.

5.3. ЗАПРЕЩАЕТСЯ хранить носители информации на рабочих столах, оставлять их без присмотра, передавать на хранение третьим лицам.

6. Действия при утрате или порче машинных носителей информации

6.1. В случае утраты или порчи пользователем МНИ, содержащих ПДн, которые обрабатываются в ИСПДн, немедленно ставится в известность администратор безопасности. Администратор безопасности вносит соответствующую запись в Журнал учета машинных носителей информации и докладывает об инциденте ответственному за организацию обработки ПДн.

6.2. По факту утраты или порчи МНИ ответственным за организацию обработки ПДн проводится служебное расследование в установленном порядке.

6.3. Носители, пришедшие в негодность или с истекшим сроком эксплуатации, подлежат уничтожению в установленном порядке.

7. Уничтожение машинных носителей информации

7.1. Уничтожение МНИ организует администратор безопасности с предоставлением Акта уничтожения машинных носителей информации (ПРИЛОЖЕНИЕ 2 к настоящей Инструкции) ответственному за организацию обработки ПДн. Акт подписывает администратор безопасности.

7.2. Уничтожение носителей информации производится способом, гарантирующим невозможность восстановления информации, содержавшейся на носителе. Такими способами являются: механическое, электрическое, электромагнитное, химическое или термическое воздействие на носитель, применение специального программного обеспечения для уничтожения информации на носителе. Способ уничтожения выбирается администратором безопасности в зависимости от типа носителя и возможностей Администрации.

8. Ограничения и ответственность

8.1. Всем пользователям ИСПДн запрещено использовать учтенные МНИ для личных целей.

8.2. Пользователям ИСПДн запрещено передавать носители информации кому-либо, осуществлять учет, хранение и выдачу носителей информации, обрабатываемой в ИСПДн. Передача носителей информации осуществляется в порядке, предусмотренном пунктами 4.5, 4.6 настоящей Инструкции.

8.3. Любое взаимодействие (чтение, запись информации, запуск программного обеспечения) между техническими средствами ИСПДн, СЗИ и неучтенными носителями информации запрещено.

8.4. В случае выявления фактов утраты, несанкционированного и (или) нецелевого использования учтенных носителей информации, использования неучтенных (личных) носителей информации в ИСПДн назначается служебное расследование. По результату расследования и по представлению ответственного за организацию обработки ПДн, директор муниципального бюджетного общеобразовательного учреждения «Искровская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области принимает решение о привлечении пользователя ИСПДн к ответственности согласно нормативным актам Администрации и действующему законодательству.

8.5. Сотрудники Администрации, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации.

9. Заключительные положения

9.1. Пользователи ИСПДн должны быть предупреждены об ответственности за невыполнение требований настоящей Инструкции и ознакомлены с Инструкцией до начала работы в ИСПДн.

9.2. Обязанность ознакомления пользователей ИСПДн с настоящей Инструкцией лежит на ответственном за организацию обработки ПДн.

ПРИЛОЖЕНИЕ 1
к инструкции по защите машинных носителей персональных данных, используемых в информационной системе персональных данных муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области.

Муниципальное бюджетное общеобразовательное учреждение «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области

ЖУРНАЛ
учета машинных носителей персональных данных

Учетный № _____20_____ год.

Листов (_____)

Учетный / заводской номер	Наименование (марка) носителя	Вид носителя (съемный /несъемный)	Цель обработки хранимых ПДн	Место установки (для несъемных носителей)	Ф.И.О. лица, эксплуатирующего носитель	Дата получения съемного носителя и подпись	Дата возврата съемного носителя и подпись администратора	Отметка об уничтожении носителя
1	2	3	4	5	6	7	8	9

ПРИЛОЖЕНИЕ 2
к инструкции по защите машинных носителей
персональных данных, используемых в
информационной системе персональных данных
муниципального бюджетного общеобразовательного
учреждения «Полянская средняя школа»
муниципального образования – Рязанский
муниципальный район Рязанской области

АКТ
уничтожения носителей персональных данных

Комиссия, назначенная указанием муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области, в составе:

Председателя комиссии _____

и членов комиссии _____
_____

настоящим актом подтверждает, что:

1. _____
(наименование цифровых носителей ПДн их серийные номера и номера в журнале учета носителей)
_____

2. _____
(наименование цифровых носителей ПДн их серийные номера и номера в журнале учета носителей)
_____

3. _____
(наименование цифровых носителей ПДн их серийные номера и номера в журнале учета носителей)
_____

4. _____
(наименование цифровых носителей ПДн их серийные номера и номера в журнале учета носителей)
_____

уничтожены по причине их неработоспособности в кабинете №__ путем разрушения их целостности "____" _____ 20__ г.

Председатель комиссии

_____ _____
(подпись) (инициалы, фамилия)

Члены комиссии

_____ _____
(подпись) (инициалы, фамилия)

_____ _____
(подпись) (инициалы, фамилия)

АКТ
уничтожения персональных данных муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области.

«____« _____20 г.

Председатель комиссии _____

Член комиссии: _____ (Ф.И.О.)

_____ (Ф.И.О.)

составили настоящий акт в том, что «____» _____ 20___ г. произведено уничтожение персональных данных, находящейся на _____

_____ (наименование носителя персональных данных, Ф.И.О. ответственного

_____ способ уничтожения информации)

Председатель комиссии: _____ (подпись)

Член комиссии: _____ (подпись)

ПРИЛОЖЕНИЕ 19
к приказу муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» администрации муниципального образования - Рязанский муниципальный район Рязанской области
от «18» сентября 2020 г. № 39/1-од

Инструкция
ответственного пользователя средств криптографической защиты информации в муниципальном бюджетном общеобразовательном учреждении «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области

1. Общие положения

1.1. Настоящая Инструкция ответственного пользователя средств криптографической защиты информации (далее – Инструкция) муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области (далее – Администрация) определяет основные обязанности и права ответственного пользователя средств криптографической защиты информации.

1.2. Ответственный пользователь средств криптографической защиты информации директором муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области и отвечает за организацию, обеспечение функционирования и безопасности средств криптографической защиты информации (далее - СКЗИ), предназначенных для защиты персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн).

1.3. Ответственный пользователь СКЗИ должен знать нормативные акты Российской Федерации и Рязанской области, методические материалы в сфере обработки персональных данных, в том числе распорядительные документы Администрации в сфере обработки персональных данных.

1.4. В своей деятельности, связанной с обработкой персональных данных, ответственный пользователь СКЗИ руководствуется настоящей Инструкцией.

2. Обязанности ответственного пользователя СКЗИ

Ответственный пользователь СКЗИ обязан:

2.1. Соблюдать требования Нормативных актов, устанавливающих порядок работы с персональными данными.

2.2. Осуществлять текущий контроль за организацией, обеспечением функционирования и безопасности СКЗИ, предназначенных для защиты персональных данных при их обработке в информационных системах персональных данных:

- контролировать соблюдение условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией к ним;
- обеспечивать надежное хранение эксплуатационной и технической документации к СКЗИ, ключевых документов, носителей информации ограниченного распространения;
- вносить предложения по режиму охраны помещений, в которых установлены СКЗИ или хранятся ключевые документы к ним;
- вести Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (далее - Журнал);
- выдавать пользователям СКЗИ экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов под расписку в соответствующем Журнале;
- контролировать передачу СКЗИ, эксплуатационной и технической документации к ним, ключевых документов между пользователями СКЗИ и (или) ответственным пользователем СКЗИ под расписку в соответствующем Журнале;
- пломбировать (опечатывать) и контролировать сохранность печатей (пломб) на аппаратных средствах, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратных и аппаратно-программных СКЗИ;
- контролировать получение и доставку СКЗИ, эксплуатационной и технической документации к ним;
- заблаговременно делать заказы на изготовление очередных ключевых документов и рассылку на места использования для своевременной замены действующих ключевых документов;
- контролировать уничтожение неиспользованных или выведенных из действия ключевых документов в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ, или, если срок

уничтожения эксплуатационной и технической документацией не установлен, не позднее 10 суток после вывода их из действия (окончания срока действия) под расписку в соответствующем Журнале;

- выводить из действия носители ключевой информации (далее - НКИ), в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие НКИ;

- принимать решение в чрезвычайных случаях, когда отсутствуют НКИ для замены скомпрометированных, об использовании скомпрометированных НКИ;

- проводить инструктаж пользователей СКЗИ по правилам работы с СКЗИ и ключевыми документами.

2.3. Требовать прекращения обработки персональных данных в случае нарушения установленного порядка работ с СКЗИ или нарушения функционирования СКЗИ.

2.4. Участвовать в анализе ситуаций, касающихся нарушения условий хранения носителей персональных данных, использования СКЗИ, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

2.5. Контролировать исполнение пользователями СКЗИ требований нормативных актов в части обеспечения защиты персональных данных с помощью СКЗИ.

2.6. Принимать все необходимые меры для обеспечения безопасности персональных данных, в случае получения от пользователей СКЗИ информации о фактах утраты, компрометации ключевой информации, в частности, обеспечить выполнение следующих мероприятий:

- в каждом случае, по факту (или предполагаемой) компрометации ключевых документов, проводится служебное расследование; результатом расследования является квалификация или не квалификация данного события как компрометация;

- о факте компрометации ключевой информации пользователями СКЗИ совместно с ответственным пользователем СКЗИ производится информирование всех заинтересованных участников информационного обмена;

- выведенные из действия скомпрометированные ключевые документы после проведения расследования уничтожаются, о чем делается соответствующая запись в Журнале;

- для своевременного восстановления связи пользователю СКЗИ выдается новый НКИ; для этого создается резервный запас НКИ, использование которых осуществляется в случаях крайней необходимости по решению ответственного пользователя СКЗИ.

2.7. Подготавливать копии НКИ, которые подлежат основному учету и хранятся в сейфе ответственного пользователя СКЗИ. Данные копии применяются с разрешения ответственного за обработку персональных данных, если по результатам расследования не было установлено факта компрометации.

2.8. Хранить резервные НКИ отдельно от рабочих (актуальных) НКИ, с целью обеспечения невозможности их одновременной компрометации.

2.9. Своевременно информировать ответственного за обработку персональных данных о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

3. Права ответственного пользователя СКЗИ

Ответственный пользователь СКЗИ имеет право:

3.1. Знакомиться с Нормативными актами, регламентирующими процессы обработки персональных данных.

3.2. Требовать от пользователей СКЗИ соблюдения требований Нормативных актов в части обеспечения защиты информации с помощью СКЗИ.

3.3. Требовать прекращения работы в ИСПДн, как в целом, так и отдельных пользователей СКЗИ, в случае выявления нарушений требований по работе с СКЗИ, предназначенными для обеспечения безопасности персональных данных, или в связи с нарушением функционирования СКЗИ.

ПРИЛОЖЕНИЕ 20
к приказу муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования - Рязанский муниципальный район Рязанской области
от «18» сентября 2020 г. № 39/1-од

Инструкция пользователя средств криптографической защиты информации в муниципальном бюджетном общеобразовательном учреждении «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области

1. Общие положения

1.1. Настоящая Инструкция пользователя средств криптографической защиты информации (далее - Инструкция) в муниципальном бюджетном общеобразовательном учреждении «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области (далее - Администрация) определяет права и обязанности пользователя средств криптографической защиты информации, порядок обращения с криптографическими средствами защиты информации (далее - СКЗИ), а также определяет порядок восстановления связи в случае компрометации действующих ключей к СКЗИ.

1.2. Пользователем СКЗИ является сотрудник Администрации, включенный в перечень сотрудников, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности персональных данных в информационных системах персональных данных, утвержденный главой Администрации.

1.3. Пользователь СКЗИ должен знать нормативные акты Российской Федерации и Рязанской области, методические материалы в сфере обработки персональных данных, в том числе распорядительные документы Администрации в сфере обработки персональных данных (далее - Нормативные акты).

1.4. В своей деятельности, связанной с обработкой персональных данных, пользователь СКЗИ руководствуется настоящей Инструкцией.

1.5. Пользователи СКЗИ несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту СКЗИ от несанкционированного использования.

2. Обязанности и права пользователя СКЗИ

2.1. Пользователь СКЗИ обязан:

- соблюдать требования по обеспечению безопасности функционирования СКЗИ;
- обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей;
- сдать ответственному пользователю СКЗИ Администрации (далее - Ответственный) носители ключевой информации (далее - НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- сдать Ответственному НКИ по окончании срока действия сертификата ключа, а также в случае компрометации ключа;
- немедленно уведомлять руководителя структурного подразделения или Ответственного о компрометации НКИ, о фактах утраты или недостачи СКЗИ;
- в пределах своей компетенции предоставлять информацию комиссии, проводящей служебные расследования по фактам компрометации, а также выявлению причин нарушения требований безопасности функционирования СКЗИ.

2.2. Пользователю СКЗИ запрещается:

- осуществлять несанкционированное и безучетное копирование ключевых данных;
- хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность;
- передавать НКИ каким бы то ни было лицам, кроме Ответственного;
- во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ);
- хранить на НКИ какую-либо информацию, кроме ключевой;
- использовать в помещениях, где применяются СКЗИ, личные технические средства, позволяющие осуществлять копирование ключевой информации;
- использовать НКИ, выведенные из действия.

2.3. Пользователь имеет право:

- вносить предложения по вопросам использования СКЗИ;
- повышать уровень квалификации по использованию СКЗИ.

3. Порядок обращения с СКЗИ

3.1. Монтаж и установка СКЗИ осуществляются органом криптографической защиты, назначенным главой муниципального образования.

3.2. Служебные помещения, в которых размещаются СКЗИ, должны отвечать всем требованиям по оборудованию и охране, предъявляемым к помещениям, выделенным для работы с конфиденциальной информацией. Для хранения НКИ помещения обеспечиваются сейфами (металлическими шкафами и по убытии сотрудников закрываются и опечатываются личными печатями ответственных лиц.

3.3. Пользователи СКЗИ хранят инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.4. К эксплуатации СКЗИ допускаются лица, прошедшие инструктаж и изучившие правила пользования данным СКЗИ.

3.5. Все программное обеспечение ПЭВМ, предназначенной для установки СКЗИ, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую СКЗИ, не допускается.

4. Восстановление связи в случае компрометации действующих ключей к СКЗИ

4.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию владельца НКИ и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

- утрата (хищение) НКИ, в том числе - с последующим их обнаружением;
- увольнение (переназначение) сотрудников, имевших доступ к НКИ;
- передача секретных ключей по линии связи в открытом виде;
- нарушение правил хранения НКИ;
- вскрытие фактов утечки передаваемой информации или ее искажения (подмены, подделки);
- ошибки при совершении криптографических операций;
- несанкционированное или безучетное копирование ключевой информации;
- все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда НКИ вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

4.2. При наступлении любого из перечисленных выше событий пользователь СКЗИ или владелец НКИ должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) Ответственному лично, по телефону, электронной почте или другим доступным способом. В любом случае пользователь СКЗИ или владелец НКИ обязан убедиться, что его сообщение получено и прочтено.

4.3. При подтверждении факта компрометации действующих ключей пользователь СКЗИ обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей и сдачу Ответственному в течение 3 рабочих дней.

4.4. Для восстановления конфиденциальной связи после компрометации действующих ключей пользователь СКЗИ получает у Ответственного новые ключи.

ПРИЛОЖЕНИЕ 21
к приказу муниципального бюджетного
общеобразовательного учреждения «Полянска
средняя школа» муниципального образования -
Рязанский муниципальный район Рязанской област

от «18» мая 2020 г. № 59/1-Р

Муниципальное бюджетное общеобразовательное учреждение «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области

Журнал поэкземплярного учета средств защиты информации

Учетный № _____20_____ год.

Листов (_____)

№ п/п	Наименование СЗИ	Серийные номера СЗИ	Номера экземпляров	Отметка о получении	Владелец сертификата, срок действия	Отметка о выдаче	Отметка о подключении (установке) СКЗИ	Отметка об изъятии СЗИ	Примечание
				От кого получены \ Дата и номер сопроводительного письма		Ф.И.О. пользователя СКЗИ \ Дата и расписка в получении	Ф.И.О.\ Дата подключения \ Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения) \ Ф.И.О. \ Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10

№ п/п	Наименование СЗИ	Серийные номера СЗИ	Номера экзем-пляров	Отметка о получении	Владелец сертификата, срок действия	Отметка о выдаче	Отметка о подключении (установке) СКЗИ	Отметка об изъя-тии СЗИ	Приме-чание
				От кого получены \ Дата и номер сопро-водительного письма		Ф.И.О. пользователя СКЗИ \ Дата и рас-писка в получении	Ф.И.О.\ Дата подключения \ Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничто-жения) \ Ф.И.О. \ Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10

ПРИЛОЖЕНИЕ 22
к приказу муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования - Рязанский муниципальный район Рязанской области
от «18» сентября 2020 г. № 39/1-од

РУКОВОДСТВО

администратора информационной системы муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее руководство определяет права и обязанности администратора информационной системы (далее – администратор ИС), ответственного за эксплуатацию информационной системы (далее – ИС).

1.1. Администратор ИС назначается приказом директора муниципального бюджетного общеобразовательного учреждения «Искровская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области (далее – Администрация) и подчиняется непосредственно главе муниципального образования.

1.2. Администратор ИС отвечает за обеспечение возможности эксплуатации ИС.

1.3. Требования администратора ИС, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями ИС.

1.4. Администратор ИС несет персональную ответственность за качество проводимых им работ по администрированию ИС, состояние и поддержание уровня защищенности информации, содержащейся в ИС.

2. ЗАДАЧИ АДМИНИСТРАТОРА ИС

2.1. Основными задачами администратора ИС являются:

– обеспечение возможности эксплуатации ИС;

– администрирование ИС.

2.2. В рамках выполнения основных задач администратор ИС осуществляет:

– создание учётных записей пользователей ИС;

– контроль за событиями безопасности и действиями администратора безопасности и пользователей ИС;

– контроль выполнения пользователями ИС мероприятий по обеспечению безопасности информации ИС;

– методическую помощь пользователям ИС.

3. ОБЯЗАННОСТИ АДМИНИСТРАТОРА ИС

3.1. Администратор ИС обязан:

– знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в ИС, в том числе содержащих персональные данные (далее – ПДн);

– осуществлять общее руководство деятельности по обработке информации в ИС, в том числе содержащих ПДн;

– участвовать в разработке организационно-распорядительной документации по вопросам обеспечения безопасности информации, содержащейся в ИС;

– анализировать состояние работоспособности и защищённости ИС;

– контролировать правильность функционирования прикладного программного обеспечения ИС и неизменность его настроек;

– контролировать исполнение пользователями ИС введенного режима безопасности, а также правильность работы с элементами ИС;

– периодически анализировать журналы учета событий безопасности, регистрируемых прикладным программным обеспечением ИС, с целью контроля действий пользователей и выявления возможных нарушений;

– контролировать выполнение администратором безопасности и пользователями ИС своих обязанностей;

– периодически представлять главе Администрации отчет о состоянии ИС и о нештатных ситуациях и допущенных пользователями и администратором безопасности нарушениях установленных требований по защите информации;

– в случае выявления нарушений режима безопасности информации (в том числе ПДн), а также возникновения внештатных и аварийных ситуаций, принимать необходимые меры с целью ликвидации их последствий и определению причин их появления;

– принимать участие в проведении работ по оценке ИС требованиям безопасности информации.

4. ПРАВА АДМИНИСТРАТОРА ИС

4.1. Администратор ИС имеет право:

– давать пользователям ИС обязательные для исполнения указания и рекомендации по вопросам безопасной эксплуатации прикладного программного обеспечения ИС;

– проводить служебные расследования по фактам нарушений установленных требований обеспечения информационной безопасности (далее – ИБ), несанкционированного доступа (далее – НСД), утраты, порчи защищаемой информации и технических средств ИС;

– организовывать и участвовать в любых проверках по использованию пользователями ИС;

– запрещать устанавливать на автоматизированных рабочих местах нештатное программное и аппаратное обеспечение;

– запрашивать и получать от главы Администрации материалы, необходимые для организации своей работы;

– вносить на рассмотрение главы Администрации предложения по улучшению состояния ИБ, по замене вышедших из строя элементов системы защиты информации ИС, а также по выведению из эксплуатации машинных носителей персональных данных, у которых закончился период эксплуатации, установленный их производителем.

5. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА ИС

5.1. Администратор ИС несет ответственность:

– за организацию безопасной эксплуатации ИС;

– за выполнение установленных условий функционирования ИС;

– за качество выполнения обязанностей, установленных настоящей Инструкцией;

– за качество проводимых работ по контролю действий администратора безопасности и пользователей ИС, состояние и поддержание необходимого уровня защиты информационных и технических ИС;

– за качество и состояние организационно-распорядительной и эксплуатационной документации по вопросам эксплуатации ИС;

– за разглашение сведений ограниченного доступа (ПДн, иная защищаемая информация), ставших известными ему по роду работы.

ОЗНАКОМЛЕНЫ:

(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*

ПРИЛОЖЕНИЕ 23
к приказу муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования - Рязанский муниципальный район Рязанской области
от «18» сентября 2020 г. № 39/1-од

РУКОВОДСТВО

пользователя информационной системы муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее руководство определяет права и обязанности Пользователя информационной системы муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области (далее – пользователь ИС), ответственного за эксплуатацию информационной системы муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области (далее - ИС).

1.1. Пользователи ИС (в том числе внешние пользователи) назначаются администрацией муниципального бюджетного общеобразовательного учреждения «Полянская средняя школа» муниципального образования – Рязанский муниципальный район Рязанской области (далее – Администрация).

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ИС

2.1. Пользователи ИС обязаны знать и выполнять требования законодательства РФ, законодательства Рязанской области, распоряжений и постановлений Правительства Рязанской области, нормативных актов Администрации, устанавливающих правила обработки и защиты информации в ИС, в том числе содержащих персональные данные (далее – ПДн).

2.2. При эксплуатации ИС с целью защиты информации, в том числе ПДн, пользователь ИС обязан:

– руководствоваться требованиями организационно – распорядительной документации по организации обработки и защиты информации в ИС;

– соблюдать установленную технологию обработки и защиты информации;

– использовать для записи информации ИС только съемные носители информации, учтенные в установленном порядке;

– использовать для вывода на печать документов, содержащих информацию, находящуюся в ИС, только устройства печати, расположенные в пределах установленных контролируемых зон, сводя к минимуму возможность доступа к ним посторонних лиц.

2.3. Пользователь должен свести к минимуму возможность неконтролируемого доступа к средствам вычислительной техники (далее – СВТ) ИС посторонних лиц, а также возможность просмотра посторонними лицами ведущихся на СВТ работ. В случаях кратковременного отсутствия (перерыв, обед) при выходе в течение рабочего дня из помещения, в котором размещаются СВТ ИС, пользователь обязан блокировать ввод-вывод информации на своем рабочем месте или выключить СВТ. Защищаемые носители информации должны быть убраны в запираемые хранилища, определенные в установленном порядке для этих целей.

2.4. Пользователь обязан докладывать администратору безопасности ИС и своему непосредственному руководителю (для сотрудников Администрации):

– о фактах имевшегося или предполагаемого несанкционированного доступа к информации, носителям информации, СВТ ИС, помещениям, в которых располагаются СВТ ИС, и хранилищам;

– об утрате носителей информации, паролей и идентификаторов, ключей от помещений, где ведется обработка информации ИС и хранилищ;

– об обнаружении вредоносного программного обеспечения или нетипичного поведения ИС;

– о попытках получения информации лицами, не имеющими к ней допуска;

– об иных внештатных ситуациях, связанных с угрозой безопасности ИС;

2.5. Пользователю запрещается:

– подключать к СВТ ИС нештатные устройства;

– самостоятельно вносить изменения в состав, конфигурацию и размещение СВТ ИС;

– самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения, установленного в ИС;

– самостоятельно вносить изменения в размещение, состав и настройку средств защиты информации (далее – СЗИ) ИС;

– сообщать устно, письменно или иным способом (показ и т.п.) другим лицам идентификаторы и пароли, передавать ключи от хранилищ и помещений и другие реквизиты доступа к ИС;

– разрешать работу с СВТ ИС лицам, не допущенным в установленном порядке к обработке информации в ИС.

3. ПРАВА ПОЛЬЗОВАТЕЛЯ ИС

3.1. Пользователь ИС имеет право:

– обращаться к администратору безопасности, администратору ИС и ответственному за организацию обработки ПДн по любым вопросам, касающихся обработки и защиты информации в ИС (выполнение режимных мер, установленной технологии обработки информации, инструкций и других документов по обеспечению безопасности информации ИС);

– обращаться к администратору безопасности с просьбой об оказании консультаций и технической помощи по обеспечению безопасности обрабатываемой в ИС информации, а также по вопросам эксплуатации установленных средств защиты информации (СЗИ);

– обращаться к администратору ИС и администратору безопасности с просьбой об оказании консультаций и технической помощи по использованию установленных программных и технических средств ИС.

4. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ ИС

4.1. Пользователь ИС несет ответственность:

– за соблюдение установленной технологии обработки информации в ИС, в том числе ПДн*;

– за соблюдение режима конфиденциальности информации;

– за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него при работе в ИС;

– за соблюдение требований локальных актов по вопросам обработки и защиты информации в ИС, в том числе ПДн.

4.2. Пользователи ИС, несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Руководством, в пределах, определенных действующим законодательством Российской Федерации.

ОЗНАКОМЛЕНЫ:

(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*
(должность)	*(дата, подпись)*	*(расшифровка подписи)*