Муниципальное бюджетное общеобразовательное учреждение средняя общеобразовательная школа № 15 имени Пяти Героев Советского Союза города Хабаровска

ПРИКАЗ

21.10.2024г. № 141 - ОД

Об организации работ
по защите информации,
содержащей персональные
данные в 2024-2025 учебном году

Во исполнении Федерального закона Российской Федерации от 27.07.2006 г. № 152-ФЗ «О персональных данных» и Постановления правительства Российской Федерации от 01.11.12г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

ПРИКАЗЫВАЮ:

1. Возложить обязанности по защите информации:
1.1. Назначить ответственным за организацию обработки персональных данных на Гусеву Л.В., заместителя директора по УВР.
1.2. Назначить ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных (администратором) Титаренко А.А., учителя информатики
1.3. Назначить ответственным за эксплуатацию ИС «ПК-sekretar» Климову Ирину Николаевну.
1.4. Назначить ответственным за прием письменных согласий законных представителей учащихся на обработку персональных данных Климову И.Н., секретаря.
1.5. Определить местом хранения письменных согласий законных представителей учащегося на обработку персональных данных личное дело учащегося.
1.6. Назначить ответственным за прием заявлений с письменным согласием на обработку персональных данных сотрудников Климову И.Н., секретаря.
1.7. Определить местом хранения заявлений с письменным согласием на обработку персональных данных сотрудников личное дело сотрудника.
1.8. Назначить ответственными за эксплуатацию средств криптографической защиты Новакова Ю.М., директора школы; Климову И.Н., секретаря.
1.9. Утвердить перечень должностей, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей согласно приложению 1 к настоящему приказу.

1.10. Утвердить перечень должностей, ведущих обработку персональных данных без использования средств автоматизации согласно приложению 2 к настоящему приказу.
1.11. Утвердить список лиц, имеющих право самостоятельного доступа в помещение с установленной информационной системой персональных данных (ПК-sekretar) согласно приложению 3 к настоящему приказу
1.12. Утвердить список лиц, допущенных к работе в информационной системе персональных данных (ПК-sekretar) согласно приложению 3а к настоящему приказу
2. Создать комиссию по защите информации:
2.1.Утвердить состав комиссии по защите информации согласно приложению 4 к настоящему приказу. приложению 5
2.2. Утвердить положение о комиссии по защите информации согласно приложению 6 к настоящему приказу.
3. Утвердить типовые формы документов по защите информации:
3.1. Согласие на обработку персональных данных согласно приложению 7 к настоящему приказу.
3.2. Разъяснение субъекту персональных данных согласно приложению 7 к настоящему приказу.
3.3. Обязательство о неразглашении информации, содержащей персональные данные, согласно приложению 8 к настоящему приказу.
3.4. Журналы по защите информации согласно приложению 9 к настоящему приказу.
3.5. Протокол заседания комиссии по защите информации согласно приложению 10 к настоящему приказу.
3.6. Акт определения уровня защищенности ПДн при их обработке в ИСПДн согласно приложению 11 к настоящему приказу.
3.7. Акт определения класса защищенности ИС персональных данных субъектов персональных данных согласно приложению 12 к настоящему приказу.
4. Утвердить перечень информационных систем персональных данных согласно приложению 13 к настоящему приказу.
5. Утвердить перечень обрабатываемых персональных данных согласно приложению 14 к настоящему приказу.
6. Утвердить 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 согласно приложению 15 к настоящему приказу.
7. Утвердить политику в отношении обработки персональных данных согласно приложению 16.
8. Утвердить инструкции и правила по защите информации:
– Инструкцию ответственного за организацию обработки персональных данных согласно приложению 17 к настоящему приказу.
– Правила рассмотрения запросов субъектов персональных данных согласно приложению 18 к настоящему приказу.
– Инструкция пользователя при обработке персональных данных на объектах вычислительной техники согласно приложению 19 к настоящему приказу;

– Инструкция пользователя при обработке персональных данных на объектах вычислительной техники согласно приложению 19 к настоящему приказу;
– Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (администратора безопасности) согласно приложению 20 к настоящему приказу;
– Инструкцию по организации резервного копирования, согласно приложению 21 к настоящему приказу;
– Инструкцию по организации парольной защиты, согласно приложению 22 к настоящему приказу;
– Инструкцию по организации антивирусной защиты, согласно приложению 23 к настоящему приказу;
– Инструкцию по проверке электронного журнала обращений к информационной системе персональных данных, согласно приложению 24 к настоящему приказу;
– Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении законных оснований, согласно приложению 25 к настоящему приказу;
– Инструкцию по обращению с криптосредствами согласно приложению 26 к настоящему приказу;
– Инструкцию по обработке персональных данных без использования средств автоматизации согласно приложению 27 к настоящему приказу;
– Инструкция ответственного за эксплуатацию информационных систем персональных данных согласно приложению 28 к настоящему приказу;
9. Утвердить план мероприятий по защите информации согласно приложению 29 к настоящему приказу.
10. Положение о работе с персональными данными работников, обучающихся и их родителей (закон. представителей).

Директор МБОУ СОШ №15 Ю.М. Новаков

С приказом ознакомлены:

Приложение 1
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

Перечень должностей, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей

Должность	ИСПДн
Директор	«ПК –sekretar»
Заместители директора по УВР	«ПК –sekretar»
Заместитель директора по ВР	«ПК –sekretar»
Педагог-психолог	«Дневник.ру»
Учителя-предметники	«Дневник.ру»
Классные руководители	«Дневник.ру»

Приложение 2
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

Перечень должностей, ведущих обработку персональных данных без использования средств автоматизации

Должность
Директор
Заместители директора по УВР
Заместитель директора по ВР
Педагог-психолог
Учителя-предметники
Классные руководители

Приложение 3
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

Список лиц,
допущенных к работе в информационной системе персональных данных (ПК-sekretar)

Nп/п	Фамилия, имя, отчество	Должность
1	Новаков Юрий Михайлович	Директор
2	Климова Ирина Николаевна	Секретарь
3	Гусева Любовь Васильевна	Зам. директора по УВР
4	Бегун Любовь Владимировна	Зам. директора по УВР
5	Вторыгина Анастасия Андреевна	Зам. директора по ВР

Приложение 3а
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

Список лиц, имеющих право самостоятельного доступа в помещение
с установленной информационной системой персональных данных (ПК-sekretar)

Nп/п	Фамилия, имя, отчество	Должность
1	Новаков Юрий Михайлович	Директор
2	Климова Ирина Николаевна	Секретарь
3	Бегун Любовь Владимировна	Зам. директора по УВР

Приложение 4
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

Состав комиссии по защите информации

Председатель комиссии	Новаков Юрий Михайлович, Директор Школы
Члены комиссии	Гусева Любовь Васильевна, зам директора по УВР
	Бегун Любовь Владимировна, зам директора по УВР
	Титаренко Алексей Анатольевич, Учитель информатики

Приложение 6
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ПОЛОЖЕНИЕ
о комиссии по защите информации

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 МБОУ СОШ №15.

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 МБОУ СОШ №15на 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 МБОУ СОШ №15, 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 МБОУ СОШ №15.

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 МБОУ СОШ №15, 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 МБОУ СОШ №15.

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. Отчетность комиссии

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

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

Приложение 7
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

СОГЛАСИЕ
на обработку персональных данных

г. Хабаровск «_ __ _» _____ _____ г.

Я, _____,
(фамилия, имя, отчество)

_____ серия _____ № _____ выдан _____
(вид документа, удостоверяющего личность)

_____
(когда и кем)

проживающий(ая) по адресу: _____
_____

настоящим даю свое согласие на обработку моих персональных данных _____
_____
(наименование и адрес оператора)

и подтверждаю, что, давая такое согласие, я действую по своей воле и в своих интересах.

Согласие дается мною для целей _____
_____
_____
(цель обработки персональных данных)

и распространяется на следующую информацию: _____
_____
_____
_____
_____
_____,

полученных лично от меня для обработки и передачи в документальной и электронной форме в различные государственные органы власти, если этого требует законодательство Российской Федерации или Хабаровского края, а также третьим лицам _____
_____
_____
(наименование и адреса третьих лиц)

с целью исполнения обязательств представителя нанимателя в рамках трудового договора, и в установленных Федеральными законами случаях их обязательного предоставления. Также не возражаю против обработки сведений обо мне, содержащих данные об имени, фамилии, отчестве, должности, телефонном номере и адресе электронной почты, полученных мною для их использования в служебных целях, в т. ч. размещения в государственных информационных системах, используемых в рамках обеспечения доступа к информации о деятельности МБОУ СОШ №15.

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу

(распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных с учетом федерального законодательства.

Настоящее согласие дается на период до истечения сроков хранения соответствующей информации или документов, содержащих указанную информацию, определяемых в соответствии с законодательством Российской Федерации.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

_____

(Ф.И.О., подпись лица, давшего согласие)

Примечание:
1. Вместо паспорта могут указываться данные иного основного документа, удостоверяющего личность субъекта персональных данных.
2. Письменное согласие заполняется и подписывается субъектом персональных данных собственноручно в присутствии должностного лица оператора.
3. Перечень персональных данных уточняется исходя из целей получения согласия.

Приложение 8
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

Разъяснение
субъекту персональных данных

Мне, _____
разъяснены юридические последствия отказа предоставить свои персональные данные в МБОУ СОШ №15.

В соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 152 ФЗ «О персональных данных», определен перечень персональных данных, которые субъект персональных данных обязан предоставить в МБОУ СОШ №15 в связи с поступлением на работу.

Без представления субъектом персональных данных обязательных для заключения трудового договора сведений, трудовой договор не может быть заключен.

_____	_____	_____
дата	подпись	расшифровка

Приложение 8
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

Обязательство
о неразглашении информации, содержащей персональные данные

Я, __
(фамилия, имя, отчество полностью)

являясь работником МБОУ СОШ №15, в должности
_____
_____,
(указать должность)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового договора.

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

_____	_____	_____
дата	подпись	расшифровка

Приложение 10
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

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 которым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка Об уничтожении	
1														

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
(для администратора зала)

№ 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
учета выявленных инцидентов информационной безопасности

№ № п/п	Дата и время	Описание инцидента	Ответственный за реагирование на инцидент	Отметка об устранении инцидента	Дата устранения инцидента	Подпись ответственного лица	Примечание

ЖУРНАЛ
учета передачи персональных данных

№ п/п	Сведения о запрашивающем лице	Состав запрашиваемых персональных данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных данных	Дата передачи/отказа в передаче персональных данных	Подпись запрашивающего лица

ЖУРНАЛ
периодического тестирования средств защиты информации

№ п/п	Наименование средства защиты информации от НСД или криптосредства	Регистрационные номера СЗИ от НСД или криптосредства	Дата тестирования	Фамилия и подпись ответсвенного пользователя, проводившего тестирование	Наименование теста, используемые средства для проведения теста	Результат тестирования (успешный/неуспешный), комментарий	Дата очередного тестирования

ЖУРНАЛ
учета проверок электронных журналов обращений к информационным системам персональных данных

№ п/п	Дата проверки	Наименование ИСПДн, компьютера, технического средства	Наименование проверяемого журнала	Выявленные нарушения требований безопасности, нештатные ситуации	Подпись администратора безопасности	Примечание

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

Приложение 10
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ПРОТОКОЛ № 1
заседания комиссии по защите информации

Дата и время проведения	27.09.2024 г
Место проведения	МБОУ СОШ №15

Присутствовали:

председатель комиссии	Новаков Ю.М.
члены комиссии	Гусева Л.В.
	Бегун Л.В.
	Титаренко А.А.

Повестка дня

Определение информационных систем персональных данных (далее - ИСПДн), принадлежащих МБОУ СОШ №15.

1. Слушали: Титаренко Алексея Анатольевича доложил исходные данные об ИСПДн «ПК-sekretar».

Выступила: Гусева Любовь Васильевна, которая предложила утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн «ПК-sekretar».

Постановили:

Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС «ПК-sekretar».

2. Слушали: Титаренко Алексея Анатольевича доложил исходные данные об ИСПДн «Дневник.ру».

Выступила: Гусева Любовь Васильевна, которая предложила утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн «Дневник.ру».

Постановили:
Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС «Дневник.ру».

Председатель комиссии	_____	Новаков Ю.М.
Члены комиссии	_____	Гусева Л.В.
	_____	Бегун Л.В.
	_____	Титаренко А.А.

Приложение 11
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

АКТ
определения уровня защищенности ПДн при их обработке в ИСПДн «ПК-sekretar». и класса защищенности ИС «ПК-sekretar».

Присутствовали:
председатель комиссии Новаков Ю.М.
члены комиссии Гусева Л.В., Бегун Л.В., Титаренко А.А.

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

– Категории персональных данных обрабатываемых в ИСПДн: 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	_____	Новаков Ю.М.
Члены комиссии	_____	Гусева Л.В.
	_____	Бегун Л.В.
	_____	Титаренко А.А.

«25» сентября 2024 г.

АКТ

определения уровня защищенности ПДн при их обработке в ИСПДн «Дневник.ру» и класса защищенности ИС «Дневник.ру»

Присутствовали:

председатель комиссии Новаков Ю.М.

члены комиссии Гусева Л.В., Бегун Л.В., Титаренко А.А.

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

– Категории персональных данных обрабатываемых в ИСПДн: 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	_____	Новаков Ю.М.
Члены комиссии	_____	Гусева Л.В.
	_____	Бегун Л.В.
	_____	Титаренко А.А.

«25» сентября 2024 г.

Приложение 12
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

Акт
определения классификации
информационной системы персональных данных
ПК - sekretar МБОУ СОШ №15,
расположенного по адресу: г. Хабаровск, ул. Серышева, д.53.

В соответствии с постановлением Правительства Российской Федерации от 13.02.2008 № 55/86/20 «Порядк проведения классификации информационных систем персональных данных» и Приказом директора МБОУ СОШ №15. № 177 от 02.09 2019 г комиссия в составе председателя Ю.М. Новакова , членов комиссии Гусевой Л.В., Титаренко А.А. произвела сбор данных об информационной системе персональных данных и установила нижеследующее:

1) в информационной системе персональных данных (ИСПДн) *ПК - sekretar МБОУ СОШ №15* обрабатываются персональные данные сотрудников школы и иных категорий персональных данных;

2) в ИСПДн одновременно обрабатываются персональные данные менее чем 100 000 субъектов персональных данных;

3) по структуре ИСПДн относится к локальной информационной системе, состоящей из одного АРМ;

4) по наличию подключений к сетям международного информационного обмена (Интернет) информационная система относится к системам, имеющим подключение;

5) по режиму обработки персональных данных в информационной системе ИСПДн относится к однопользовательским;

6) по разграничению прав доступа пользователей ИСПДн относится к системам с разграничением прав доступа;

7) в зависимости от местонахождения технических средств ИСПДн относится к системам, технические средства которых размещены в Российской Федерации;

8) речевая обработка сведений составляющих ПДн в информационной системе не осуществляется.

9) условие обработки персональных данных – для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных менее чем 100 000 субъектов персональных данных, являющихся сотрудниками оператора персональных данных.

В соответствии с пунктами 14 и 15 «Порядка проведения классификации информационных систем персональных данных», утвержденного совместным приказом ФСТЭК России, ФСБ России, Министерства информационных технологий и связи Российской Федерации от 13.02.2008 № 55/86/20 и на основании анализа исходных данных,

РЕШИЛА:

информационной системе персональных данных ПК - sekretar МБОУ СОШ №15 установить класс: третий.

Председатель комиссии Ю.М. Новаков

Члены комиссии_____ Л.В. Гусева

_____ А.А. Титаренко

«25» сентября 2024 г.

Приложение 13
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

Перечень информационных систем персональных данных

Наименование	Адрес расположения
Информационная система «ПК - sekretar»;	г. Хабаровск, ул. Серышева, д. 53, к. директора
Образовательная сеть «Дневник.ру	*Расположение серверов компании ООО «Дневник.ру»*
Персональные данные, хранимые в виде твердых (бумажных) копий	г. Хабаровск, ул. Серышева, д. 53, к. директора

Приложение 13
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ПЕРЕЧЕНЬ
информационных систем персональных данных

Перечень информационных систем персональных данных является систематизированным изложением перечня информационных систем персональных данных (далее ИСПДн), подлежащих защите в МБОУ СОШ №15 и разработан в соответствии с Федеральными законами Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлений Правительства РФ от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использовании средств автоматизации», приказа федеральной службы по техническому и экспортному контролю России от 05 февраля 2010 года № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных», специальным требованиям и рекомендациям по технической защите конфиденциальной информации (СТР-К).

Для создания Перечня и определения соответствия ИСПДн информационной безопасности организации требованиям вышеперечисленных нормативно-правовых актов определены:

– состав информационной системы персональных данных;
– структура информационной системы персональных данных;
– состав, объем и режимы обработки персональных данных;
– права доступа лиц, допущенных к обработке персональных данных;
– существующие меры защиты персональных данных.

Данные проведенного обследования служат информационной основой для внутренних нормативно-организационных документов организации, а именно:

– данные о составе и структуре ИСПДн и существующие меры защиты персональных данных служат основой для составления Модели угроз безопасности персональных данных;

– состав и объем обрабатываемых персональных данных служат основой для составления: Перечня категорий персональных данных, Перечня должностей работников, осуществляющих обработку персональных данных, Перечня помещений, в которых размещены технические средства, используемые для обработки персональных данных, и сейфы для хранения документов, связанных с обработкой персональных данных.

В МБОУ СОШ №15 следующие информационные системы установлены:

-Информационная система «ПК - sekretar»;

используются:

-Информационная система - Образовательная сеть «Дневник.ру;

-персональные данные, хранимые в виде твердых (бумажных) копий.

Информационная система «ПК - sekretar»

Описание информационной системы

Информационная система «ПК - sekretar», месторасположение – Россия, г. Хабаровск, развернута на одном рабочем месте, расположенном в кабинете №1 (приемная директора), на 1 этаже. Имеется выход в сеть Интернет. Данные из системы передаются в Федеральную налоговую службу, Пенсионный фонд, Фонд социального страхования, Росстат, другие органы надзора по запросу.

Основание для обработки

Трудовой кодекс РФ, Налоговый кодекс РФ.

Объекты защиты

– средства обработки информации (персональные компьютеры, линии связи, коммутационное оборудование);

– персональные данные: Ф.И.О., документа, удостоверяющего личность, место жительства, ИНН, СНИЛС, дополнительная информация.

Разграничение прав доступа

В соответствии с Положением о разграничении прав доступа к обрабатываемым персональным данным.

Источник получения персональных данных Субъект персональных данных

Перечень должностей работников, осуществляющих обработку персональных данных Секретарь

Классификация информационной системы

В соответствии с приказом ФСТЭК, ФСБ, Мининформсвязи от 13.02.2008 № 55/86/20, а также исходя из того, что в информационных системах обрабатываются персональные данные второй категории (Категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1), работающие в отрасли образования Российской Федерации, проживающие в пределах муниципального образования и в количестве более тысячи субъектов персональных данных,

Образовательная сеть «Дневник.ру»

Описание информационной системы

Образовательная сеть «Дневник.ру» (разработчик ООО «Дневник.ру» , Россия, г. Санкт-Петербург) является разработчиком решений и единой электронной среды для учителей, учеников и их родителей, администрации образовательных организаций, а также представителей органов исполнительной власти. Работа в образовательной сети регламентируется локальным нормативным актом «Положение о ведении журнала, обеспечивающего учет выполнения образовательной программы, в электронном виде». Имеется выход в сеть Интернет. Доступ осуществляется с рабочих мест работников в соответствии с Перечнем должностей работников, осуществляющих обработку персональных данных, и Положением о разграничении прав доступа к обрабатываемым персональным данным.

Основание для обработки

ФЗ «Об образовании в Российской Федерации».

Соглашение ООО «Дневник.ру» и МБОУ СОШ №15 от 01.08.2014 № 1/54-110, срок действия – до выполнения сторонами обязательств по Соглашению.

Объекты защиты

– средства обработки информации (персональные компьютеры, линии связи, коммутационное оборудование);

– персональные данные: Ф.И.О., класс, успеваемость, пропуски, адрес электронной почты, дополнительная информация.

Разграничение прав доступа

В соответствии с Положением о разграничении прав доступа к обрабатываемым персональным данным.

Источник получения персональных данных Субъект персональных данных

Перечень должностей работников, осуществляющих обработку персональных данных

В соответствии с Перечнем должностей работников, осуществляющих обработку персональных данных

Расположение серверов компании ООО «Дневник.ру»

Дата-центры ООО «Селектел» соответствуют международному стандарту Tier III и требованиям безопасности банков, платежных систем и предприятий электронной коммерции PCI DSS.

Юридический адрес: 196084, г. Санкт-Петербург, ул. Цветочная, дом 21 литера А. Адреса нахождения серверов:

г. Санкт-Петербург, ул. Цветочная. Общая площадь — 1 500 м². Площадь серверного помещения — 700 м². В помещениях расположено 200 телекоммуникационных шкафов, прецизионные кондиционеры и кластеры источников бесперебойного питания.

1.Санкт-Петербург, ул. Цветочная. Общая площадь — 12 000 м². Площадь серверных помещений — 2 450 м². В помещениях размещено 850 серверных стоек, прецизионные кондиционеры и кластеры источников бесперебойного питания.

Адрес официального сайта: https://selectel.ru

Сертификат соответствия системы защиты информации

ООО «Дневник.ру» обладает встроенными средствами защиты от несанкционированного доступа к информации и соответствует требованиям руководящего документа Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации» для 5-го класса защищенности.

Лицензии на разработку средств защиты конфиденциальной информации Подтверждено право ООО «Дневник.ру» на деятельность по разработке средств защиты конфиденциальной информации, а также на деятельность по ее технической защите. *Аттестат соответствия требованиям по безопасности информации* Информационная система персональных данных «Дневник.ру» (класс ИСПДн —К2) соответствует требованиям нормативной документации по безопасности информации. Аттестация выполнена в соответствии с методикой и программой аттестационных испытаний, утвержденной Заместителем генерального директора-директором СПбФ ФГУП «ЗащитаИнфоТранс» в 2015 году.

Электронная программа заполнения аттестатов

Основание для обработки

Приказ Минобрнауки РФ от 14.02.2014 № 115 «Об утверждении Порядка заполнения, учета и выдачи аттестатов об основном общем и среднем общем образовании и их дубликатов»;

Приказ Минобрнауки РФ от 14.10.2013 № 1145 «Об утверждении образца свидетельства об обучении и порядка его выдачи лицам с ограниченными возможностями здоровья (с различными формами умственной отсталости), не имеющим основного общего и среднего общего образования и обучавшимся по адаптированным основным общеобразовательным программам»

Объекты защиты

– средства обработки информации (персональные компьютеры, линии связи, коммутационное оборудование);

– персональные данные: Ф.И.О., класс, успеваемость, пропуски, адрес электронной почты, дополнительная информация.

Разграничение прав доступа

В соответствии с Положением о разграничении прав доступа к обрабатываемым персональным данным.

Источник получения персональных данных Субъект персональных данных

Перечень должностей работников, осуществляющих обработку персональных данных В соответствии с Перечнем должностей работников, осуществляющих обработку персональных данных

Официальный сайт образовательной организации

Основание для обработки

Федеральный закон от 08.11.2010 № 29Э-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием контрольно-надзорных функций и оптимизацией предоставления государственных слуг в сфере образования»

ст. 29 Федерального закона от 29.12.2012 г. №273-ФЗ «Об образовании в РФ», Постановление Правительства РФ от 29.05.2014 № 785 «Об утверждении требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления на нем информации»

Объекты защиты

Педагогические работники:

− Ф.И.О. работников;

− Уровень образования;

− Квалификация и опыт работы;

Занимаемая должность;

− Преподаваемые дисциплины;

− Ученая степень;

− Ученое звание;

− Наименование направления подготовки и (или) специальности;

− Данные о повышении квалификации и (или) профессиональной переподготовке (при наличии);

− Общий стаж работы;

− Стаж работы по специальности;

− Фото работника;

Обучающиеся:

− Ф.И.О. обучающихся;

− Фото обучающихся;

− Достижения в олимпиадах, конкурсах, соревнованиях, научно-практических конференциях.

Персональные данные, хранимые в виде твердых (бумажных) копий

4. МБОУ СССОШ №15 обрабатываются документы, содержащие персональные данные в виде твердых (бумажных) копий.

В соответствии с п.15 постановления правительства РФ от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации» перечень мер защиты от несанкционированного доступа к материальным носителям определяется оператором. В соответствии с этим рекомендуется документы хранить в металлических шкафах, сейфах, либо в выделенных помещениях, а также составить перечень лиц, допущенных к работе с документами содержащими персональные данные.

5.соответствии с этим в МБОУ СОШ №15 разработаны и утверждены: Перечень должностей работников, осуществляющих обработку персональных данных, Перечень помещений, в которых размещены технические средства, используемые для обработки персональных данных, и сейфы для хранения документов, связанных с обработкой персональных данных, Требования к оборудованию помещений, размещению технических средств, используемых для обработки персональных данных, и сейфов для хранения документов, связанных с обработкой персональных данных, а также к допуску к ним ответственных лиц.

Приложение 14
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

Перечень персональных данных,
обрабатываемых в информационной системе персональных данных «ПК-sekretar» МБОУ СОШ №15

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
1.	Заявление о приеме на работу	Фамилия, имя, отчество	Трудовой кодекс РФ	Оформление трудового договора, приказа
2.	Трудовой договор	Фамилия, имя, отчество, паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, дата выдачи, наименование органа, выдавшего документ, код подразделения), адрес места жительства (по паспорту)	Трудовой кодекс РФ	Оформление приказа
3.	Трудовые книжки работников ОУ	Фамилия, имя, отчество, дата рождения, образование, профессия, специальность, подпись владельца трудовой книжки, сведения о приеме на работу и переводах на другую должность и об увольнении (дата) с указанием причин и со ссылкой на статью, пункт закона, сведения о присвоении классного чина, сведении об аттестации руководителей ОУ, сведения о поощрениях и награждениях, дата и номер документа, на основании которого внесена запись	Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ; Постановление Правительства РФ от 16.04.2003 N 225 (ред. от 25.03.2013) "О трудовых книжках" (вместе с "Правилами ведения и хранения трудовых книжек, изготовления бланков трудовой книжки и обеспечения ими работодателей")	Исполнение трудового договора, исполнение обязанностей, возложенных на организацию Трудовым Кодексом, Федеральными законами РФ

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
4.	Личная карточка работника ОУ	Фамилия, имя, отчество, дата и место рождения, гражданство, идентификационный номер налогоплательщика (ИНН), номер страхового свидетельства государственного пенсионного страхования, паспорт (серия, номер, дата выдачи, наименование органа выдавшего документ), адрес места жительства (по паспорту и фактический), дата регистрации по месту жительства, номер телефона; сведения о (об): - образовании, квалификации и наличии специальных знаний или специальной подготовки; - послевузовском профессиональном образовании; - учёной степени; - знании иностранных языков и степени владения ими; - повышении квалификации и профессиональной переподготовке; - стаже работы; - состоянии в браке; - составе семьи (семьи (степени родства, ФИО, годе рождения); - воинском учете; - трудовой деятельности (характер и вид работы, прием на работу и переводы на другую работу; основании прекращения трудового договора (увольнения), номере и дате приказа об увольнении, дате увольнения); - присвоенном квалификационном разряде (до 2014 г.), классном чине; - аттестации и оценке работника;	Трудовой кодекс РФ Постановление Госкомстата России от 05.01.2004 № 1	Оформление личной карточки работника ОУ

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
5.	Приказы об оплате	Должностной оклад, доплаты и надбавки, премии (разовые, квартальные, по итогам полугодия и календарного года), материальная помощь	Трудовой кодекс РФ	Формирование заработной платы
6.	Листок нетрудоспособности	Фамилия, имя, отчество, страховой стаж, дата рождения, ИНН, номер страхового свидетельства государственного пенсионного страхования	Федеральный закон РФ от 29.12.2006 № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством»	Оплата труда работников в период нетрудоспособности
7.	Обращения граждан	Фамилия, имя, отчество, адрес проживания, E-mail, номер телефона и другие персональные данные, указанные в обращении	Федеральный закон РФ от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращения граждан РФ»	Рассмотрение обращения и подготовка ответа
8.	Справка о заработной плате и трудовом стаже	Фамилия, имя, отчество, адрес, номер телефона, место работы, периоды работы, должность	ФЗ от 22.10.2004 № 125-ФЗ «Об архивном деле в РФ»	Оформление пенсии работников
9.	Приказы МБОУ СОШ №15	Ф.И.О., должность работника ОУ, Ф.И.О., должность руководителя ОУ и другие персональные данные, указанные в согласии на обработку персональных данных		Реализация функций ОУ
10.	Заявление о приеме в 1 класс ребенка	Ф.И.О, дата рождения ребенка, Ф.И.О., место жительства, паспортные данные родителя (законного представителя)	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ» (ст. 67, ч.1)	Учет детей, подлежащих обучению

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
11.	Сведения об учащихся, зачисленных в ОУ, отчисленных из ОУ	Ф.И.О., дата рождения, место учебы учащегося	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ» (ст. 9, ч.1, п.6)	Учет детей, подлежащих обучению по образовательным программам начального общего, основного общего, среднего общего образования
12.	Сведения о несовершеннолетних, не посещающих или систематически пропускающих по неуважительным причинам занятия в ОУ	Ф.И.О.	Федеральный закон от 24.06.1999 № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» (ст.14, ч.1 п. 4)	Учет несовершеннолетних, не посещающих или систематически пропускающих по неуважительным причинам занятия
13.	Информация о победителях и призерах конкурсов школьного уровня	Ф.И.О. учащегося, возраст	Приказы управления образования	Подведение итогов конкурсов школьного уровня, составление списков победителей и призеров для церемонии награждения

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
14.	Заявление на участие в итоговом сочинении (изложении) от учащегося 11класса	Ф.И.О., серия и номер паспорта	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ» Постановление Правительства РФ от 31.08.2013 № 755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» Порядок проведения государственной итоговой аттестации по образовательным программам среднего общего образования (приказ Минобрнауки РФ от 26.12.2013г. №1400)	Формирование муниципального сегмента федеральной информационной системы (далее-ФИС) и региональной информационной системы обеспечения проведения государственной итоговой аттестации (далее-РИС)

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
15.	Заявление на участие в едином государственном экзамене от учащегося 11класса	Ф.И.О., серия и номер паспорта, дата рождения, СНИЛС	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ», Постановление Правительства РФ от 31.08.2013 № 755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» Порядок проведения государственной итоговой аттестации по образовательным программам среднего общего образования (приказ Минобрнауки РФ от 26.12.2013г. №1400)	Формирование муниципального сегмента ФИС и РИС

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
16.	Заявление на участие в основном государственном экзамене от учащегося 9 класса	Ф.И.О., серия и номер паспорта	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ» Постановление Правительства РФ от 31.08.2013 № 755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» Порядок проведения государственной итоговой аттестации по образовательным программам основного общего образования (приказ Минобрнауки РФ от 25.12.2013г. № 1394)	Формирование муниципального сегмента ФИС и РИС

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
17.	Заявление на участие в государственном выпускном экзамене от учащегося 9(11) класса	Ф.И.О., серия и номер паспорта, справка о состоянии здоровья (МСЭ или заключение ПМПК)	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ» Постановление Правительства РФ от 31.08.2013 № 755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» Порядок проведения государственной итоговой аттестации по образовательным программам среднего общего образования (приказ Минобрнауки РФ от 26.12.2013г. № 1400) Порядок проведения государственной итоговой аттестации по образовательным программам основного общего образования (приказ Минобрнауки РФ от 25.12.2013г. № 1394)	Формирование муниципального сегмента ФИС И РИС

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
18.	Сведения о педагогах, выполняющих на едином государственном экзамене, основном государственном экзамене функции организаторов ППЭ	Ф.И.О., серия и номер паспорта, год рождения, уровень профессионального образования, квалификация, предметная специализация, должность, стаж работы	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ» Постановление Правительства РФ от 31.08.2013 № 755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» Порядок проведения государственной итоговой аттестации по образовательным программам среднего общего образования (приказ Минобрнауки РФ от 26.12.2013г. № 1400)	Формирование муниципального сегмента ФИС И РИС

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
19.	Протокол результатов государственной итоговой аттестации в форме ЕГЭ, ОГЭ, ГВЭ	Ф.И.О., серия и номер паспорта, результаты ЕГЭ	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ» Постановление Правительства РФ от 31.08.2013 № 755 «О федеральной информационной системе обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования, и приема граждан в образовательные организации для получения среднего профессионального и высшего образования и региональных информационных системах обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования» Порядок проведения государственной итоговой аттестации по образовательным программам среднего общего образования (приказ Минобрнауки РФ от 26.12.2013г. № 1400)	Ознакомление участников единого государственного экзамена, их родителей с результатами экзаменов

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
20.	Информация о несчастных случаях с учащимися, воспитанниками учреждения образования в образовательном процессе, дорожно-транспортных происшествиях и несчастных случаях со смертельным исходом	Ф.И.О., год рождения (возраст) пострадавших, место учебы, медицинский диагноз, Ф.И.О. педагогов, учащихся и др. очевидцев, участников несчастных случаев	Приказ Гособразования СССР от 01.10.1990 № 639	Обеспечение контроля за расследованием несчастных случаев. Составление акта формы Н-2. Учет несчастных случаев, выполнение мероприятий по устранению причин несчастных случаев
21.	Акт формы Н-2	Ф.И.О., год рождения, место учебы, класс (группа), медицинское заключение о НС, Ф.И.О. педагогов, учащихся и др. очевидцев, участников НС	Приказ Гособразования СССР от 01.10.1990 № 639 (п.п. 1.4., 1.6., 2.4.2.)	Обеспечение контроля за расследованием несчастных случаев
22.	Материалы расследований несчастных случаев	Ф.И.О. пострадавших, педагогов, учащихся и др. очевидцев, участников несчастных случаев	Приказ Гособразования СССР от 01.10.1990 № 639 (п.2.4.2.)	Обеспечение контроля за расследованием несчастных случаев, выполнение мероприятий по устранению причин несчастных случаев

N п/п	Наименование документов, содержащих персональные данные	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цель обработки персональных данных
1	2	3	4	5
23.	Информация для официального сайта МБОУ СОШ №15	Фамилия, имя, отчество, место работы (учебы) и другая информация, указанная в согласии на обработку персональных данных		Размещение информации на официальном сайте МБОУ СОШ№15

Перечень персональных данных, обрабатываемых в информационной системе персональных данных «Дневник.ру» МБОУ СОШ №15

Группа персональных данных	Перечень персональных данных, используемых в документе	Регламентирующие документы	Цели обработки персональных данных
1. Обработка персональных данных в ИСПДн «Дневник.ру»			
Общие сведения о гражданах	Фамилия, имя, отчество. Дата и место рождения. Паспортные данные. Данные Пенсионного страхового свидетельства. Место работы. Должность. Состав семьи. Телефоны домашний и сотовый. Сведения о ближайших родственниках (Фамилия Имя Отчество, дата рождения, степень родства). Класс. Фотография. Текушая и итоговая успкваемость, посещаемость.	Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в РФ»	Ведение электронного журнала педагогами. Обеспечение информации и контроля за успеваемостью обучающегося

Приложение 15а
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

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 МБОУ СОШ №15 (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. Хабаровск, ул. Серышева, д. 53 приведена в Комплекте документов для ИСПД «ПК-sekretar»

3. Порядок доступа в помещения

3.1. Перечень лиц, доступ которых в помещения находящиеся в пределах границы контролируемой зоны, необходим для выполнения ими

служебных (трудовых обязанностей) приведен в приложении 3 к настоящему приказу.

3.2. Неконтролируемое пребывание лиц в помещениях, находящихся в пределах границы контролируемой зоны, указанных в п. 3.1 настоящего Положения разрешено в период рабочего времени в соответствии с утвержденным графиком работы Оператора, либо вне периода рабочего времени с письменного разрешения ответственного за организацию обработки персональных данных или ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.

3.3. Лица, не указанные в п. 3.1 настоящего Положения, допускаются в помещения в присутствии лиц, имеющих право пребывания в данных помещениях.

Приложение 16
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

Политика
муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школы №15 имени Пяти Героев Советского Союза в отношении обработки персональных данных сотрудников учреждения, а также обучающихся и (или) родителей (законных представителей).

1. Общие положения

Настоящая Политика разработана на основании Конституции РФ, Гражданского Кодекса РФ, Трудового Кодекса РФ, и в соответствии с требованиями Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных», Постановления Правительства РФ от 21.03.2012 N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Цель данной Политики – обеспечение прав граждан при обработке их персональных данных, и принятие мер от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных Субъектов.

Персональные данные могут обрабатываться только для целей, непосредственно связанных с деятельностью учреждения, в частности для:

- предоставления образовательных услуг;
- проведения олимпиад, консультационных семинаров;
- направления на обучение;
- направления работ сотрудников (учащихся) на конкурсы;
- дистанционного обучения;
- ведения электронного дневника и электронного журнала успеваемости;
- ведения сайта ОУ;
- автоматизации работы библиотеки;
- проведения мониторинга деятельности школы.

МБОУ СОШ №15 собирает данные только в объеме, необходимом для достижения выше названных целей.

Передача третьим лицам персональных данных без письменного согласия не допускается.

Режим конфиденциальности персональных данных снимается в случаях обезличивания или включения их в общедоступные источники персональных данных, если иное не определено законом.

Сотрудники, в обязанность которых входит обработка персональных данных Субъекта, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и

свободы, если иное не предусмотрено законом, а также настоящей Политикой.

Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

Настоящая политика утверждается Директором МБОУ СОШ №15 и является обязательной для исполнения всеми сотрудниками, имеющими доступ к персональным данным Субъекта.

2. Понятие и состав персональных данных

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (далее – Субъекту). К персональным данным Субъекта, которые обрабатывает МБОУ СОШ №15 (далее - Учреждение) относятся:

- фамилия, имя, отчество;
- адрес места жительства;
- паспортные данные;
- данные свидетельства о рождении;
- контактный телефон;
- результаты успеваемости и тестирования;
- номер класса;
- данные о состоянии здоровья;
- данные страхового свидетельства;
- данные о трудовой деятельности;
- биометрические данные (фотографическая карточка);
- иная необходимая информация, которую Субъект добровольно сообщает о себе для получения услуг предоставляемых Учреждением, если ее обработка не запрещена законом.

3. Принципы обработки персональных данных Субъекта

Обработка персональных данных – любое действие (операция) или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Учреждение ведет обработку персональных данных Субъекта с использованием средств автоматизации (автоматизированная обработка), и без использования таких средств (неавтоматизированная обработка).

Обработка персональных данных должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Учреждения;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;
- уничтожения персональных данных после достижения целей обработки или в случае утраты необходимости в их достижении;
- личной ответственности сотрудников Учреждения за сохранность и конфиденциальность персональных данных, а также носителей этой информации.

4. Обязанности Учреждения

В целях обеспечения прав и свобод человека и гражданина Учреждение при обработке персональных данных Субъекта обязано соблюдать следующие общие требования:

- обработка персональных данных Субъекта может осуществляться исключительно в целях оказания законных услуг Субъектам;
- персональные данные Субъекта следует получать у него самого. Если персональные данные Субъекта возможно получить только у третьей стороны, то Субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Сотрудники Учреждения должны сообщить Субъектам о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа Субъекта дать письменное согласие на их получение;
- Учреждение не имеет права получать и обрабатывать персональные данные о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни, за исключением случаев, предусмотренных законом. В частности, вправе обрабатывать указанные персональные данные Субъекта только с его письменного согласия;
- предоставлять Субъекту или его представителю информацию о наличии персональных данных, относящихся к соответствующему

Субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении Субъекта персональных данных или его представителя либо в течение тридцати дней с даты получения запроса Субъекта персональных данных или его представителя;

- хранение и защита персональных данных Субъекта от неправомерного их использования или утраты обеспечивается учреждением, за счет его средств в порядке, установленном действующим законодательством РФ;
- в случае выявления недостоверных персональных данных или неправомерных действий с ними оператора при обращении или по запросу Субъекта либо уполномоченного органа по защите прав субъектов персональных данных Учреждение обязано осуществить блокирование персональных данных на период проверки;
- в случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных Субъектом либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование;
- в случае достижения цели обработки персональных данных Учреждение обязано незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней, и уведомить об этом Субъекта, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган;
- в случае отзыва Субъектом согласия на обработку своих персональных данных учреждение обязано прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней, если иное не предусмотрено соглашением между Учреждением и Субъектом. Об уничтожении персональных данных Учреждение обязано уведомить Субъекта.

5. Права Субъекта

- Право на доступ к информации о самом себе.
- Право на определение форм и способов обработки персональных данных.
- Право на отзыв согласия на обработку персональных данных.
- Право ограничивать способы и формы обработки персональных данных, запрет на распространение персональных данных без его согласия.
- Право требовать изменение, уточнение, уничтожение информации о самом себе.
- Право обжаловать неправомерные действия или бездействия по обработке персональных данных и требовать соответствующей компенсации в суде.
- Право на дополнение персональных данных оценочного характера заявлением, выражающим его собственную точку зрения.

- Право определять представителей для защиты своих персональных данных.
- Право требовать от Учреждения уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные Субъекта, обо всех произведенных в них изменениях или исключениях из них.

6. Доступ к персональным данным Субъекта

Персональные данные Субъекта могут быть предоставлены третьим лицам только с письменного согласия Субъекта.

Доступ Субъекта к своим персональным данным предоставляется при обращении либо при получении запроса Субъекта. Учреждение обязано сообщить Субъекту информацию о наличии персональных данных о нем, а также предоставить возможность ознакомления с ними в течение тридцати рабочих дней с момента обращения или получения запроса.

Запрос должен содержать номер основного документа, удостоверяющего личность Субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись Субъекта персональных данных или его законного представителя. Запрос может быть направлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации.

Клиент имеет право на получение при обращении или при отправлении запроса информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных МБОУ СОШ №15, а также цель такой обработки;
- способы обработки персональных данных, применяемые учреждением;
- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для Субъекта может повлечь за собой обработка его персональных данных.

Сведения о наличии персональных данных должны быть предоставлены Субъекту в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

Право Субъекта на доступ к своим персональным данным ограничивается в случае, если предоставление персональных данных нарушает конституционные права и свободы других лиц.

7. Защита персональных данных

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или

пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе деятельности Учреждения.

Регламентация доступа персонала к документам и базам данных с персональными сведениями входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами Учреждения. Для защиты персональных данных Субъектов необходимо соблюдать ряд мер:

- осуществление пропускного режима в служебные помещения;
- назначение должностных лиц, допущенных к обработке ПД;
- хранение ПД на бумажных носителях в охраняемых или запираемых помещениях, сейфах, шкафах;
- наличие необходимых условий в помещениях для работы с документами и базами данных с персональными сведениями; в помещениях, в которых находится вычислительная техника;
- организация порядка уничтожения информации;
- ознакомление работников, непосредственно осуществляющих обработку ПД, с требованиями законодательства РФ в сфере ПД, локальными актами оператора в сфере ПД и обучение указанных работников;
- осуществление обработки ПД в автоматизированных информационных системах на рабочих местах с разграничением полномочий, ограничение доступа к рабочим местам, применение механизмов идентификации доступа по паролю и электронному ключу, средств криптозащиты;
- осуществление внутреннего контроля соответствия обработки ПД требованиям законодательства.

Для защиты персональных данных создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности школы, посетители, работники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов.

Для защиты персональных данных Субъектов необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- технические средства охраны, сигнализации;
- порядок охраны помещений;
- · требования к защите информации, предъявляемые соответствующими нормативными документами.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

8. Ответственность за разглашение персональных данных и нарушение

Учреждение ответственно за персональную информацию, которая находится в его распоряжении и закрепляет персональную ответственность сотрудников за соблюдением, установленных в организации принципов уважения приватности.

Каждый сотрудник Учреждения, получающий для работы доступ к материальным носителям персональным данных, несет ответственность за сохранность носителя и конфиденциальность информации.

Учреждение обязуется поддерживать систему приема, регистрации и контроля рассмотрения жалоб Субъектов, доступную с помощью телефонной, телеграфной или почтовой связи.

Любое лицо может обратиться к сотруднику Учреждения с жалобой на нарушение данной Политики. Жалобы и заявления по поводу соблюдения требований обработки данных рассматриваются в течение тридцати рабочих дней с момента поступления.

Сотрудники Учреждения обязаны на должном уровне обеспечивать рассмотрение запросов, заявлений и жалоб Субъектов, а также содействовать исполнению требований компетентных органов. Лица, виновные в нарушении требований настоящей политики, привлекаются к дисциплинарной ответственности.

Приложение 17
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная Инструкция определяет основные обязанности и права ответственного за организацию обработки персональных данных МБОУ СОШ №15 (далее – школа).

1.2. Ответственный за организацию обработки персональных данных является сотрудником школы и назначается приказом директора.

1.3. Решение вопросов организации защиты персональных данных в школе входит в прямые служебные обязанности ответственного за организацию обработки персональных данных.

1.4. Ответственный за организацию обработки персональных данных обладает правами доступа к любым носителям персональных данных в школе.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.2. **Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.3. **Доступ к информации** – возможность получения информации и её использования.

2.4. **Защита информации** — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.5. **Информация** - сведения (сообщения, данные) независимо от формы их представления.

2.6. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.7. **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

2.8. **Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.

2.9. **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

2.10. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.11. **Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.12. **Угрозы безопасности персональных данных (УБПДн)** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение

персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

2.13. **Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

III. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Ответственный за организацию обработки персональных данных обязан:

3.1. Знать перечень и условия обработки персональных данных в школе.

3.2. Знать и предоставлять на утверждение директора школы изменения к списку лиц, доступ которых к персональным данным необходим для выполнения ими своих служебных (трудовых) обязанностей.

3.3. Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей.

3.4. Осуществлять учёт документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения.

3.5. Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.

3.6. Реагировать на попытки несанкционированного доступа к информации в установленном ст.4 настоящей Инструкции порядке.

3.7. Контролировать осуществление мероприятий по установке и настройке средств защиты информации.

3.8. По указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в ИСПДн и правилам обработки персональных данных.

3.9. Проводить занятия и инструктажи с сотрудниками школы о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности персональных данных.

3.10. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

3.11. Контролировать соблюдение сотрудниками локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными.

3.12. Вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.

3.13. Организовать учет обращений субъектов персональных данных, контролировать заполнение «Журнала учета обращений субъектов персональных данных».

3.14. Представлять интересы школы при проверках надзорных органов в сфере обработки персональных данных.

3.15. Знать законодательство РФ о персональных данных, следить за его изменениями.

3.16. Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

IV. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

4.1. К попыткам несанкционированного доступа относятся:

4.1.1. сеансы работы с персональными данными незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по

доступу к данным;

4.1.2. действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

4.2. При выявлении факта несанкционированного доступа ответственный за организацию обработки персональных данных обязан:

4.2.1. прекратить несанкционированный доступ к персональным данным;

4.2.2. доложить директору школы служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

4.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

4.2.4. известить администратора безопасности ИСПДн о факте несанкционированного доступа.

V. ПРАВА

Ответственный за организацию обработки персональных данных имеет право:

5.1. Требовать от сотрудников выполнения локальных нормативно-правовых актов в части работы с персональными данными.

5.2. Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.

5.3. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

VI. ОТВЕТСТВЕННОСТЬ

6.1. Ответственный за организацию обработки персональных данных несёт персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

6.2. Ответственный за организацию обработки персональных данных при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

С инструкцией ознакомлен

Приложение 18
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей

1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

– Подтверждение факта обработки персональных данных;

– Правовые основания и цели обработки персональных данных;

– Цели и применяемые оператором способы обработки персональных данных;

– Наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон);

– Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;

– Сроки обработки персональных данных, в том числе сроки их хранения;

– Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу.

2. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3. Сведения должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

4. Сведения предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса

субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

5. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной по которому является субъект персональных данных.

6. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 5 настоящих правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 4 настоящих правил, должен содержать обоснование направления повторного запроса.

7. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 5 и 6 настоящих правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

8. Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных:

– Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к

соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 30 (тридцати) дней с даты получения запроса субъекта персональных данных или его представителя.

– В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати) дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

– Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 (семи) рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий 7 (семи) рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях, предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

– Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Приложение 19
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

Инструкция
пользователя при обработке персональных данных на объектах вычислительной техники

I. Общие положения

1. Инструкция пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники (далее - Инструкция), регламентирует основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) образовательного учреждения (далее - ОУ).

2. Инструкция регламентирует деятельность пользователя, который имеет допуск к обработке соответствующих категорий персональных данных и обладает необходимыми навыками работы на ПЭВМ.

II. Обязанности пользователя

1. При выполнении работ в пределах своих функциональных обязанностей пользователь несет персональную ответственность за соблюдение требований нормативных документов по защите информации.

2. Пользователь обязан:

- выполнять требования Положения о порядке обработки и защите персональных данных в МБОУ СОШ №15
- при работе с персональными данными исключать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц, а также располагать во время работы экран видеомонитора так, чтобы отображаемая на нем информации была недоступна для просмотра посторонними лицами;
- соблюдать правила работы со средствами защиты информации, а также установленный режим разграничения доступа к техническим средствам, программам, данным и файлам с персональными данными при ее обработке;
- после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня производить стирание остаточной информации с жесткого диска ПЭВМ;
- оповещать обслуживающий ПЭВМ персонал, а также непосредственного руководителя обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;
- не допускать "загрязнения" ПЭВМ посторонними программными средствами;
- помнить личные пароли и персональные идентификаторы;
- знать штатные режимы работы программного обеспечения, пути проникновения и распространения компьютерных вирусов;
- при применении внешних носителей информации перед началом работы проводить их проверку на наличие компьютерных вирусов.

3. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции.

В случае обнаружения зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя, администратора системы, а также смежные подразделения, использующие эти файлы в работе;

- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

4. Пользователю ПЭВМ запрещается:

- записывать и хранить персональные данные на неучтенных в установленном порядке машинных носителях информации;
- удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;
- самостоятельно подключать к ПЭВМ какие-либо устройства, а также вносить изменения в состав, конфигурацию и размещение ПЭВМ;
- самостоятельно устанавливать и/или запускать на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей; осуществлять обработку персональных данных в условиях, позволяющих просматривать их лицами, не имеющими к ним допуска, а также нарушающих требования к эксплуатации ПЭВМ;
- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;
- отключать (блокировать) средства защиты информации;
- производить какие-либо изменения в подключении и размещении технических средств;
- производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями;
- бесконтрольно оставлять ПЭВМ с загруженными персональными данными, установленными маркированными носителями, электронными ключами и выведенными на печать документами, содержащими персональные данные.

III. Права пользователя

1. Пользователь ПЭВМ имеет право:

- обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий;
- обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

IV. Заключительные положения

1. Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

2. Работники подразделений ОУ и лица, выполняющие работы по договорам и контрактам и имеющие отношение к обработке персональных данных на объектах вычислительной техники, должны быть ознакомлены с инструкцией.

Приложение 20
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (администратор информационной безопасности)

1. Общие положения

Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – ИСПДн).

Лицо ответственное за обеспечение безопасности персональных данных в ИСПДн (далее – администратор информационной безопасности) это лицо, отвечающее за обеспечение заданных характеристик информации, содержащей персональные данные (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

Администратор информационной безопасности в ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием автоматизированных рабочих мест.

2. Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

– Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в ИСПДн;

– Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных.

– Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование;

– Еженедельно осуществлять резервное копирование информации, содержащей персональные данные (при необходимости);

– Обязан осуществлять периодический контроль за выполнением работниками эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн;

– Участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации;

– Обязан анализировать журнал системы защиты информации от несанкционированного доступа (НСД), проводить проверки электронного журнала обращений к информационным системам персональных данных;

– Обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ;

– Обязан вести журнал учета средств защиты информации, используемых в ИСПДн;

– Обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ;

– Обязан проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты;

– Обязан проводить мероприятия по организации антивирусной защиты;

– Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно инструкции по организации парольной защиты в информационных системах персональных данных;

– Обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации;

– Обязан немедленно сообщать ответственному за организацию обработки персональных данных, информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:

– Установить причины, по которым стал возможным НСД;

– Установить последствия, к которым привел НСД;

– Зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;

– Провести проверку настроек средств защиты информации и операционных систем на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей к защищаемым информационным ресурсам и объектам доступа ИСПДн, при необходимости провести настройку;

– Провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты персональных данных.

3. Права администратора информационной безопасности.

Администратор информационной безопасности имеет право:

– Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;

– Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

– Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за организацию обработки персональных данных в ИСПДн и/или ответственному за эксплуатацию ИСПДн;

4. Ответственность администратора информационной безопасности

На администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн;

Администратор информационной безопасности в ИСПДн несет ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 21
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ИНСТРУКЦИЯ
по организации резервного копирования

1. Общие положения

Настоящая инструкция разработана с целью обеспечения возможности оперативного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных (далее – ИСПДн).

2. Резервируемое программное обеспечение и базы персональных данных

В ИСПДн резервированию подлежит:

– Общее программное обеспечение (операционная система и программные драйверы устройств (принтера, монитора, видеокарты и т.п.), поставляемые с компонентами автоматизированных рабочих мест (далее – АРМ), входящими в состав ИСПДн);

– Прикладное программное обеспечение, используемое для обработки персональных данных (средства обработки текстов и таблиц, специализированные программы и т.п.);

– Базы персональных данных (тестовые и табличные файлы, а также файлы баз данных специализированных программ);

– Программное обеспечение средств защиты информации, в том числе средств антивирусной защиты.

3. Порядок резервирования и хранения резервных копий

Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения у администратора информационной безопасности в ИСПДн машинных носителей информации, содержащих дистрибутивы данного программного обеспечения.

Машинные носители информации обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны также храниться у администратора информационной безопасности в ИСПДн.

Допускается хранение машинных носителей прикладного программного обеспечения и машинных носителей с обновлениями к нему в структурных подразделениях, эксплуатирующих ИСПДн.

Резервирование баз персональных данных, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные установленным порядком машинные носители информации.

Резервирование осуществляется ежемесячно.

Резервные носители персональных данных хранятся в структурных подразделениях, эксплуатирующих ИСПДн, в порядке, предусмотренном для носителей информации персональных данных.

К резервному носителю персональных данных должна быть приложена учетная карточка, в которой делаются отметки о дате резервирования.

Резервные носители персональных данных не могут быть переданы за пределы структурных подразделений, эксплуатирующих ИСПДн.

Копирование информации с резервных носителей персональных данных, за исключением случая восстановления работоспособности ИСПДн, запрещается.

4. Порядок восстановления работоспособности ИСПДн

Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.

Данные работы осуществляются администратором информационной безопасности в ИСПДн в соответствии с эксплуатационной документацией на программное обеспечение до полного восстановления работоспособности.

В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на администратора информационной безопасности в ИСПДн и руководителя структурного подразделения, обеспечивающего ее эксплуатацию.

Учетная карточка резервного носителя персональных данных
№ _____

Дата резервного копирования	Объект копирования	Кто производил копирование	Подпись

Приложение 22
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

Инструкция по организации парольной защиты

I. Общие положения

1. Инструкция по организации парольной защиты (далее - Инструкция) призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах образовательного учреждения (далее - ОУ), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах информационной системы (далее - ИС) ОУ и контроль за действиями исполнителей и обслуживающего персонала при работе с паролями возлагается на системного администратора ОУ или лаборанта.

II. Правила формирования паролей

1. Личные пароли генерируются и распределяются централизованно либо выбираются пользователями информационной системы самостоятельно с учетом следующих требований:

- пароль должен состоять не менее чем из восьми символов;
- в пароле обязательно должны присутствовать буквы из верхнего и нижнего регистров, цифры и специальные символы (@, #, $, &, *, % и т. п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т. д.), последовательности символов и знаков (111, qwerty, abed и т. д.), общепринятые сокращения (ЭВМ, ЛВС, USER, и т. п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- при смене пароля новый пароль должен отличаться от старого не менее чем в шести позициях.

2. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственных лиц.

III. Ввод пароля

1. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т. п.).

IV. Порядок смены личных паролей

1. Смена паролей проводится регулярно, не реже одного раза в пол года.

2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т. п.) системный администратор должен немедленно удалить его учетную запись сразу после окончания последнего сеанса работы данного пользователя с системой.

3. Срочная (внеплановая) полная смена паролей производится в случае прекращения полномочий (увольнение, переход на другую работу и т. п.) администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

4. Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 5 (IV) Инструкции.

5. Временный пароль, заданный системным администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

V. Хранение пароля

1. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе либо в сейфе у системного администратора или руководителя подразделения в опечатанном пенале.

2. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

3. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

VI. Действия в случае утери и компрометации пароля

1. В случае утери или компрометации пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 9 или 10 (IV) Инструкции.

VII. Ответственность при организации парольной защиты

1. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, несоответствующих данным требованиям, а также за разглашение информации о пароле.

2. Ответственность за организацию парольной защиты в структурных подразделениях ОУ возлагается на системного администратора.

3. Работники ОУ и лица, имеющие отношение к обработке персональных данных в информационных системах ОУ, должны быть ознакомлены с инструкцией.

С инструкцией ознакомлены:

Приложение 22
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ИНСТРУКЦИЯ

по организации парольной защиты на объектах информатизации **ПК-sekretar** предназначенных для обработки информации ограниченного распространения

Данная Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей на объектах информатизации муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школы № 15 имени Пяти Героев Советского Союза, предназначенных для обработки информации ограниченного распространения, а также контроль за действиями пользователей при работе с паролями.

ПОРЯДОК РАБОТЫ ПО ОБЕСПЕЧЕНИЮ ПАРОЛЬНОЙ ЗАЩИТЫ

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах автоматизированной системы и контроль за действиями пользователей при работе с паролями возлагается на администратора безопасности.

2. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

- длина пароля должна быть не менее шести символов;
- в числе символов пароля обязательно должны присутствовать символы из следующих категорий: строчные буквы латинского алфавита, прописные буквы латинского алфавита, десятичные цифры;
- символы паролей должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ADMIN, SECRET, USER и т.п.);
- использование трех и более подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо;
- использование двух и более подряд одинаковых символов недопустимо;
- при смене пароля новое значение должно отличаться от предыдущего минимум в 6-ти символах;
- новый пароль не должен совпадать с одним из 10-ти предыдущих паролей;
- пользователь обязан сохранять в тайне свой личный пароль.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за разглашение парольной информации.

3. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в один квартал.

4. При смене пароля администратором безопасности производится тестирование функций средств защиты информации от несанкционированного доступа путем ввода с клавиатуры заведомо ложного пароля, при наличии считывателя – предъявления стороннего идентификатора.

5. Внеплановая смена личного пароля или удаление учетной записи пользователя объекта информатизации в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

6. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора безопасности.

7. В случае компрометации (утеря, передача парольной информации) личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.4 или п.5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

8. Хранение сотрудником (исполнителем) значений своих паролей на любом носителе не допускается.

Приложение 23
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ИНСТРУКЦИЯ
по организации антивирусной защиты в информационных системах
МБОУ СОШ № 15имени Пяти Героев Советского Союза

1. ОБЩИЕ ТРЕБОВАНИЯ

1.1. Настоящая Инструкция определяет требования к организации защиты объектов информатизации от разрушающего воздействия компьютерных вирусов и устанавливает ответственность сотрудников МБОУ СОШ № 15, эксплуатирующих и сопровождающих информационные системы персональных данных (далее – ИСПДн), за их выполнение. Инструкция распространяется на автоматизированные системы, предназначенные для обработки информации ограниченного распространения (персональных данных). Для отдельных автоматизированных систем могут быть разработаны свои инструкции, учитывающие особенности их работы.

1.2. К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств и прошедшие в установленном порядке процедуру оценки соответствия требованиям по безопасности.

1.3. Установка и настройка средств антивирусного контроля, контроль за состоянием антивирусной защиты в ИСПДн осуществляется администратором безопасности.

1.4. Установка средств антивирусного контроля производится в программную папку «C:\Program Files/Kasperske Lab».

1.5. После установки и настройки средств антивирусного контроля администратором безопасности в обязательном порядке должна быть произведено тестирование системы антивирусной защиты.

1.6. Ответственность за организацию и проведение мероприятий антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на администратора безопасности.

1.7. Ответственность за ежедневный антивирусный контроль в процессе эксплуатации ИСПДн и своевременное информирование администратора безопасности в случае обнаружения действий вредоносных программ возлагается на пользователей ИСПДн.

2. ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОГО КОНТРОЛЯ

2.1. Ежедневно в начале работы при загрузке компьютеров в автоматическом режиме должен проводиться антивирусный контроль всех электронных носителей информации ИСПДн.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях.

Настройка средств антивирусной защиты должна реализовывать следующие функции:

− Непрерывный автоматический мониторинг информационного обмена в ИСПДн с целью выявления программно-математического воздействия (далее – ПМВ).

− Автоматическая проверка на наличие вредоносных программ или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных

программ), которые могут содержать вредоносные программы, по их типовым шаблонам и с помощью эвристического анализа.

− Реализация механизма автоматического блокирования обнаруженных вредоносных программ путем их удаления из программных модулей или уничтожения.

− Автоматическая проверка критических областей автоматизированных рабочих мест и серверов, таких как системная память, загрузочные секторы дисков, объекты автозапуска, каталоги операционной системы «system» и «system32» при каждом запуске операционной системы.

− Полная автоматическая проверка носителей информации всех автоматизированных рабочих мест и серверов не реже одного раза в неделю.

− Регулярное обновление антивирусных баз и программных модулей средств антивирусной защиты.

− Автоматическое документирование состояния системы антивирусной защиты ИСПДн.

2.2. Пользователи ИСПДн при работе со съемными носителями информации (flash-накопители, CD/DVD диски, жесткие диски USB и т.д.) обязаны перед началом работы осуществить их проверку на предмет отсутствия вредоносных программ выполнив следующие действия:

− Подключить съемный носитель информации.

− Открыть значок Рабочего стола «Мой компьютер».

− Установить курсор мыши на имя выбранного носителя.

− По правой клавише мыши открыть контекстное меню Microsoft Windows и выбрать пункт, запускающий антивирусную проверку электронного носителя информации.

2.3. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, администратором безопасности также должна быть выполнена антивирусная проверка электронных средств обработки персональных данных.

2.5. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, появление сообщений о системных ошибках и т.п.) пользователь ИСПДн самостоятельно или вместе с администратором безопасности информации должен провести внеочередной антивирусный контроль рабочей станции.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов:

- пользователи ИСПДн обязаны:
  - приостановить работу в ИСПДн;
  - немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности и других сотрудников, использующих эти файлы в работе;
  - совместно с администратором безопасности провести анализ необходимости дальнейшего использования зараженных файлов;
- администратор безопасности обязан провести лечение зараженных файлов или их гарантированное удаление.

Приложение 24
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ИНСТРУКЦИЯ
по проверке электронного журнала обращений к информационной системе персональных данных

1. Задачи проверки.

Под проверкой понимается отслеживание событий, происходивших на автоматизированных рабочих местах (далее – АРМ) в течение определенного времени.

Общими задачами проверки являются:

– Контролирование состояния защищенности системы;

– Выявление причин произошедших изменений;

– Определение лиц или процессов, деятельность которых привела к изменению состояния защищенности системы или к НСД;

– Установление времени изменений.

Проверку средств защиты осуществляет администратор информационной безопасности.

2. Журналы записей о событиях.

События, происходящие на АРМ, входящем в состав ИСПДн, регистрируются в журналах.

Каждому событию соответствует отдельная запись в журнале, содержащая подробную информацию для анализа события.

В состав используемых в ИСПДн средств защиты информации может входить специальное программное средство для аудита журналов событий, предназначенное для загрузки и просмотра журналов (далее — программа просмотра журналов). В программу просмотра журналов могут быть загружены записи следующих журналов:

– Штатные журналы операционной системы Windows;

– Журналы событий средств защиты информации.

3. Штатные журналы операционной систем.

В штатных журналах ОС Windows регистрируются только те события, которые имеют отношение к операционной системе. События используемых средств защиты информации в них не регистрируются.

Информация о событиях, происходящих на АРМ под управлением ОС Windows, сохраняется в следующих штатных журналах:

– Журнал приложений – содержит сведения об ошибках, предупреждениях и других событиях, возникающих при исполнении приложений;

– Системный журнал – содержит сведения об ошибках, предупреждениях и других событиях, возникающих в операционной системе;

– Журнал безопасности – хранит информацию о попытках регистрации, а также о событиях, связанных с использованием ресурсов.

Подробное описание содержимого штатных журналов ОС Windows отражено в документации к операционной системе.

Загрузка и просмотр записей штатных журналов может осуществляться как в программе просмотра журналов средств защиты, так и с помощью стандартных средств работы с журналами ОС Windows — в оснастке «Просмотр событий» («Eventviewer»).

4. Журнал событий средств защиты информации.

Журналы средств защиты информации (далее – СЗИ) хранят информацию о событиях, отслеживаемых средствами самих СЗИ, в этом журнале регистрируются события, заданные параметрами СЗИ для локальной политики безопасности.

5. Аудит.

Сведения, содержащиеся в журнале, позволяют отслеживать использование механизмов защиты, которые предоставляют средства защиты информации АРМ (шифрование файлов, полномочное управление, замкнутая программная среда и др.) подробное описание регистрируемых событий указано в соответствующих руководствах к используемым СЗИ.

6. Просмотр событий электронных журналов.

Администратор информационной безопасности в ИСПДн производит проверку электронных журналов.

В случае обнаружения нарушений администратор информационной безопасности докладывает о данном факте ответственному за организацию обработки персональных данных.

Приложение 25
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ПОРЯДОК
уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований

Настоящий документ устанавливает порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки, или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению.

Уничтожение документов производится в присутствии ответственного за организацию обработки персональных данных, который несет персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (Акт составляется в свободной форме).

Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

После уничтожения материальных носителей ответственный за организацию подписывает акт в двух экземплярах, также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__(дата)».

Уничтожение информации на носителях необходимо осуществлять путем стирания информации с использованием сертифицированного программного обеспечения, установленного на АРМ с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

Информация, содержащая персональные данные при достижении целей обработки или при наступлении иных законных оснований (например, утратившие практическое значение, с истекшим сроком хранения) в электронном виде, подлежит уничтожению.

Приложение 26
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

Инструкция
по работе с СКЗИ, сертификатами ключей подписи, открытыми и закрытыми ключами электронной подписи

2. Нормативные документы

1. Федеральный закон от 6 апреля 2011 года N 63-ФЗ «Об электронной подписи». Принят Государственной Думой 25 марта 2011 года.
2. Федеральный закон от 20.07.06. №149 ФЗ «Об информации, информационных технологиях и о защите информации». Принят Государственной Думой 08.07.2006

3. Термины и определения

Администратор безопасности информации – лицо, организующее, обеспечивающее и контролирующее выполнение требований безопасности информации при осуществлении обмена электронными документами. В штатной структуре МБОУ СОШ №15 – учитель информатики.

Электронная цифровая подпись (ЭЦП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации и позволяющий идентифицировать владельца ключа, а также установить отсутствие искажения информации в электронном документе.

Средства криптографической защиты информации (далее - СКЗИ) и квалифицированная электронная цифровая подпись предназначены для подписания электронных документов ЭЦП с целью подтверждения подлинности информации, ее авторства и шифрования при передаче по открытым каналам связи для обеспечения конфиденциальности.

Закрытый ключ подписи – уникальная последовательность символов, известная владельцу сертификата и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств ЭЦП.

Открытый ключ подписи – уникальная последовательность символов, соответствующая закрытому ключу подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения подлинности ЭЦП в электронном документе.

Сертификат ключа подписи (сертификат) **–** документ на бумажном носителе или электронный документ, который включает в себя открытый ключ ЭЦП и который выдается удостоверяющим центром для подтверждения подлинности ЭЦП и идентификации владельца сертификата.

Носитель ключевой информации (ключевой носитель) – материальный носитель информации, содержащий закрытый ключ подписи или шифрования.

Шифрование – способ защиты информации от несанкционированного доступа за счет ее обратимого преобразования с использованием одного или нескольких ключей.

3. Общие положения

СКЗИ и средства ЭЦП могут использоваться для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

Электронная цифровая подпись выдается сроком на один год с момента изготовления. Срок действия ЭЦП указан в сертификате. По истечении этого срока владельцу ЭЦП необходимо провести плановую смену ЭЦП в Удостоверяющем центре.

Использование ЭЦП в конкретной информационной системе (программе) определяется руководством по эксплуатации данной системы (программы).

ЭЦП является аналогом собственноручной подписи и должна использоваться только ее владельцем в соответствии с ограничениями, содержащимися в сертификате. Пользователь принимает на себя риски, связанные с неправомочным использованием ЭЦП и средств ЭЦП, с подделкой, подлогом либо иным искажением информации, которая содержится в документах, предоставленных Пользователем для получения ЭЦП, компрометацией используемых ключей ЭЦП, нарушений положений Регламента оказания услуг Удостоверяющего центра.

6.Работа с СКЗИ и средствами ЭЦП

Для работы с СКЗИ и средствами ЭЦП в качестве пользователя привлекаются уполномоченные лица, назначенные соответствующим приказом руководителя организации. Работу с ключами ЭЦП и шифрования координирует администратор безопасности. Должностные лица, уполномоченные соответствующим приказом руководителя организации, могут эксплуатировать СКЗИ, получать и использовать ключи шифрования и ЭЦП, несут персональную ответственность за:

- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы СКЗИ;
- сохранение в тайне содержания закрытых ключей ЭЦП;
- сохранность носителей ключевой информации.

В организации должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

Для обеспечения безопасности ЭЦП Пользователя, необходимо:

1) хранить ключи ЭЦП на специальных защищенных носителях – электронных идентификаторах с использованием надежного пароля.
2) обеспечить надежное хранение носителей ключевой информации, исключающее доступ к ним посторонних лиц, не передавать сами носители лицам, к ним не допущенным;
3) вставлять ключевой носитель при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.);
4) не записывать на ключевой носитель постороннюю информацию;
5) не вносить какие-либо изменения в программное обеспечение СКЗИ и средств ЭЦП;
6) не использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования.

5. Проверка электронной цифровой подписи.

Для создания и проверки электронной подписи используются средства ЭЦП, которые:

1) позволяют установить факт изменения подписанного электронного документа после момента его подписания;
2) обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки.

При проверке электронной подписи средства ЭЦП должны:

3) показывать содержимое электронного документа, подписанного электронной подписью;
4) показывать информацию о внесении изменений в подписанный электронной подписью электронный документ;
5) указывать на лицо, с использованием ключа электронной подписи которого подписаны электронные документы.

Пользователь может осуществлять проверку ЭЦП как с помощью используемых средств ЭЦП, так и обратившись в Удостоверяющий центр. Процедура проверки ЭЦП в электронном документе в Удостоверяющем центре описана в Регламенте оказания услуг Удостоверяющего центра, опубликованного на сайте ca.citvo.ru.

6. Уничтожение ключевой информации.

После прекращения действия ключей ЭЦП пользователь должен удалить их путем форматирования ключевого носителя. Инструкцию по форматированию конкретного ключевого носителя необходимо скачать с сайта производителя.

7. Плановая замена ключей и сертификатов ключей

Плановая смена ключей и сертификатов открытых ключей осуществляется за месяц до окончания срока действия имеющихся ответственным лицом организации пользователя.

После окончания действия ключей ЭЦП пользователь должен удалить их с ключевого носителя путем его форматирования (утилита для форматирования Rutoken опубликована на сайте http://developer.rutoken.ru/pages/viewpage.action?pageId=7995615)

8. Внеплановая замена ключей и сертификатов ключей

Внеплановая замена ключей и сертификатов закрытых ключей проводится в следующих случаях:

Компрометация ключей;

1. Изменение идентификационных данных и/или областей использования ключа, указанных в заявлении на изготовление ключей;
2. Выход из строя ключевого носителя.

К событиям, относящимся к компрометации ключей, относятся следующие ситуации:

1) утрата ключевых носителей ключа;
2) утрата носителей ключа с последующим обнаружением;
3) увольнение сотрудников, имевших доступ к ключевой информации;
4) возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
5) нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;
6) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;
7) утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;
8) доступ посторонних лиц к ключевой информации.

Пользователь самостоятельно должен определить факт компрометации закрытого ключа и оценить значение этого события для Пользователя. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием СКЗИ, организует и осуществляет организация, в которой работает Пользователь.

При компрометации ключа пользователь должен немедленно поставить в известность Удостоверяющий центр о факте компрометации ключей, сообщив номер сертификата. В течение 30 минут после поступления сообщения о компрометации ключа, действие его будет приостановлено до подачи в Удостоверяющий центр письменного заявления об аннулировании скомпрометированных ключей.

Возобновление работы с ЭЦП будет возможно только после замены скомпрометированных ключей.

9. **Эксплуатация и хранение электронного идентификатора (носителя ЭЦП)**

1. Рекомендуется хранить ключевые носители в помещениях, которые имеют прочные входные двери с установленными на них надежными замками. В обязательном порядке для хранения ключевых носителей в помещении должно использоваться металлическое хранилище (сейф, шкаф, секция) заводского изготовления, оборудованное приспособлением для его опечатывания.

2. Транспортирование ключевых носителей за пределы организации допускается только в случаях, связанных с производственной необходимостью. Транспортирование ключевых носителей должно осуществляться способом, исключающим их утрату, подмену или порчу.

3. На технических средствах, оснащенных средствами ЭЦП, должно использоваться только лицензионное программное обеспечение фирм-производителей.

4. Запрещается оставлять без контроля вычислительные средства, на которых эксплуатируется ЭЦП после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.

5. Ключевая информация содержит сведения конфиденциального характера, хранится на учтенных в установленном порядке носителях и не подлежит передаче третьим лицам.

6. Ответственные исполнители ЭЦП обязаны вести журнал учета хранения электронных носителей конфиденциальной информации и своевременно заполнять его (см. Приложение №1).

7. Закрытые ключи изготавливаются в 2-х экземплярах: эталонная и рабочая копии. В повседневной работе используется рабочая копия ключевого носителя.

8. При физической порче рабочей копии ключевого носителя, пользователь немедленно уведомляет об этом администратора безопасности.

Категорически не допускается:

1. осуществлять несанкционированное администратором безопасности копирование ключевых носителей;

2. разглашать содержимое ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей и принтер;

3. использовать ключевые носители в режимах, не предусмотренных правилами пользования ЭЦП, либо использовать ключевые носители на посторонних ПЭВМ;

4. записывать на ключевые носители постороннюю информацию.

Для нормальной работы носителя ЭЦП, необходимо придерживаться следующих правил эксплуатации и хранения:

1. Не разбирать электронный идентификатор, это ведет к потере гарантии! Кроме того, при этом возможна поломка корпуса электронного идентификатора, поломка элементов печатного монтажа и т. д.

2. Оберегать электронный идентификатор от механических воздействий (падения, сотрясения, вибрации и т. п.), воздействия высоких и низких температур, агрессивных сред, высокого напряжения.

3. Не прилагать излишних усилий при подсоединении электронного идентификатора к порту компьютера.

4. Не допускать попадания на электронный идентификатор (особенно на его разъем) пыли, грязи, влаги и т. п. При засорении разъема электронного идентификатора принять меры для его очистки. Для очистки корпуса и разъема использовать сухую ткань. Использование органических растворителей недопустимо.

В случае неисправности или неправильного функционирования электронного идентификатора обращаться в Удостоверяющий центр.

С инструкцией ознакомлены:

Приложение 27
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ИНСТРУКЦИЯ
по обработке персональных данных без использования средств автоматизации

1. Общие положения.

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому гражданину, обратившемуся в МБОУ СОШ №15, или сотруднику (далее – субъекту персональных данных) МБОУ СОШ №15.

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные настоящим Положением, должны применяться с учетом требований Постановления Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687, а также требований нормативных правовых актов федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации.

2. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники МБОУ СОШ №15 или лица, осуществляющие такую обработку по договору с МБОУ СОШ №15), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется МБОУ СОШ №15 без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами МБОУ СОШ №15.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

− типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес учреждения, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых учреждением способов обработки персональных данных;

− типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации,– при необходимости получения письменного согласия на обработку персональных данных;

− типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещения МБОУ СОШ №15или в иных аналогичных целях, должны соблюдаться следующие условия:

− необходимость ведения такого журнала должна быть предусмотрена актом МБОУ СОШ №15, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и

ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных;

− копирование содержащейся в таких журналах информации не допускается;

− персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более одного раза в каждом случае пропуска субъекта персональных данных.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя,– путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Приложение 28
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ИНСТРУКЦИЯ
ответственного за эксплуатацию информационных систем персональных данных

1. Общие положения

Ответственный за эксплуатацию информационной системы персональных данных (далее – ИСПДн) в МБОУ СОШ №15 назначается Директором.

Методическое руководство работой ответственного за эксплуатацию ИСПДн осуществляется ответственным за организацию обработки персональных данных в МБОУ СОШ №15.

Ответственный за эксплуатацию в своей работе руководствуется положениями, руководящими и нормативными документами ФСТЭК и ФСБ России по защите информации и организационно-распорядительными документами для данной ИСПДн, а также иными нормативными документами в части защиты информации.

Ответственный за эксплуатацию ИСПДн несет ответственность за свои действия, и действия сотрудников вверенного структурного подразделения в соответствии с действующим законодательством РФ.

2. Функции ответственного за эксплуатацию ИСПДн

Осуществление контроля за целевым использованием ИСПДн, всех периферийных устройств и технических средств, входящих в состав ИСПДн.

Контроль за отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации.

Контроль использования сотрудниками структурных подразделений, эксплуатирующими ИСПДн, средств защиты информации, установленных на АРМ, входящих в состав ИСПДн.

Контроль за правильностью использования и хранения сотрудниками структурных подразделений, эксплуатирующими ИСПДн, машинных носителей информации и документов, содержащих персональные данные.

Представление заявок на пользователей, допускаемых к защищаемым ресурсам ИСПДн, с целью закрепления за ними носителей информации устройств блокировки, паролей и других средств разграничения доступа к информации, а также прав пользования средствами вычислительной техники.

Организация повышения уровня осведомленности подчиненных должностных лиц по вопросам информационной безопасности.

3. Обязанности ответственного за эксплуатацию ИСПДн

Четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

Обеспечивать функционирование ИСПДн в пределах возложенных на него функций.

Обеспечивать контроль выполнения установленного комплекса мероприятий по обеспечению безопасности ПДн.

Контролировать целостность печатей (пломб) на устройствах ИСПДн.

Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств ИСПДн и отправке их в ремонт.

Присутствовать при выполнении технического обслуживания ИСПДн при установке (модификации) программного обеспечения.

Информировать администратора информационной безопасности о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

Контролировать соответствие состава ИСПДн техническому паспорту на ИСПДн.

Приложение 29
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ПЛАН
мероприятий по защите информации в МБОУ СОШ №15

Приложение 30
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ИНСТРУКЦИЯ
по работе с инцидентами информационной безопасности

Ответственность за выявление инцидентов ИБ и реагирование на них в организации возлагается на администратора информационной безопасности.

Администратор информационной безопасности имеет полномочия инициировать проведение служебных проверок (ходатайствовать о наложении дисциплинарного взыскания перед руководителем организации по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

Администратор информационной безопасности обязан вести журнал учёта инцидентов ИБ (событий, действий повлекших за собой риски безопасности защищаемой информации и создающих предпосылки к нарушению критериев безопасности информации). Сюда относятся нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в ИС, разглашение защищаемой информации и любые действия, направленные на это, не антропогенные инциденты (сбои ПО, стихийные бедствия).

В журнале в свободной форме описывается инцидент с указанием следующих данных:

- даты и времени;
- причин (умышленные и неумышленные действия, не антропогенные инциденты и т.п.) и описания инцидента и задействованных лиц;
- информации о последствиях;
- информации о возможных последствиях (экономические убытки (в связи с заменой СЗИ, повторной аттестации; временные и трудозатраты на устранение последствий, нарушение работы пользователей, ущерб субъектам ПДн и юридические последствия для организации и т.п.).

Журнал с данным отчётом об инциденте предоставляется на ознакомление ответственному за организацию обработки персональных данных для принятия мер по предотвращению рецидива (возникновения повторного инцидента).

В случае возникновения рецидива со стороны пользователя или администратора информационной безопасности, по ходатайству ответственного за организацию обработки персональных данных руководителем организации накладывается дисциплинарное взыскание.

Сокрытие нарушений и инцидентов ИБ, вызванных любыми должностными лицами организации, является грубым нарушением трудовой дисциплины. Сокрытие нарушений и инцидентов ИБ, вызванных действиями администратора информационной безопасности и ответственным за организацию обработки персональных данных, является грубейшим нарушением дисциплины, и при выяснении данного факта должно строго наказываться.

Любой сотрудник должен согласовывать следующие действия с администратором информационной безопасности:

- замена прикладного оборудования (мышь, клавиатура, принтер, монитор);
- установка дополнительного ПО;
- изменение сетевых настроек рабочего места;
- замена, изменение любой аппаратной части рабочего места.

Ответственный за организацию обработки персональных данных не может требовать от администратора информационной безопасности действий, направленных на нарушение настоящего руководства и других организационно-распорядительных документов организации, требовать сокрытия инцидентов ИБ, вызванных любыми должностными лицами, требовать сообщения ему паролей на средства защиты информации и нарушения установленного разграничения прав по допуску к информационным ресурсам, установленным матрицей доступа к информационными ресурсам ИС.

Приложение 31
к приказу МБОУ СОШ №15
от 21. 10.2024 № 141

ИНСТРУКЦИЯ
о пропускном и внутриобъектовом режимах

1. Общие положения

Данная Инструкция регламентирует условия и порядок осуществления доступа лиц в помещения со средствами информационных систем персональных данных (далее – ИСПДн) МБОУ СОШ №15, в целях обеспечения предотвращения несанкционированного доступа к персональным данным (далее – ПДн). При обеспечении доступа лиц соблюдаются требования по защите ПДн.

Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности подразделений и определяет порядок пропуска сотрудников МБОУ СОШ №15, сотрудников иных организаций и учреждений, граждан в помещения.

Помещения и оборудование размещены таким образом, чтобы исключить возможность бесконтрольного проникновения в данные помещения и к данному оборудованию посторонних лиц.

2. Организация пропускного и внутриобъектового режима

Пропускной режим в МБОУ СОШ №15 устанавливается в целях:

- исключения фактов хищений собственности МБОУ СОШ №15;
- исключения фактов вандализма со стороны недобросовестных посетителей;
- исключения возможности несанкционированного доступа персонала и посетителей в помещения МБОУ СОШ №15.

Внутриобъектовый режим устанавливается в целях:

- соблюдения персоналом и посетителями правил внутреннего распорядка и пожарной безопасности;
- установления порядка допуска персонала в помещения ограниченного доступа предприятия;
- исключения возможности бесконтрольного передвижения посетителей по территории предприятия.

Надёжность пропускного и внутриобъектового режимов достигается:

- осуществлением контроля за перемещением персонала;
- осуществлением охраны помещений предприятия силами ЧОП;
- контролем за состоянием технических средств охраны.

Ответственным за организацию пропускного и внутриобъектового режимов является Директор МБОУ СОШ №15.

Организация пропускного и внутриобъектового режимов МБОУ СОШ №15 осуществляется руководителями соответствующих подразделений.

3. Порядок доступа в помещения сотрудников и граждан

Устанавливаются следующие часы работы Наименование организации:

- С 7-45-00 до 19-00 с понедельника по субботу;
- без обеда;
- без выходных.

Всем сотрудникам МБОУ СОШ №15 оформляется постоянный электронный пропуск.

Выполнение работ по учету, оформлению и выдаче пропусков для персонала осуществляется зам директора по административно-хозяйственной деятельности.

При увольнении сотрудника пропуск подлежит изъятию.

Контроль за правильностью учета, хранения и выдачи пропусков осуществляет Директор организации или лицо, его замещающее.

Основанием для выдачи пропуска работнику является заключенный с организации трудовой договор. С целью установления материальной ответственности персонала за выданные пропуска факт выдачи пропуска сотруднику регистрируется зам. Директора по административно-хозяйственной деятельности в журнале учета выдачи пропусков под роспись сотрудника.

4. Внутриобъектовый режим на территории МБОУ СОШ №15.

Ответственным за соблюдение правил внутреннего трудового распорядка, установленного режима функционирования, порядка содержания служебных помещений и мер противопожарной безопасности на объектах является Директор МБОУ СОШ №15.

Сотрудники кабинетов по окончании рабочего дня должны закрывать на ключ кабинеты (помещения) и сдавать ключ на пост охраны.

В случае отсутствия сотрудников в кабинетах в рабочее время, помещения должны быть закрыты на ключ.

На территории предприятия запрещается:

- проводить без разрешения руководства фото-, кино-, видеосъемки, в том числе с использованием мобильных телефонов;
- курить;
- пользоваться неисправными или самодельными электронагревательными и другими электробытовыми приборами;
- загромождать территорию, основные и запасные входы (выходы), лестничные площадки материалами и предметами, которые создают помехи для системы видеонаблюдения, затрудняют эвакуацию людей, материальных ценностей, препятствуют ликвидации очагов возгорания;

– совершать действия, нарушающие установленные режимы функционирования технических средств охраны и пожарной сигнализации.

–

5. Организация и порядок производства ремонтно - строительных работ в здании

Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных руководством. Работы проводятся только в присутствии контролирующего лица из числа сотрудников.

Для предотвращения несанкционированного доступа к информации, содержащей ПДн, осуществляется контроль деятельности рабочих.

6. Организация охраны

Должна быть организована охрана МБОУ СОШ №15. Режим работы охраны устанавливается штатным расписанием и должностными инструкциями.

Для исключения несанкционированного доступа к информации, содержащей ПДн, при покидании помещения необходимо запирать его на ключ.

7. Уборка помещений

Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

Во время уборки в помещении должна быть приостановлена работа с ПДн, должны быть заблокированы все АРМ, на которых хранятся ПДн, носители, содержащие ПДн должны быть убраны в сейф.

8. Требования по техническому укреплению

Ответственный за обеспечение безопасности ПДн обеспечивает обязательное выполнение мероприятий по техническому укреплению помещений, в которых обрабатываются ПДн, и должен руководствоваться следующими основными требованиями:

– двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек;

конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол. Стекла в рамах должны быть надежно закреплены в пазах. Рамы указанных оконных проемов оборудуются запорными устройствами. На окнах первого этажа, а также верхних этажей – при возможности прямого просмотра помещения с улицы, должны быть установлены жалюзи