Приложение №1
к приказу
от «09» марта 2022 г. № 84-п

Положение
о комиссии по защите персональных данных в информационных системах
МБОУ «Нетьинская СОШ им. Ю.Лёвкина»

1. Комиссии при работе руководствуется следующими нормативными документами:

– Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных»;

– Постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– приказом ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Порядком обращения со съемными машинными носителями персональных данных в МБОУ «Нетьинская СОШ им. Ю.Лёвкина»*)*;

– Регламентом проведения внутреннего контроля соответствия обработки персональных данных в МБОУ «Нетьинская СОШ им. Ю.Лёвкина» требованиям к защите персональных данных;

- Регламентом реагирования на инциденты информационной безопасности в информационных системах персональных данных МБОУ «Нетьинская СОШ им. Ю.Лёвкина».

2. Комиссии необходимо:

– определить уровень защищенности персональных данных, обрабатываемых в информационных системах в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– провести оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства Российской Федерации в области персональных данных;

– отбирать и уничтожать материальные носители персональных данных, обработка которых в МБОУ «Нетьинская СОШ им. Ю.Лёвкина» прекращена;

– проводить внутренний контроль соответствия обработки персональных данных в соответствии с планом, утвержденном в «Регламенте проведения внутреннего контроля соответствия обработки персональных данных в МБОУ «Нетьинская СОШ им. Ю.Лёвкина» требованиям к защите персональных данных»;

– проводить разбирательства по фактам возникновения инцидентов информационной безопасности, фиксировать их в журнале учета нештатных ситуаций и своевременно реагировать на инциденты информационной безопасности в информационных системах персональных данных.

Приложение №2
к приказу
от «09» марта 2022 г. № 84-п

РЕГЛАМЕНТ
проведения внутреннего контроля соответствия обработки персональных данных в МБОУ «Нетьинская СОШ им. Ю.Лёвкина» требованиям к защите персональных данных

1. Термины и определения

1.1. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.2. Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность. Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по информационной безопасности;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

1.3. 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.

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

1.5. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящий Регламент проведения внутреннего контроля соответствия обработки персональных данных в МБОУ «Нетьинская СОШ им. Ю.Лёвкина» требованиям к защите персональных данных (далее – Регламент), разработан в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).

2.2. Настоящий Регламент определяет порядок проведения внутреннего контроля соответствия обработки ПДн (далее – Внутренний контроль), требованиям к защите ПДн.

2.3. Регламент обязателен для исполнения ответственным за организацию обработки ПДн, ответственным за обеспечение безопасности ПДн и администратором информационных систем персональных данных.

3. Порядок проведения внутреннего контроля

3.1. Внутренний контроль в ИСПДн осуществляет комиссия для организации работ по защите персональных данных в информационных системах МБОУ «Нетьинская СОШ им. Ю.Лёвкина», состав которой утверждается приказом директора учреждения.

3.2. Допускается привлечение к проверкам сторонних экспертных организаций.

3.3. Председатель комиссии организует работу комиссии, решает вопросы взаимодействия комиссии с руководителями и работниками Учреждения, готовит и ведёт заседания комиссии, подписывает протоколы заседаний. По окончании работы комиссии готовится заключение по результатам внутреннего контроля, которое передается на рассмотрение директору Учреждения.

3.4. Внутренний контроль проводится в соответствии с «Планом проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных», утвержденным приказом МБОУ «Нетьинская СОШ им. Ю.Лёвкина», форма которого приведена в Приложении 1 к настоящему Регламенту.

3.5. В «Плане проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных» указывается перечень проводимых мероприятий внутреннего контроля и периодичность их проведения.

3.6. Комиссия проводит внутренний контроль непосредственно на месте обработки ПДн, опрашивает работников Учреждения, осуществляющих обработку ПДн, осматривает рабочие места.

3.7. При проведении внутреннего контроля должен присутствовать руководитель проверяемого подразделения.

3.8. В ходе проведения внутреннего контроля осуществляется:

- контроль выполнения организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн, необходимых для выполнения требований к защите ПДн;
- анализ изменения угроз безопасности ПДн в ИСПДн, возникающих в ходе ее эксплуатации;
- проверка параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (далее – СЗИ);
- контроль состава технических средств, программного обеспечения и СЗИ;
- состояние учета СЗИ;
- состояние учета средств шифровальной (криптографической) защиты информации;
- состояние учета съемных машинных носителей ПДн;
- соблюдение правил доступа к ПДн;
- контроль наличия (отсутствия) фактов несанкционированного доступа к ПДн;
- соблюдение пользователями ИСПДн парольной политики;
- соблюдение пользователями ИСПДн антивирусной политики;
- соблюдение пользователями ИСПДн правил работы со съемными машинными носителями ПДн;
- контроль соблюдения работниками требований локальных нормативных актов, в т.ч. требований законодательства по вопросам обработки и защиты ПДн;
- выявление уязвимостей в ИСПДн с использованием специализированных средств инструментального анализа защищенности.

3.9. Все работники обязаны по требованию членов комиссии предъявить для проверки все числящиеся за ними материалы и документы, дать устные или письменные объяснения по существу заданных им вопросов.

3.10. По завершении внутреннего контроля комиссией составляется «Акт о проведении контроля соответствия обработки персональных данных», форма которого приведена в Приложении 2 к настоящему Регламенту.

3.11. В «Акте о проведении контроля соответствия обработки персональных данных» указываются:

- перечень проведенных мероприятий;
- выявленные нарушения;
- мероприятия по устранению нарушений;
- решения по результатам внутреннего контроля;
- сроки устранения нарушений.

3.12. Периодичность проведения внутреннего контроля составляет не реже 1 раза в год.

3.13. Предложения о создании комиссии и о плановом/внеплановом проведении внутреннего контроля представляются Руководителю МБОУ «Нетьинская СОШ им. Ю.Лёвкина» ответственным за организацию обработки ПДн и ответственным за обеспечение безопасности ПДн в ИСПДн.

3.14. Внеплановый контроль проводится в следующих случаях:

- наличие подозрений на нарушение требований по защите ПДн;
- наличие подозрений на осуществление попыток несанкционированного доступа к ПДн;
- наличие подозрений на сбой в работе технических средств ИСПДн, в т.ч. средств защиты информации;
- предстоящая проверка надзорными органами.

3.15. Порядок проведения внепланового контроля совпадает с порядком проведения планового контроля.

3.16. При выявлении в ходе планового/внепланового контроля нарушений требований по обработке и защите ПДн осуществляется оперативное устранение выявленных нарушений.

3.17. Выявленные нарушения должны быть устранены в срок не превышающий 30 дней с момента утверждения «Акта о проведении контроля соответствия обработки персональных данных».

3.18. По истечению срока, данного на устранение замечаний, комиссия проводит повторный контроль.

4. Ответственность

4.1. Ответственный за организацию обработки ПДн в Учреждении несет ответственность за организацию проведения внутреннего контроля соответствия обработки ПДн в Учреждении требованиям к защите ПДн.

Приложение №1
к Регламенту проведения внутреннего контроля соответствия обработки персональных данных в МБОУ «Нетьинская СОШ им. Ю.Лёвкина» требованиям к защите персональных данных

ФОРМА

План проведения внутреннего контроля соответствия обработки персональных данных в МБОУ «Нетьинская СОШ им. Ю.Лёвкина»

№ п/п	Мероприятие	Регулярность проведения
1.	Анализ актуальности локальных нормативных актов (внутренних документов) по вопросам обеспечения безопасности персональных данных: – Проверка соответствия локальных нормативных актов (внутренних документов) по вопросам обеспечения безопасности персональных данных действующему законодательству РФ по защите персональных данных; – Учет в локальных нормативных актах (внутренних документах) по вопросам обеспечения безопасности персональных данных изменений в деятельности МБОУ «Нетьинская СОШ им. Ю.Лёвкина» по обработке и защите персональных данных.	1 раз в три года или по мере обновления законодательства РФ
2.	Проверка ознакомления работников с положениями законодательства РФ по защите персональных данных, документами, определяющими политику МБОУ «Нетьинская СОШ им. Ю.Лёвкина» в отношении обработки персональных данных и организационно-распорядительными документами по вопросам персональных данных.	1 раз в год
3.	Проверка выполнения работниками – пользователями информационных систем персональных данных инструкций по эксплуатации информационных систем персональных данных, положения о разрешительной системе доступа.	1 раз в год
4.	Проверка актуальности прав разграничения доступа пользователей информационных систем персональных данных, необходимых для выполнения должностных обязанностей.	1 раз в год
5.	Проверка актуальности определенных угроз безопасности персональных данных для информационных систем персональных данных.	1 раз в год
6.	Проверка полноты реализованных технических мер по обеспечению безопасности персональных данных в информационных системах персональных данных с учетом	1 раз в год

№ п/п	Мероприятие	Регулярность проведения
	структурно-функциональных характеристик информационных системах персональных данных, информационных технологий, особенностей функционирования информационных системах персональных данных.	
7.	Проверка наличия сертифицированных средств защиты информации, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.	1 раз в год
8.	Проверка правил обращения со съемными машинными носителями персональных данных.	1 раз в год
9.	Проверка актуальности информации, содержащейся в Уведомлении об обработке персональных данных, предоставленной в Роскомнадзор.	1 раз в год
10.	Проверка соответствия условий использования средств криптографической защиты (при их использовании) условиям, предусмотренным эксплуатационной и технической документацией к ним.	1 раз в год
11.	Выявление уязвимостей в информационных системах персональных данных в т.ч. в системе защиты с использованием средства инструментального анализа защищенности.	1 раз в год

Приложение №2
к Регламенту проведения внутреннего контроля соответствия обработки персональных данных в МБОУ «Нетьинская СОШ им. Ю.Лёвкина» требованиям к защите персональных данных

ФОРМА
АКТ

«___» _____ 20__ г. № _____

О проведении контроля соответствия обработки персональных данных

Комиссия в составе:
Председатель:
_____ _____
Члены комиссии:
1. _____ _____
2. _____ _____
3. _____ _____

составила настоящий акт о том, что комиссией были проведены мероприятия по контролю соответствия обработки персональных данныхв МБОУ «Нетьинская СОШ им. Ю.Лёвкина» требованиям к защите персональных данных. Результат проведенного внутреннего контроля отражен в Таблице 1.

Таблица 1

№ п/п	Мероприятие	Выявленные недостатки	Мероприятия по устранению недостатков	Срок проведения мероприятий	Ответственное лицо

Внутренний контроль проводился в соответствии с «Регламентом проведения внутреннего контроля соответствия обработки персональных данных в МБОУ «Нетьинская СОШ им. Ю.Лёвкина» требованиям к защите персональных данных».

Председатель:
_____ _____ _____
Члены комиссии:
_____ _____ _____
_____ _____ _____
_____ _____ _____

Приложение №3
к приказу
от «09» марта 2022 г. № 84-п

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных
МБОУ «Нетьинская СОШ им. Ю.Лёвкина»

1. Термины и определения

Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

Антивирусная защита – защита информации и компонентов информационной системы от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование «зараженных» объектов, удаление вредоносных компьютерных программ (вирусов) из «зараженных» объектов).

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

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.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

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

Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.

Средство антивирусной защиты – программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации.

Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

Настоящая Инструкция пользователя информационных систем персональных данных МБОУ «Нетьинская СОШ им. Ю.Лёвкина» (далее – Инструкция) определяет обязанности, права и ответственность работников при работе в информационных системах персональных данных (далее – ИСПДн).

Требования настоящей Инструкции являются обязательными для всех работников, осуществляющих обработку и защиту персональных данных (далее – ПДн) в ИСПДн – пользователей ИСПДн (далее – Пользователи).

К защищаемой информации, обрабатываемой в ИСПДн МБОУ «Нетьинская СОШ им. Ю.Лёвкина» (далее – Учреждение), относятся ПДн, служебная (технологическая) информация системы защиты и другая информация ограниченного доступа.

Все пользователи ИСПДн Учреждения должны быть ознакомлены с требованиями настоящей Инструкции под подпись.

Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и ПДн, и не исключает обязательного выполнения их требований.

3. Допуск пользователей к информационным системам персональных данных

Допуск пользователей к работе с ПДн в ИСПДн осуществляется в соответствии с «Перечнем должностей работников МБОУ «Нетьинская СОШ им. Ю.Лёвкина», допущенных к обработке персональных данных».

К самостоятельной работе на автоматизированных рабочих местах (далее –АРМ), входящих в состав ИСПДн, допускаются лица, изучившие требования настоящей Инструкции и локальных нормативных актов по защите информации, освоившие правила эксплуатации АРМ и технических средств защиты.

Допуск производится после проверки знания настоящей Инструкции и практических навыков в работе.

4. Обязанности пользователя

Каждый Пользователь имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

4.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн.

4.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными в ИСПДн.

4.3. Выполнять требования по антивирусной защите в части, касающейся действий Пользователей.

4.4. Немедленно ставить в известность ответственного за обеспечение безопасности ПДн в ИСПДн или администратора ИСПДн:

при подозрении компрометации личного пароля;

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

отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИСПДн;

некорректного функционирования установленных средств защиты;

обнаружения непредусмотренных отводов кабелей и подключенных устройств;

обнаружения фактов, попыток несанкционированного доступа и случаев нарушения установленного порядка обработки ПДн.

4.5. Экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами.

4.6. Пользователям ИСПДн запрещается:

отключать (блокировать) средства защиты информации, предусмотренные организационно-распорядительными документами на ИСПДн;

производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;

самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

обрабатывать в ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав Пользователя по доступу к ИСПДн;

сообщать (или передавать) посторонним лицам личные атрибуты и пароли доступа к ресурсам ИСПДн;

работать в ИСПДн при обнаружении каких-либо неисправностей;

оставлять включенным без присмотра АРМ, не активизировав средства защиты от несанкционированного доступа;

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к ознакомлению с защищаемой информацией посторонних лиц;

производить перемещения технических средств АРМ без согласования с ответственным за обеспечение безопасности ПДн в ИСПДн;

вскрывать корпуса технических средств АРМ и вносить изменения в схему и конструкцию устройств.

5. Организация работы со съемными машинными носителями информации

5.1. Организация работы со съемными машинными носителями информации (далее – СМНИ), содержащие ПДн и иную информацию конфиденциального характера, осуществляется в соответствии с «Порядком обращения со съемными машинными носителями информации в МБОУ «Нетьинская СОШ им. Ю.Лёвкина».

5.2. Пользователи обязаны знать и соблюдать установленные требования по учету и хранению СМНИ.

5.3. СМНИ должны быть зарегистрированы в «Журнале учета съемных машинных носителей информации».

5.4. СМНИ закрепляется за определенным лицом, несущим ответственность за сохранность и местонахождение данного СМНИ.

5.5. При необходимости передачи информации на СМНИ, лицо ответственное за хранение уведомляет ответственного за обеспечение безопасности ПДн в ИСПДн о необходимости передачи информации с помощью СМНИ, доставляет СМНИ по месту назначения, передает информацию с него и возвращает его на место хранения.

5.6. Хранение СМНИ осуществляется:

для флеш-карт, смарт-карт, компакт дисков и др.) в защищенных сейфах;

для СМНИ, входящих в состав ИСПДн, производится опечатывание корпуса АРМ.

5.7. Пользователям запрещается:

записывать и хранить ПДн и иную информацию конфиденциального характера на неучтенных СМНИ;

оставлять СМНИ без присмотра, передавать их другим лицам и выносить за пределы контролируемой зоны, за исключением случаев, в которых разрешена передачаСМНИ;

хранить СМНИ вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;

хранить на учтенных СМНИ программы и данные, не относящиеся к рабочей информации.

6. Организация парольной защиты

6.1. Организация парольной защиты производится в соответствии с «Инструкцией по парольной защите информации в МБОУ «Нетьинская СОШ им. Ю.Лёвкина».

6.2. Лица, использующие пароли, обязаны:

хранить в тайне свой пароль

четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов;

своевременно сообщать ответственному за обеспечение безопасности ПДн в ИСПДн обо всех нештатных ситуациях, нарушениях работы систем защиты от несанкционированного доступа, возникающих при работе с паролями.

6.3. Во время ввода паролей необходимо исключить возможность его просмотра посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или отражённом свете) или техническими средствами (видеокамеры, фотоаппараты и др.)

6.4. Для предотвращения доступа к персональным данным, пользователь во время перерыва в работе обязан осуществить блокирование системы нажатием комбинации Ctrl+Alt+Delete и кнопки «Блокировать» или нажатием комбинации Win+L.

6.5. Блокирование сеанса доступа пользователя в ИСПДн осуществляется после 15 минут его бездействия (неактивности).

6.6. В случае утери пароля работник ставит в известность своего непосредственного руководителя и ответственного за обеспечение безопасности ПДн в ИСПДн для принятия последующих решений.

6.7. В случае компрометации пароля (просмотр посторонними, разглашение пароля и др.) необходимо известить своего непосредственного руководителя и ответственного за обеспечение безопасности ПДн в ИСПДн для принятия последующих решений.

7. Правила работы в сетях общего доступа и (или) международного обмена

7.1. Работа в сетях общего доступа и на элементах ИСПДн, должна осуществляться исключительно в служебных целях.

7.2. При работе в сетях общего доступа запрещается:

осуществлять работу при отключенных средствах защиты;

передавать по сетям общего доступа защищаемую информацию без использования средств шифрования;

запрещается скачивать из сети Интернет программное обеспечение и другие файлы, если это не определено его должностными обязанностями;

запрещается посещение и использование сети Интернет в личных целях.

8. Порядок установки обновлений программного обеспечения

8.1. Установке крупных обновлений программного обеспечения должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий от устанавливаемых обновлений.

8.2. В случае обнаружения негативного воздействия устанавливаемого обновления на штатное функционирование информационной инфраструктуры, данное обновление устанавливаться не должно по согласованию с администратором ИСПДн.

8.3. Установке новых версий программного обеспечения или внесению серьезных изменений и дополнений в действующее программное обеспечение должно предшествовать тестирование информационной инфраструктуры на отсутствие негативных воздействий указанного программного обеспечения.

8.4. Установка протестированных обновлений, новых версий программного обеспечения или внесение изменений и дополнений в действующее программное обеспечение может быть произведено только по согласованию с администратором ИСПДн и ответственным за обеспечение безопасности ПДн в ИСПДн.

9. Технология обработки персональных данных

9.1. При первичном допуске к работе в ИСПДн Пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации, изучает Инструкцию, получает персональный идентификатор или личный пароль у ответственного за обеспечение безопасности ПДн в ИСПДн.

9.2. В процессе работы Пользователь производит обработку ПДн в ИСПДн.

9.3. При необходимости вывод ПДн из ИСПДн осуществляется следующим образом:

копированием ПДн на учтенные СМНИ;

передача ПДн по каналам связи с обязательным применением средств криптографической защиты.

Приложение №4
к приказу
от «09» марта 2022 г. № 84-п

ИНСТРУКЦИЯ
по парольной защите информации
в МБОУ «Нетьинская СОШ им. Ю.Лёвкина»

1. Термины и определения

1.1. Автоматизированное рабочее место – программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида.

1.2. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.3. 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.

1.4. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

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

1.6. Пользователь информационной системы персональных данных – работник, осуществляющий обработку персональных данных в информационной системе персональных данных.

1.7. Средство защиты информации – программное обеспечение, программно-аппаратное обеспечение, аппаратное обеспечение, вещество или материал, предназначенное или используемое для защиты информации.

2. Общие положения

2.1. Настоящая Инструкция по парольной защите информации в МБОУ «Нетьинская СОШ им. Ю.Лёвкина» (далее – Инструкция) устанавливает требования и ответственность при организации парольной защиты информации, а также определяет порядок контроля за действиями пользователей и обслуживающего персонала информационных систем персональных данных (далее – ИСПДн) при работе с паролями.

2.2. Требования настоящей Инструкции являются обязательными для исполнения всеми пользователями и администраторами ИСПДн МБОУ «Нетьинская СОШ им. Ю.Лёвкина» (далее – Учреждение), использующими в своей работе средства вычислительной техники.

2.3. Все пользователи и администраторы ИСПДн Учреждения, использующие в своей работе средства вычислительной техники, должны быть ознакомлены с требованиями настоящей Инструкции под роспись.

2.4. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и персональных данных (далее – ПДн), и не исключает обязательного выполнения их требований.

3. Требования, предъявляемые к идентификаторам (кодам) и паролям (порядок формирования и обращения с ними)

3.1. Авторизация пользователей ИСПДн осуществляется путем ввода идентификатора и/или пароля.

3.2. Требования к формированию паролей и обращению с ними.

3.2.1. Пароль формируется при создании учетной записи ответственным обеспечение безопасности ПДн в ИСПДн или администратором ИСПДн, при первичном входе в учетную запись пароль должен быть изменен владельцем.

3.2.2. Владельцы личных паролей обязаны обеспечить их тайну.

3.2.3. Пароли генерируются с учетом следующих требований:

−пароль должен знать только его владелец;

−длина пароля должна быть не менее 8 символов;

−в пароле обязательно должны присутствовать как цифры, так и буквы на верхнем и нижнем регистрах;

−пароль не должен включать смысловую нагрузку (имена, фамилии, наименования организаций, улиц, городов и т.д.), общепринятые сокращения (userOl, password02 и т.п.) и последовательные сочетания клавиш клавиатуры (qwertyOl, Ицукен12);

−максимальный срок действия пароля составляет 120 дней;

−минимальный срок действия пароля составляет 2 дня;

−количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя должно быть не более 6.

3.2.4. Требования к формированию паролей обеспечиваются техническими возможностями используемых операционных систем, средств защиты информации и информационных ресурсов.

3.2.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в полгода. Внеплановая смена пароля производится в случае его компрометации, а также по просьбе пользователя ИСПДн.

3.2.6. Хранение пользователями ИСПДн значений своих паролей на бумажном носителе ЗАПРЕЩЕНО.

3.2.7. Пользователь не имеет права сообщить личный пароль другим лицам (разрешается только с согласования ответственного за обеспечение безопасности или администратора ИСПДн при наличии технологической необходимости использования имен и паролей работников в их отсутствие в случае возникновения нештатбных ситуаций, форс-мажорных обстоятельств и т.п. По возвращению работники обязаны сразу же сменить свои пароли на новые значения согласно данной Инструкции).

3.3. Порядок смены паролей и идентификаторов при изменениях в организационно-штатной структуре (кадровые перестановки, увольнение работников):

3.3.1. При прекращении действия трудового договора с работником все созданные для этого работника учетные записи (пользовательское имя) подлежат блокированию не позднее, чем в день увольнения работника. Полное удаление учетных записей производится в течении 5 рабочих дней со дня увольнения работника. Основанием для блокирования и последующего удаления учетных записей работника является заявка, представленная непосредственным руководителем увольняемого не позднее, чем за 3 рабочих дня до дня его увольнения.

3.3.2. При проведении организационно-штатных мероприятий (кадровые перестановки) непосредственный руководитель структурного подразделения обязан представить администратору ИСПДн заявку на изменение в правах доступа.

3.4. Порядок действий при компрометации идентификаторов и паролей.

3.4.1. Под компрометацией понимается: утрата пароля учетной записи и (или) пароля идентификатора, разглашение учетной записи пароля или пароля идентификатора (явная компрометация), или иная ситуация, которая дает основание для предположения о нарушении конфиденциальности паролей и идентификаторов (неявная компрометация).

3.4.2. При выявлении факта утраты пароля, разглашения пароля, пароля идентификатора, самого идентификатора пользователь обязан незамедлительно сообщить о данных фактах своему непосредственному руководителю и ответственному за обеспечение безопасности ПДн в ИСПДн или администратору ИСПДн.

3.4.3. В случае выявления факта компрометации идентификаторов и паролей пользователя администратор ИСПДн или ответственный за обеспечение безопасности ПДн в ИСПДн обязан немедленно заблокировать учетную запись данного пользователя и незамедлительно произвести внеплановую смену пароля для этого пользователя.

4. Права и обязанности

4.1. Основные задачи администратора ИСПДн:

- организация установки средств идентификации и аутентификации;
- организация парольной защиты во всех ИСПДн;
- выдача первичных паролей, и электронных персональных идентификаторов и паролей к ним;
- осуществление контроля за состоянием системы парольной защиты информации в ИСПДн.

4.2. Администратор ИСПДн имеет право:

- вносить предложения по совершенствованию системы парольной защиты информации в ИСПДн;
- принимать участие в планировании мероприятий по парольной защите информации в ИСПДни планировании оснащения средствами идентификации и аутентификации;
- осуществлять контроль состояния средств идентификации и аутентификации в ИСПДн;
- инициировать служебные проверки и участвовать в проведении расследований по фактам компрометации;
- оказывать помощь в решении проблем, возникающих при эксплуатации средств идентификации и аутентификации.

4.3. Обязанности в части парольной защиты информации отражены в инструкции администратора ИСПДн.

4.4. Пользователям ИСПДн в своей работе запрещается:

- сообщать кому-либо свой личный пароль и/или пароль к электронному персональному идентификатору;
- передавать кому-либо выданный электронный персональный идентификатор;
- осуществлять вход в операционные системы ИСПДн и в информационные ресурсы под чужими идентификаторами и паролями;
- отключать средства идентификации и аутентификации.

4.5. В случае появления подозрений на факт компрометации пароля, а также в случае выявления инцидентов (фактов и т.п.), связанных со сбоями в работе средств идентификации и аутентификации, пользователи обязаны немедленно проинформировать об этом ответственного заобеспечение безопасности ПДн в ИСПДн или администратора ИСПДн.

5. Ответственность должностных лиц в рамках системы парольной защиты информации

5.1. Пользователи, ответственный за обеспечение безопасности ПДн в ИСПДн и администратор ИСПДн несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации. За несоблюдение требований законодательства Российской Федерации предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность.

5.2. Пользователи, ответственный за обеспечение безопасности ПДн в ИСПДн и администратор ИСПДн несут ответственность по действующему законодательству Российской Федерации за разглашение сведений конфиденциального характера, ставших известными при выполнении служебных обязанностей, в том числе предусмотренных настоящей Инструкцией.