Принято
Управляющим советом
МБОУ ООШ 9
Протокол № 2
от 31 мая 2021г.

Утверждаю
Директор МБОУ ООШ № 9
_____ Н.Е. Прошкина
Приказ № 37/09 от «31» мая 2021г.

Принято
на заседании совета родителей
Протокол № 1
от 31 мая 2021г

Принято
на заседании совета обучающихся
Протокол № 1
от 31 мая 2021г.

Положение о комиссии по уничтожению носителей персональных данных МБОУ ООШ № 9

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о комиссии по уничтожению носителей персональных данных МБОУ ООШ № 9 (далее – ОУ) регламентирует порядок работы комиссии и уничтожения носителей персональных данных.

1.2. Настоящее Положение утверждается заведующей ОУ и действует до замены его новым Положением.

1.3. Основной задачей Комиссии является документирование процесса уничтожения носителей персональных данных.

2. ПОРЯДОК ФОРМИРОВАНИЯ КОМИССИИ

2.1. Комиссия формируется из числа штатных сотрудников ОУ и назначается Приказом директора.

2.2. В состав Комиссии входит не менее четырех человек – членов Комиссии, в их числе – Председатель Комиссии.

2.3. Комиссия формируется из сотрудников, участвующих в процессе обработки персональных данных.

2.4. В случае изменения состава Комиссии, в Приказ вносятся соответствующие изменения.

3. ПОРЯДОК УНИЧТОЖЕНИЯ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Носителями персональных данных являются:

3.1.1. бумажные носители (заявления субъектов о предоставлении субсидий с приложениями);

3.1.2. накопители на жестких магнитных дисках (НЖМД) установленные в системных блоках рабочих мест обработки персональных данных;

3.1.3. съемные носители (дискеты, диски, USB-носители, съемные НЖМД) используемые для переноса, передачи и (или) хранения персональных данных.

3.2. Бумажные носители персональных данных могут быть уничтожены путем сожжения или измельчения.

3.3. НЖМД, съемные НЖМД и USB-носители должны быть уничтожены путем форматирования данных и физического повреждения (разбить молотком), исключающего возможность восстановления носителя.

3.4. Дискеты и диски могут уничтожаться простым физическим повреждением, без возможности восстановления носителя.

4. ПОРЯДОК РАБОТЫ КОМИССИИ

4.1. По пришествия в негодное состояние электронных носителей персональных данных или по истечению срока хранения бумажных носителей персональных данных, собирается комиссия для их уничтожения.

4.2. Председатель комиссии по согласованию с членами комиссии определяет место и время проведения процедуры уничтожения. Может быть назначено постоянное место и время проведения процедуры уничтожения носителей внутренним документом ДОУ.

4.3. Комиссия составляет опись уничтожаемых носителей и производит их уничтожение соответствующими способами, перечисленными в п.3 настоящего Положения.

4.4. Оставшиеся после уничтожения остатки носителей, по которым невозможно восстановить персональные данные, допускается выбрасывать в отведенные для мусора места.

4.5. Результатом работы комиссии является документально оформленный Акт уничтожения, который должен содержать перечень уничтоженных носителей, способ, дату и место уничтожения и подписи членов Комиссии.

4.6. Акты уничтожения хранятся вместе с Журналом учета носителей персональных данных у ответственного сотрудника.

ПРИЛОЖЕНИЕ 4. АКТ УНИЧТОЖЕНИЯ МАШИННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

АКТ
УНИЧТОЖЕНИЯ МАШИННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ

от «_____»_____20__ г. №_____

Комиссия МБОУ ООШ №9 в составе: Председатель

Должность *ФИО*

Секретарь

Должность *ФИО*

Участвовали:

Должность *ФИО*

Должность *ФИО*

Должность *ФИО*

составила настоящий акт о том, что произведено уничтожение машинных носителей/ПДн, содержащихся на машинных носителях, предназначенных для обработки конфиденциальной информации в составе:

«*тип носителя, учётный номер носителя, тип конфиденциальной информации*»

«*тип носителя, учётный номер носителя, тип конфиденциальной информации*»

…

Носители уничтожены путём _____ (сжигания/размагничивания/физического уничтожения и т.п.).

Председатель

_____*Должность* *ФИО*

Секретарь

_____*Должность* *ФИО*

Участвовали:

_____*Должность* *ФИО*

_____*Должность* *ФИО*

ПРИЛОЖЕНИЕ 5. ПОРЯДОК ОБЕСПЕЧЕНИЯ АНТИВИРУСНОЙ ЗАЩИТЫ ИСПДН МБОУ ООШ № 9

ПОРЯДОК ОБЕСПЕЧЕНИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

1. ПОРЯДОК ИСПОЛЬЗОВАНИЯ АНТИВИРУСНЫХ СРЕДСТВ

1.2. Применение средств антивирусного контроля

Средства антивирусной защиты установлены и настроены на всех допускающих такую установку программно-технических средствах до начала их использования для обработки ПДн.

Модуль средства антивирусной защиты, отвечающий за мониторинг вирусной активности в реальном времени (антивирусный монитор), запускается при загрузке операционной системы в автоматическом режиме вместе с основным модулем средства антивирусной защиты.

Антивирусный контроль рабочих станций проводится ежедневно в автоматическом режиме. В тех случаях, когда проверка всех файлов на дисках рабочих станциях занимает неприемлемо большое время, проводится выборочная проверка загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и файлов, загружаемых по сети или с внешних носителей. В этом случае полная проверка осуществляется не реже одного раза в неделю в период неактивности пользователя.

Антивирусный контроль серверов проводится ежедневно, а также при перезапуске сервера.

Проводится антивирусная проверка на рабочих станциях и серверах, вернувшихся с технического обслуживания или ремонта (в том числе, гарантийного), производимого сторонними организациями.

Любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD/DVD – R/RW, USB Flash drive и т.п.) подлежит обязательному антивирусному контролю.

Контроль исходящей информации проводится непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив, в обязательном порядке проходят антивирусный контроль. Периодические проверки электронных архивов проводятся не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение предварительно проверяется на отсутствие вредоносных программ. Непосредственно после установки (изменения) программного обеспечения компьютера системным администратором ИСПДн «НО» выполняется антивирусная проверка.

Обновления антивирусных баз производятся не реже одного раза в сутки в автоматическом режиме, согласно возможностям программного обеспечения. В случае сбоя автоматического обновления обновление баз производится вручную с той же периодичностью.

Установка, настройка и использование стандартного антивирусного пакета для серверов и рабочих станций производятся в соответствии инструкциями производителя конкретного антивирусного продукта.

2. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ВРЕДОНОСНЫХ ПРОГРАММ

В случае обращений Пользователей ИСПДн МБОУ ООШ № 9, связанных с подозрением на наличие вредоносных программ, проводится внеочередной антивирусный контроль рабочих станций обратившихся Пользователей.

В случае подтверждения наличия вредоносных программ в результате проведения контроля делается вывод либо об их уничтожении, либо о необходимости дальнейшего восстановления работоспособности компьютера.

В случае поражения программ вирусом, уничтожение вируса выполняется путем уничтожения программ на диске либо ином носителе. После уничтожения зараженных программ их исходные версии восстанавливаются из резервных копий.

Если вирус поразил файлы, его уничтожение производится путем стирания этих файлов, либо путем лечения файлов с использованием возможностей системы антивирусной защиты или специализированных лечащих утилит. Лечение файлов не дает полной гарантии их восстановления. Поэтому после лечения проводится проверка восстановления данных файлов. Лечащие программы используются лишь в тех случаях, когда отсутствует резервная копия зараженных файлов с данными, либо восстановление уничтоженных файлов из резервной копии невозможно выполнить в допустимые сроки.

После уничтожения вирусов и восстановления зараженных программ и файлов с данными проводится повторная антивирусная проверка. Перед повторной проверкой компьютер перезагружается через выключение и последующее включение. Если повторная проверка не выявила вирусов, то можно быть уверенным в их отсутствии.

При обнаружении вредоносных программ в результате проверки рабочей станции, работающей в локальной сети, проводится проверка всех компьютеров, включенных в эту сеть и работающих с общими данными и программным обеспечением.

В зависимости от критичности ситуации антивирусная проверка и выполнение действий по уничтожению вредоносных программ и восстановлению работоспособности системы проводится системным администратором ИСПДн МБОУ ООШ № 9 самостоятельно, либо инцидент эскалируется на уровень Администратора информационной безопасности ИСПДн МБОУ ООШ № 9 и Лица, ответственного за обеспечение безопасности ПДн.

3. ОТВЕТСТВЕННОСТЬ

В рамках организации антивирусной защиты систем обработки ПДн Администратор информационной безопасности ИСПДн МБОУ ООШ № 9 несёт ответственность за обеспечение правильного и непрерывного функционирования подсистемы антивирусной защиты.

Администратор информационной безопасности производит мониторинг и анализ состояния антивирусной защиты ПДн.

Системный администратор ИСПДн МБОУ ООШ № 9 несёт ответственность за своевременное обновление антивирусных баз.

Администратор информационной безопасности ИСПДн МБОУ ООШ № 9 несёт ответственность за настройку конфигурации средств антивирусной защиты, используемых для обеспечения безопасности ПДн. Системный администратор ИСПДн МБОУ ООШ № 9 производит настройку параметров антивирусной защиты по поручению Администратора информационной безопасности ИСПДн МБОУ ООШ № 9.

Администратор информационной безопасности ИСПДн МБОУ ООШ № 9 несёт ответственность за надлежащее хранение эталонных дистрибутивов средств антивирусной защиты.

Администратор информационной безопасности ИСПДн МБОУ ООШ № 9 и системный администратор ИСПДн МБОУ ООШ № 9 принимают участие в мероприятиях по реагированию на инциденты информационной безопасности, связанные с нарушением антивирусной безопасности.

ПРИЛОЖЕНИЕ 6. ПОРЯДОК ОБЕСПЕЧЕНИЯ ПАРОЛЬНОЙ ЗАЩИТЫ ИСПДН МБОУ ООШ № 9ПОРЯДОК ОБЕСПЕЧЕНИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

1. ОБЩИЕ ТРЕБОВАНИЯ К ИСПОЛЬЗОВАНИЮ ПАРОЛЕЙ

При создании новой учётной записи для неё устанавливается первичный пароль.

При создании первичного пароля используется опция, требующая смены пароля при первом входе в систему, и производится соответствующее уведомление владельца учетной записи о необходимости произвести смену пароля.

Пользователи ИСПДн МБОУ ООШ № 9 всегда положительно идентифицируются до изменения пароля и предоставления нового пароля.

Реинициализованные пароли принудительно меняются при первом входе в систему. Система автоматически блокирует учётную запись после 3 неудачных попыток ввода

пароля. Блокировка учётной записи автоматически снимается по прошествии одной минуты, после чего пользователь вновь получает возможность авторизоваться в системе. Неудачные попытки авторизации регистрируются в системном журнале.

Если система предоставляет автоматизированные инструменты для конфигурирования требуемых опций, то они соответствующим образом настроены.

Хранение работником значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте или пенале.

2. ПРАВИЛА ФОРМИРОВАНИЯ ПАРОЛЯ

Персональные пароли генерируются специальными программными средствами Администраторами ИСПДн МБДОУ №25 с учетом следующих требований:

- длина пароля составляет не менее 7-ми символов;
- длина пароля для привилегированных пользователей составляет не менее 10-ти символов;
- в составе символов пароля обязательно присутствуют буквы в верхнем и нижнем регистрах, цифры и специальные символы (“ ~ ! @ # $ % ^ & * ( ) - + _ = \ | / ? ,);
- при смене пароля новое значение отличается от предыдущего не менее чем в 4-ех позициях;
- пароль может повторяться не менее чем после использования 5-ти различных паролей;
- личный пароль пользователь не имеет права сообщать никому;
- пароль не включает в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе.

3. СРОК ДЕЙСТВИЯ ПАРОЛЯ

Пароли на серверы, рабочие станции, сетевые устройства, базы данных и приложения изменяются согласно требованиям, изложенным в Таблице 1. Блокирование учетной записи с истекшим паролем автоматизировано. Если это не возможно, пользователь изменяет свои пароли, основываясь на приведённом в Таблице 1 расписании.

Таблица 1. Сроки действия паролей

Категория учётных записей	Описание	Примеры	Срок действия
Учетные записи конечных пользователей	Все учетные записи, не перечисленные ниже	Учетные записи пользователей Windows, Unix, AS/400, Mainframe	45 дней

Административные и другие привилегированные учетные записи	Учетные записи с расширенными полномочиями	Административные учетные записи: Administrator в Windows, root в Unix, Secadm и Qsecofcr в AS/400; сетевой администратор	90 дней
Сервисные учетные записи и записи, принадлежащие приложениям	Учётные записи с некими административными привилегиями или привилегиями внутри приложения, активно используемые, связь компьютер-компьютер, редко используемые людьми	msexch, sms, учетные записи владельца приложения, учетные записи для передачи файлов (FTP)	Никогда, если не используется персоналом поддержки. В случае обнаружения подозрительной активности пароль должен меняться немедленно.
Пользовательские команды и административные записи на внутренних сетевых устройствах	Привилегированные записи и записи «только для чтения» на маршрутизаторах и коммутаторах	Cisco-connect, mstat, mtrace, rlogin, traceroute, where; Cisco-configure, copy, erase, mrinfo, reload, rsh, setup, tunnel	90 дней
Пользовательские команды и административные записи на внешних сетевых устройствах и шлюзах	Привилегированные записи и записи «только для чтения» на маршрутизаторах и коммутаторах	Cisco-connect, mstat, mtrace, rlogin, traceroute, where; Cisco-configure, copy, erase, mrinfo, reload, rsh, setup, tunnel	90 дней

В случае увольнения работника удаление соответствующей ему учётной записи пользователя ИСПДн МБОУ ООШ № 9 производится немедленно после окончания последнего сеанса работы данного пользователя. Основанием для прекращения действий прав доступа к ИСПДн МБДОУ №25 является заявка в установленной форме.

В случае компрометации персонального пароля пользователя системы немедленно выполняется внеплановая смена пароля.

4. ОТВЕТСТВЕННОСТЬ

Администратор информационной безопасности ИСПДн МБОУ ООШ № 9 несёт ответственность за корректное и непрерывное функционирование подсистемы парольной защиты систем, в которых производится обработка ПДн.

Администратор информационной безопасности ИСПДн МБОУ ООШ № 9 несёт ответственность за настройку конфигурации подсистемы парольной защиты. Системный администратор ИСПДн МБОУ ООШ № 9 производит настройку параметров парольной защиты по поручению Администратора информационной безопасности ИСПДн МБОУ ООШ № 9.

Администратор информационной безопасности ИСПДн МБОУ ООШ № 9 и системный администратор ИСПДн МБОУ ООШ № 9принимают участие в мероприятиях по реагированию на инциденты информационной безопасности, связанные с нарушением требований к организации парольной защиты ИСПДн МБОУ ООШ № 9.

Приложение 7. Журнал учета мероприятий по контролю за соблюдением режима защиты персональных данных в МБОУ ООШ № 9

ЖУРНАЛ
учета мероприятий по контролю за соблюдением режима защиты персональных данных в
МБОУ ООШ № 9

Срок хранения:
Начат «___»_____20__г.
Окончен «___»_____20__г.
На _____ листах

	Мероприятие	Дата проведения	Результаты проверки	Подпись исполнителя

	Мероприятие	Дата проведения	Результаты проверки	Подпись исполнителя

Приложение 8

ЖУРНАЛ
учета съемных носителей персональных данных
МБОУ ООШ № 9

Срок хранения:
Начат «___»_____20__г.
Окончен «___»_____20__г.
На _____ листах

Учетный №	Дата	Вид носителя	Подпись ответственного	Отметка о выдаче		Отметка о возврате		Примечание	Отметка об уничтожении
				Дата выдачи	Подпись получившего	Дата возврата	Подпись сдавшего		

Учетный №	Дата	Вид носителя	Подпись ответственного	Отметка о выдаче		Отметка о возврате		Примечание	Отметка об уничтожении
				Дата выдачи	Подпись получившего	Дата возврата	Подпись сдавшего		

Приложение 9

ЖУРНАЛ
учета процедур резервного копирования в МБОУ ООШ № 9

Срок хранения:
Начат «___»_____20__г.
Окончен «___»_____20__г.
На _____ листах

	Что подлежит резервному копированию	Дата проведения процедуры	Место создания (номер носителя) резервной копии	Подпись ответственного

Приложение № 10

ПЛАН МЕРОПРИЯТИЙ
по обеспечению защиты персональных данных
в МБОУ ООШ № 9

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. План мероприятий по обеспечению защиты персональных данных (далее – План), содержит необходимый перечень мероприятий для обеспечения защиты персональных данных.

1.2. Выбор конкретных мероприятий осуществляется на основании анализа Модели угроз безопасности.

1.3. В План включены организационные (административные), технические (аппаратные и программные) и контролирующие мероприятия.

2. ПЛАН МЕРОПРИЯТИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

	Мероприятия	**Срок выполнения Периодичность**	**Исполнитель**
Организационные мероприятия			
1.	Аудит информационных систем персональных данных	Актуализация ежегодно до 31 декабря	Ответственный за организацию обработки персональных данных, администратор безопасности обработки персональных данных
2.	Составление Перечня обрабатываемых персональных данных	Актуализация ежегодно до 31 декабря	
3.	Разработка Описания технологических процессов обработки персональных данных	Актуализация ежегодно до 31 декабря	Ответственный за организацию обработки персональных данных, администратор безопасности обработки персональных данных
4.	Составление матрицы доступа к персональным данным	Актуализация ежегодно до 31 декабря	
5.	Разработка Инструкции по защите персональных данных, обрабатываемых неавтоматизированным способом	Актуализация ежегодно до 31 декабря	
6.	Разработка Инструкции по защите персональных данных, обрабатываемых в информационных системах персональных данных	Актуализация ежегодно до 31 декабря	
7.	Разработка форм учетных Журналов	Актуализация ежегодно до 31 декабря	
Технические мероприятия			
1.	Определение необходимости	Актуализация	Ответственный

	использования технических средств защиты информации	ежегодно до 31 декабря	за организацию обработки персональных данных, администратор безопасности обработки персональных данных
2.	Внедрение системы защиты персональных данных от несанкционированного доступа.	до 31 декабря	
3.	Внедрение системы межсетевого экранирования от воздействия из сети Интернет и сегментирования информационной системы персональных данных из общей ЛВС.	до 31 декабря	
Контрольные мероприятия			
1.	Контроль за соблюдением режима обработки ПДн	Ежеквартально, в срок до 10-го числа месяца следующего за отчетным	Ответственный за организацию обработки персональных данных, администратор безопасности обработки персональных данных
2.	Контроль за соблюдением режима защиты	Ежеквартально, в срок до 10-го числа месяца следующего за отчетным	
3.	Контроль за выполнением антивирусной защиты	Ежеквартально, в срок до 10-го числа месяца следующего за отчетным	
4.	Контроль за соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Ежеквартально, в срок до 10-го числа месяца следующего за отчетным	
5.	Контроль за обеспечением резервного копирования	Ежеквартально, в срок до 10-го числа месяца следующего за отчетным	
6.	Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз	Ежеквартально, по мере необходимости	
7.	Поддержание в актуальном состоянии нормативно-организационных документов	По мере необходимости	