Управление образования администрации
Николаевского муниципального района
муниципальное бюджетное общеобразовательное учреждение средняя общеобразовательная школа имени Виктора Романовича Поликанова р.п. Многовершинный Николаевского муниципального района Хабаровского края

ВЫПИСКА ИЗ ПРИКАЗА

30.10.2020 №194-осн

р.п. Многовершинный

Об утверждении Политики информационной безопасности информационных систем персональных данных муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школе имени Виктора Романовича Поликанова р.п. Многовершинный Николаевского муниципального района Хабаровского края

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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»

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемую Политику информационной безопасности информационных систем персональных данных муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школе имени Виктора Романовича Поликанова р.п. Многовершинный Николаевского муниципального района Хабаровского края.
2. Разместить настоящий приказ на официальном сайте муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школе имени Виктора Романовича Поликанова р.п. Многовершинный Николаевского муниципального района Хабаровского края
3. Контроль за исполнением данного приказа оставляю за собой.

Директор МБОУ СОШ
Р.п. Многовершинный И.А.Павлюкова

Копия верна. Директор МБОУ СОШ р.п. Многовершинный И.А.Павлюкова

УТВЕРЖДЕНА

приказом директора МБОУ СОШ р.п. Многовершинный

от 30.10.2020 г. № 194-осн

ПОЛИТИКА
информационной безопасности информационных систем персональных данных муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школе имени Виктора Романовича Поликанова р.п. Многовершинный Николаевского муниципального района Хабаровского края

1. Общие положения

1.1. Настоящая Политика информационной безопасности информационных систем персональных данных (далее – Политика информационной безопасности) муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школе имени Виктора Романовича Поликанова р.п. Многовершинный Николаевского муниципального района Хабаровского края (далее – МБОУ СОШ р.п. Многовершинный) определяет основные направления в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, а именно порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, защищаемой информации и средств защиты информации, порядок обучения пользователей практике работы в информационных системах персональных данных, правила организации антивирусной и парольной защиты информационных систем персональных данных, порядок стирания защищаемой информации и уничтожения носителей защищаемой информации в МБОУ СОШ р.п. Многовершинный.

1.2. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

1.3. Информация и связанные с ней ресурсы должны быть доступны для авторизированных пользователей.

1.4. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожение данных.

1.5. Состав объектов защиты регламентируется в соответствии с «Перечнем персональных данных, обрабатываемых в МБОУ СОШ р.п. Многовершинный», утвержденный приказом директора МБОУ СОШ р.п. Многовершинный от 30 октября 2020 г. № 189 -осн «Об обработке персональных данных в муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школе имени Виктора Романовича Поликанова р.п. Многовершинный Николаевского муниципального района Хабаровского края».

Копия верна. Директор МБОУ СОШ р.п. Многовершинный **И.А.Павлюкова**

2. Основные понятия

Для целей настоящей Политики информационной безопасности используются следующие термины, определения и сокращения:

- информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

- конфиденциальность персональных данных – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

- несанкционированный доступ (НСД) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств;

- персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

- пользователь ИСПДн (пользователь) – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования;

- ПК – персональный компьютер;

- ПО – программное обеспечение;

- ПЭВМ – персональная электронно-вычислительная машина;

- СЗИ – средства защиты информации.

3. Порядок работы пользователей в части обеспечения безопасности ПДн при их обработке в ИСПДн

3.1. Допуск пользователей для работы на компьютерах ИСПДн осуществляется на основании приказа МБОУ СОШ р.п. Многовершинный и в соответствии с перечнем должностей МБОУ СОШ р.п. Многовершинный, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн. Для каждой ИСПДн приказом директора назначается администратор информационной безопасности. С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в ИСПДн приказом директора назначается ответственный за обеспечение безопасности информационных систем персональных данных (далее – Ответственный за безопасность).

3.2. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. Полномочия пользователей к информационным ресурсам определяются Ответственным за безопасность по согласованию с директором МБОУ СОШ р.п. Многовершинный.

3.3. Запись информации, содержащей ПДн, может осуществляться на машинные носители информации, соответствующим образом учтенные в Журнале учета машинных носителей информации.

4. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, защищаемой информации и средств

защиты информации

4.1. Администратор информационной безопасности обязан осуществлять не реже раза в месяц резервное копирование информации, содержащей ПДн.

4.2. Для хранения резервных копий в ИСПДн используются соответствующие машинные носители информации. Запрещается запись посторонней информации в электронный архив резервных копий.

4.3. При необходимости ремонта технических средств оборудование передается в сервисный центр производителя. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с установленным порядком уничтожения носителей защищаемой информации (п.8 настоящей Инструкции). Работа с использованием неисправных технических средств запрещается.

4.4. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в надежном месте и файлов настроек данных средств, хранящихся на зарегистрированных носителях.

4.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания.

4.6. В случае выявления сбоя в функционировании элементов ИСПДн и/или системы защиты ПДн администратор информационной безопасности в кратчайшие сроки, не превышающие одного рабочего дня, предпринимает меры по восстановлению работоспособности ИСПДн и/или системы защиты ПДн. Предпринимаемые меры по возможности согласуются с директором МБОУ СОШ р.п. Многовершинный. По необходимости иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

4.7. Все действия в процессе реагирования на инциденты должны документироваться в Журнале учета мероприятий по защите информации (Приложение 1).

5. Порядок обучения пользователей практике работы в ИСПДн в части обеспечения безопасности персональных данных

5.1. С вновь принятыми работниками МБОУ СОШ р.п. Многовершинный Ответственный за безопасность, назначенный приказом директора, в обязательном порядке проводит инструктаж по защите ПДн.

5.2. Пользователи должны продемонстрировать Ответственному за безопасность наличие необходимых знаний и умений для работы в ИСПДн. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности персональных данных, к работе в ИСПДн не допускаются.

6. Правила антивирусной защиты

6.1. К использованию на компьютерах, входящих в состав ИСПДн, допускаются только лицензионные и сертифицированные по требованиям безопасности антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанные средств.

6.2. Администратор информационной безопасности осуществляет контроль за периодическим обновлением антивирусных пакетов и их работоспособностью.

6.3. Антивирусное средство должно быть настроено таким образом, чтобы антивирусный контроль проводился в реальном времени. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).

6.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера ответственным за безопасность должна быть выполнена антивирусная проверка ИСПДн.

6.5. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в три месяца. Периодическая проверка жестких магнитных дисков на отсутствие программных вирусов должна проводиться не реже одного раза в месяц.

6.6. 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.) необходимо провести внеочередной антивирусный контроль компьютера.

6.7. При повреждении программных средств и информационных массивов программными вирусами должны выполняться мероприятия по восстановлению их работоспособности.

6.8. Обновление баз данных вирусных описаний средств антивирусной защиты, используемых для защиты серверов и рабочих станций, должно осуществляться централизованно администратором информационной безопасности без участия пользователей посредством механизма централизованного управления и обновления баз данных вирусных описаний.

6.9. Процедура обновления антивирусных баз должна проводиться ежедневно.

6.10. Для рабочих станций, являющихся автономными с точки зрения централизованного управления, обновление баз данных вирусных описаний должно осуществляться непосредственно самими работниками школы, за которыми закреплен данный компьютер. В качестве источника обновлений может выступать общая папка, содержащая необходимые файлы, на одном из компьютеров ИСПДн.

7. Правила парольной защиты

7.1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИСПДн самостоятельно с учетом сле-

дующих требований:

7.1.1. Длина пароля должна быть не менее восьми символов.

7.1.2. В числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.).

7.1.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).

7.2. При смене пароля новое значение должно отличаться от предыдущих.

7.3. Пользователь не имеет права сообщать личный пароль другим лицам.

7.4. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

7.5. В случае возникновения технологической необходимости использования имен и паролей работников (исполнителей) в их отсутствие, работники по возвращению обязаны сразу же сменить значения паролей.

7.6. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение трех месяцев.

7.7. Внеплановая смена личного пароля или удаления учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой на основании указания директора МБОУ СОШ р.п. Многовершинный.

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

7.9. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно приняты меры по восстановлению парольной защиты.

8. Порядок обращения с носителями персональных данных

8.1. Все машинные носители информации, используемые в ИСПДн, подлежат обязательному учету в Журнале учета машинных носителей информации. Места хранения должны быть учтены в Журнале учета места хранения носителей персональных данных (Приложение 2).

8.2. Выдача машинных носителей информации фиксируется в Журнале учета машинных носителей информации и подтверждается подписью пользователя. Все машинные носители информации должны маркироваться:

- на жестких магнитных дисках и внешних накопителях (USB и т.п.) штамп проставляется на этикетке, закрепленной с помощью липкой ленты на лицевой стороне носителя;
- на несъемных носителях информации штамп ставится на корпусе системного блока персонального компьютера, в котором установлен носитель. Несъем-

ные жесткие магнитные диски учитываются отдельно и (или) в составе системного блока ПК. Системный блок ПК для маркировки и контроля его наличия вскрывается в присутствии ответственного за его эксплуатацию, а для ПК, находящегося на гарантийном или после гарантийном обслуживании, кроме того и в присутствии (с разрешения) представителя обслуживающей организации.

8.3. После вскрытия, маркировки или контроля наличия системный блок должен быть надежно опечатан двумя наклейками с печатью организации и подписями ответственного ПК и администратора информационной безопасности.

8.4. В случае служебной необходимости (убытие в отпуск, увольнение, перевод и т.п.) машинный носитель может быть передан другому пользователю ИСПДн. Передача носителя другим пользователям осуществляется с фиксацией факта передачи в Журнале учета машинных носителей информации.

8.5. В оде обратного приема проверяются учетные данные передаваемого носителя – производитель, модель и серийный номер. По результатам проверки администратором информационной безопасности делается отметка в графе обратного приема.

8.6. Вышедшие из строя машинные носители ПДн ремонту не подлежат. Такие носители уничтожаются методом разборки и физического разрушения носителей информации.

8.7. Уборка и технические работы в помещениях, в которых установлены ПК с носителями информации, содержащими персональные данные, производятся в присутствии одного из должностных лиц, допущенных в указанное помещение установленным порядком.

8.8. Для хранения носителей ПДн используются специально оборудованные хранилища (сейфы, шкафы и т.п.), исключающие возможность несанкционированного копирования информации и хищения носителей.

8.9. Необходимо обеспечивать раздельное хранение ПДн (материальных носителей ПДн на бумажной основе), обработка которых осуществляется в различных целях.

8.10. Машинные носители с резервными копиями ПДн не выдаются для работы обычным пользователям и служат только для восстановления ПДн в случае аварии или поломки основного машинного носителя ПДн.

8.11. Машинные носители с резервными копиями ПДн рекомендуется хранить в отдельном хранилище.

8.12. В случае, если МБОУ СОШ р.п. Многовершинный на основании договора поручает хранение носителей ПДн другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности ПДн и безопасности ПДн при их хранении.

8.13. В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИСПДн.

8.14. Стирание должно производиться по технологии, предусмотренной для данного типа носителя, с применением средств гарантированного уничтожения информации (допускается задействовать механизмы затирания, встроенные в сер-

тифицированные средства защиты информации).

8.15. Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантированное стирание информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны быть достаточны для исключения возможности восстановления информации.

8.16. Бумажные носители уничтожают путем сжигания или с помощью любых бумагорезательных машин.

8.17. По факту уничтожения или стирания носителей составляется акт уничтожения, в журналах учета делаются соответствующие записи.

Копия верна. Директор МБОУ СОШ р.п. Многовершинный

И.А.Павлюкова

Приложение 1

к Политике информационной безопасности
информационных систем персональных
данных МБОУ СОШ р.п. Многовершинный

ЖУРНАЛ
учета мероприятий по защите информации

№ п/п	Дата	Мероприятие	Результат	Должность и ФИО исполнителя	Подпись

Начат _____ 20___ г.
Окончен _____ 20___ г.

Срок хранения:
Осн.:

Приложение 2

к Политике информационной безопасности информационных систем персональных данных МБОУ СОШ р.п. Многовершинный

ЖУРНАЛ
учета мест хранения носителей персональных данных

№ п/п	Наименование (сейф, металл. шкаф, кладовая, склад, спец. хранилище)	Инвентарный номер места хранения	Местонахождение (отдел, номер кабинета, адрес)	Что хранится	Фамилия ответственного за шкаф, сейф, спец. хранилище	Кол. ключей и их номера	Подпись, получившего рабочего экз. ключ.	Место хранения запасного ключа	Примечание

Начат _____ 20___ г.
Окончен _____ 20___ г.

Срок хранения:
Осн.: