ПРИНЯТО
Заседание Педагогического совета
Протокол от 29.03.2024 № 11

УТВЕРЖДЕНО
Директор МБОУ СОШ с.Чуваш-Кубово
Им.Пономарева П.И.
_____П.И. Коваленко
Приказ от 29.03.2024 г. № 29

ИНСТРУКЦИЯ
по обращению с материальными носителями персональных данных
МБОУ СОШ с.Чуваш-Кубово им.Пономарева П.И.

Допуск пользователей для работы в информационной системе персональных данных (далее по тексту- ИСПДн), осуществляется в соответствии с приказом директора школы и разрешительной системой доступа. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам компьютера. При этом для хранения файлов, содержащих конфиденциальную информацию, разрешается использовать только специально выделенные каталоги на несъемных носителях информации, а также соответствующим образом учтенные съёмные носители информации. Присвоение пользователю полномочий доступа к ресурсам компьютера, состав необходимого системного и прикладного программного обеспечения для решения поставленных задач и определение возможного времени работы пользователя в ИСПДн, осуществляется при первичной регистрации пользователя специалистом защиты информации. Пользователь отвечает за правильность включения и выключения технических средств и систем, входа в систему и все действия при работе в ИСПДн.

Вход в систему может осуществляться по разным моделям:
Модель № 1 - вход пользователя в систему предусматривающую наличие пароля осуществляется на основе ввода имени, присвоенного при первичной регистрации и ввода личного пароля. Требования к парольной защите определяется инструкцией по парольной защите (Модель №1).
Модель № 2 - вход пользователя в систему осуществляется на основе персонального средства (в форме - фактора USB-ключа) аутентификации и защищённого хранения данных, аппаратно-поддерживающего работу с цифровыми сертификатами и электронной цифровой подписью (ЭЦП) (далее - eToken).

В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам пользователя осуществляется периодическая (раз в месяц) замена пароля постоянного пользователя. Замена личного пароля осуществляется пользователем самостоятельно. (Модель №1).
При работе со съемными носителями информации пользователь каждый раз перед началом работы обязан проверить их на наличие вирусов с использованием установленных антивирусных программ.
Пользователь обязан:
• знать и строго выполнять установленные правила и обязанности по доступу к защищаемым ресурсам и соблюдению принятого режима информационной безопасности;
• обеспечить правильность вводимых данных;
• своевременно сообщать специалисту по защите информации об изменениях статуса пользователя;
• незамедлительно сообщить специалисту по защите информации факты выявления инцидентов с доступом к конфиденциальной информации.

В процессе работы пользователю запрещается:

• использовать для постоянного хранения и обработки конфиденциальной информации каталюги несъемных носителей информации, за исключением выделенных каталогов;

• осуществлять попытки несанкционированного доступа к ресурсам операционной системы;

• в рамках выделенных ресурсов и полномочий доступа к ним обрабатывать информацию с уровнем конфиденциальности, выше заявленного при регистрации;

• пытаться подменять функции администратора по перераспределению времени работы и полномочий доступа к ресурсам компьютера;

• покидать помещение с незаблокированной учетной записью;

•отключать установленные средства защиты информации;

• использовать машинные носители без их предварительной проверки антивирусными средствами;

• устанавливать программное обеспечение;

• менять параметры конфигурации ранее установленных программных средств;

• использовать пароль, предоставленный специалистом по защите информации для первоначального доступа в качестве постоянного рабочего пароля (Модель №1);

• использование различными пользователями одной и той же учетной записи, даже если пользователи имеют одинаковые полномочия по доступу (Модель №1);

• использование различными пользователями одного и того же eToken, даже если пользователи имеют одинаковые полномочия по доступу (Модель №2);

• запрещается передавать в любом виде или сообщать идентификаторы и пароли для доступа другим лицам, в том числе и своим руководителям (Модель №1);

•запрещается передавать eToken другим лицам, в том числе и своим руководителям(Модель №2);

• хранение пароля на любых твердых носителях, позволяющих другим лицам получить информацию о пароле (Модель №1).

Ответственность за сохранность и правильное использование информации, ставшей известной в процессе обработки конфиденциальной информации несет пользователь. Возможность получения технического доступа к конфиденциальной информации не дает права пользователям обработки такой информации, если им не предоставлены права доступа к этой информации. Такие действия рассматриваются как попытки несанкционированного доступа. При выявлении инцидентов с доступом к конфиденциальной информации доступ пользователей к ней может быть ограничен до окончания расследования инцидента, о чем пользователь уведомляется в кратчайшие сроки. По результатам служебного расследования нарушитель может быть лишен прав доступа к конфиденциальной информации, материалы расследования могут быть направлены в соответствующие службы для привлечения нарушителя к ответственности. Пользователь несет ответственность за все действия, совершенные от имени его учетной записи, если не доказан факт несанкционированного использования этой учетной записи.

В моделе № 1 личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями 4 автоматизированной системы самостоятельно с учетом следующих требований:

• длина пароля должна быть не менее 6 символов;

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

• пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

• при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;

• личный пароль пользователь не имеет права сообщать никому. 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. Для генерации «стойких» значений паролей могут применяться специальные программные средства. При наличии технологической необходимости использования eToken, имен и паролей некоторых сотрудников (исполнителей) в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.):

- в Модели № 1 такие сотрудники обязаны сразу же после сменсвоих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение специалисту по защите информации.

Сотрудники обязаны в опечатанном пенале передавать eToken на хранение специалисту по защите информации. Опечатанные конверты должны храниться в сейфе.

При нарушениях пользователем правил, связанных с информационной безопасностью, он несет ответственность, установленную действующим законодательством Российской Федерации.