ГБОУ РХ «Черногорская школа-интернат»

СОГЛАСОВАНО на общем собрании трудового коллектива Протокол № 2 от «11» 01 2022 г.	УТВЕРЖДАЮ и. о. директора _____ С. И. Бутенко Приказ № 10 от 10 » 01 2022 г.

ИНСТРУКЦИЯ
по организации парольной защиты

1. Общие положения

1.1. Инструкция по организации парольной защиты (далее - Инструкция) разработана в соответствии со следующими нормативными правовыми актами: Федеральным законом от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации; Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»; Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными Постановлением Правительства РФ от 01.11.2012 №1119; Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 №17 (Зарегистрировано в Минюсте России 31.05.2013 №28608); Специальными требованиями и рекомендации по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30.08.2002 № 282.

1.2. Настоящая Инструкция призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах ГБОУ РХ «Черногорская школа-интернат», а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.3. Настоящая инструкция оперирует следующими основными понятиями:

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

ИСПДн – информационная система персональных данных.

Компрометация- факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

Объект доступа - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Пароль – уникальный признак субъекта доступа, который является его (субъекта) секретом.

Правила доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Субъект доступа - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Несанкционированный доступ - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или АС.

2. Правила формирования паролей

2.1. 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.

2.2. При технологической необходимости использования имен и паролей некоторых работников (исполнителей) в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т. п.) такие работники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передать на хранение ответственному за информационную безопасность. Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для их опечатывания рекомендуется использовать печать отдела кадров.

3. Ввод пароля

3.1. 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.).

4. Порядок смены личных паролей

4.1. Смена паролей проводится регулярно, не реже одного раза в шесть месяцев.

4.2. 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.

4.3. 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.

4.4. Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 4.5. Инструкции и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

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

5. Хранение пароля

5.1 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.

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

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

6. Действия в случае утери и компрометации пароля

6.1. В случае утери или компрометации пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 4.3 или п. 4.4 Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Ответственность при организации парольной защиты

7.1. Владельцы паролей должны быть ознакомлены под расписку с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение информации о пароле.

7.2. Ответственность за организацию парольной защиты в ГБОУ РХ «Черногорская школа-интернат» возлагается на администратора безопасности.

Учитель ответственный за защиту персональных данных Коваленко Л.Н.

возможность обеспечения заданных свойств обезличенных данных, относятся:
обратимость (возможность преобразования, обратного обезличиванию (деобезличивание), которое позволит привести обезличенные данные к исходному виду, позволяющему определить принадлежность персональных данных конкретному субъекту, устранить анонимность);
вариативность (возможность внесения изменений в параметры метода и его дальнейшего применения без предварительного деобезличивания массива данных);
изменяемость (возможность внесения изменений (дополнений) в массив обезличенных данных без предварительного деобезличивания);
стойкость (стойкость метода к атакам на идентификацию субъекта персональных данных);
возможность косвенного деобезличивания (возможность проведения деобезличивания с использованием информации других операторов);
совместимость (возможность интеграции персональных данных, обезличенных различными методами);
параметрический объем (объем дополнительной (служебной) информации, необходимой для реализации метода обезличивания и деобезличивания);
возможность оценки качества данных (возможность проведения контроля качества обезличенных данных и соответствия применяемых процедур обезличивания установленным для них требованиям).
6. Требования к методам обезличивания подразделяются на:
требования к свойствам обезличенных данных, получаемых при применении метода обезличивания;
требования к свойствам, которыми должен обладать метод обезличивания.
7. К требованиям к свойствам получаемых обезличенных данных относятся:
сохранение полноты (состав обезличенных данных должен полностью соответствовать составу обезличиваемых персональных данных);
сохранение структурированности обезличиваемых персональных данных;
сохранение семантической целостности обезличиваемых персональных данных;
анонимность отдельных данных не ниже заданного уровня (количества возможных сопоставлений обезличенных данных между собой для деобезличивания).
8. К требованиям к свойствам метода обезличивания относятся:
обратимость (возможность проведения деобезличивания);
возможность обеспечения заданного уровня анонимности;
увеличение стойкости при увеличении объема обезличиваемых персональных данных.
9. Выполнение приведенных в пунктах 7 и 8 Требований и методов требований обязательно для обезличенных данных и применяемых методов обезличивания.
10. Методы обезличивания должны обеспечивать требуемые свойства обезличенных данных, соответствовать предъявляемым требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных программных средах и позволять решать поставленные задачи обработки персональных данных.
11. К наиболее перспективным и удобным для практического применения относятся следующие методы обезличивания:
метод введения идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным); метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений);

метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);
метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных).
12. Метод введения идентификаторов реализуется путем замены части персональных данных, позволяющих идентифицировать субъекта, их идентификаторами и созданием таблицы соответствия.
Метод обеспечивает следующие свойства обезличенных данных:
полнота;
структурированность;
семантическая целостность;
применимость.
Оценка свойств метода:
обратимость (метод позволяет провести процедуру деобезличивания);
вариативность (метод позволяет перейти от одной таблицы соответствия к другой без проведения процедуры деобезличивания);
изменяемость (метод не позволяет вносить изменения в массив обезличенных данных без предварительного деобезличивания);
стойкость (метод не устойчив к атакам, подразумевающим наличие у лица, осуществляющего несанкционированный доступ, частичного или полного доступа к справочнику идентификаторов, стойкость метода не повышается с увеличением объема обезличиваемых персональных данных);
возможность косвенного деобезличивания (метод не исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);
совместимость (метод позволяет интегрировать записи, соответствующие отдельным атрибутам);
параметрический объем (объем таблицы (таблиц) соответствия определяется числом записей о субъектах персональных данных, подлежащих обезличиванию);
возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).
Для реализации метода требуется установить атрибуты персональных данных, записи которых подлежат замене идентификаторами, разработать систему идентификации, обеспечить ведение и хранение таблиц соответствия.
13. Метод изменения состава или семантики реализуется путем обобщения, изменения или удаления части сведений, позволяющих идентифицировать субъекта.
Метод обеспечивает следующие свойства обезличенных данных:
структурированность;
релевантность;
применимость;
анонимность.
Оценка свойств метода:
обратимость (метод не позволяет провести процедуру деобезличивания в полном объеме и применяется при статистической обработке персональных данных);
вариативность (метод не позволяет изменять параметры метода без проведения предварительного деобезличивания);
изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);

стойкость (стойкость метода к атакам на идентификацию определяется набором правил реализации, стойкость метода не повышается с увеличением объема обезличиваемых персональных данных);
возможность косвенного деобезличивания (метод исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);
совместимость (метод не обеспечивает интеграции с данными, обезличенными другими методами);
параметрический объем (параметры метода определяются набором правил изменения состава или семантики персональных данных);
возможность оценки качества данных (метод не позволяет проводить анализ, использующий конкретные значения персональных данных).
Для реализации метода требуется выделить атрибуты персональных данных, записи которых подвергаются изменению, определить набор правил внесения изменений и иметь возможность независимого внесения изменений для данных каждого субъекта.
При этом возможно использование статистической обработки отдельных записей данных и замена конкретных значений записей результатами статистической обработки (средние значения, например).
14. Метод декомпозиции реализуется путем разбиения множества записей персональных данных на несколько подмножеств и создание таблиц, устанавливающих связи между подмножествами, с последующим раздельным хранением записей, соответствующих этим подмножествам.
Метод обеспечивает следующие свойства обезличенных данных:
полнота;
структурированность;
релевантность;
семантическая целостность;
применимость.
Оценка свойств метода:
обратимость (метод позволяет провести процедуру деобезличивания);
вариативность (метод позволяет изменить параметры декомпозиции без предварительного деобезличивания);
изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);
стойкость (метод не устойчив к атакам, подразумевающим наличие у злоумышленника информации о множестве субъектов или доступа к нескольким частям раздельно хранимых сведений);
возможность косвенного деобезличивания (метод не исключает возможность деобезличивания с использованием персональных данных, имеющихся у других операторов);
совместимость (метод обеспечивает интеграцию с данными, обезличенными другими методами);
параметрический объем (определяется числом подмножеств и числом субъектов персональных данных, массив которых обезличивается, а также правилами разделения персональных данных на части и объемом таблиц связывания записей, находящихся в различных хранилищах);
возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).
Для реализации метода требуется предварительно разработать правила декомпозиции, правила установления соответствия между записями в различных хранилищах, правила внесения изменений и дополнений в записи и хранилища.

15. Метод перемешивания реализуется путем перемешивания отдельных записей, а также групп записей между собой.
Метод обеспечивает следующие свойства обезличенных данных:
полнота;
структурированность;
релевантность;
семантическая целостность;
применимость;
анонимность.
Оценка свойств метода:
обратимость (метод позволяет провести процедуру деобезличивания);
вариативность (метод позволяет изменять параметры перемешивания без проведения процедуры деобезличивания);
изменяемость (метод позволяет вносить изменения в набор обезличенных данных без предварительного деобезличивания);
стойкость (длина перестановки и их совокупности определяет стойкость метода к атакам на идентификацию);
возможность косвенного деобезличивания (метод исключает возможность проведения деобезличивания с использованием персональных данных, имеющихся у других операторов);
совместимость (метод позволяет проводить интеграцию с данными, обезличенными другими методами); параметрический объем (зависит от заданных методов и правил перемешивания и требуемой стойкости к атакам на идентификацию);
возможность оценки качества данных (метод позволяет проводить анализ качества обезличенных данных).
Для реализации метода требуется разработать правила перемешивания и их алгоритмы, правила и алгоритмы деобезличивания и внесения изменений в записи.
Метод может использоваться совместно с методами введения идентификаторов и декомпозиции.