«РАССМОТРЕНО»
На Педагогическом совете
КОУ РК «ЛКШИ»
Протокол № 2
от «01» 11 2023 г.

«УТВЕРЖДАЮ»
от «02» 11 2023 г.
Директор КОУ РК «ЛКШИ
Харкебенов А. А.

ПОЛОЖЕНИЕ
об обеспечении автоматизированной информационной системы (АИС) КОУРК «Лаганская коррекционная школа – интернат»

I.Общие положения

1. Настоящая инструкция определяет порядок организации работ по обеспечению защиты информации, обрабатываемой и хранимой в автоматизированных информационных системах (АИС) КОУРК «Лаганская коррекционная школа-интернат», определяет правовые последствия за нарушение правил информационной безопасности согласно Российского законодательства.
2. Инструкция разработана в соответствии с Конституцией Российской Федерации, Федеральными законами и иными нормативно-правовыми актами Российской Федерации, приказами Министерства образования Российской Федерации, Положением об обеспечении безопасности автоматизированной информационной системы КОУРК «ЛКШИ».
3. В своей работе сотрудники доступа к информационным ресурсам АИС КОУРК «ЛКШИ» должны руководствоваться требованиями настоящей инструкции, приказом Министерства образования Российской Федерации 343-55-148 ИН/СМИ от 03.07.02г., а также другими документами о порядке разграничения доступа на ЭВМ и защиты информации ограниченного доступа, всей информационной системы в целом, локальных вычислительных сетей и т.д.
4. Термины и определения, употребляемые в настоящей инструкции:

Автоматизированная информационная система- организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной технике и связи, реализующих информационные процессы.

Программное обеспечение (ПО) - совокупность компьютерных программ, описаний и инструкций по их применению на ЭВМ.

Информационные ресурсы (ИР) – отдельные документы и отдельные массивы документов, документы и массивы документов в АИС.

Информационное обеспечение (ИО) – совокупность единой системы классификации и кодирования технико-экономической информации, унифицированной системы документации и информационных ресурсов.

База данных (БД) – объективная форма представления и организации совокупности данных (например, статей, расчётов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Объект ЭВТ –электронно-вычислительная техника (ЭВМ, принтер и т.п), группа ПЭВМ в одном помещении, выполняющая одну задачу, локальная сеть ЭВМ.

Подразделение-пользователь (также сотрудник доступа) –пользователь, получивший разрешение (доступ) к БД и информационным ресурсам КОУРК «ЛКШИ».

Сотрудник доступа (пользователь) – лицо, непосредственно осуществляющее доступ к информационным ресурсам.

Собственник информационных ресурсов, автоматизированных информационных систем, технологий и средств обеспечения – сотрудник, осуществляющий владение и пользование указанными объектами и реализующий полномочия владения, пользования, распоряжения указанными объектами. Собственник ИР имеет право устанавливать в пределах своей компетенции режим и правила обработки, защиты автоматизированных ИР и доступа к ним, определять условия расположения документами при их копировании и распространении.

Ответственный за безопасность автоматизированной информационной системы (далее Ответственный) –лицо, осуществляющее контроль за соблюдением информационной безопасности, назначенное приказом по КОУРК «ЛКШИ».

Локальная вычислительная сеть (ЛВС) – объединенные в единый комплекс и расположенные на небольшом расстоянии друг от друга ЭВМ для оперативного обмена данными между пользователями.

II. Основные положения

2.1. Основными видами угроз безопасности информационных систем являются:

* противоправные действия третьих лиц;
* ошибочные действия пользователей и обслуживающего персонала АИС;
* отказы и сбои технических средств АИС, приводящие к её модификации, блокированию, уничтожению или несанкционированному копированию, а также нарушению правил эксплуатации ЭВМ и сетевого оборудования.

2.2. Реализация угроз безопасности информации сопровождается нарушением законных прав собственника ИР или пользователя этих ресурсов, нанесением ему материального ущерба.

2.3. Целью защиты информации является:

2.3.1. Предотвращение утечки, хищения, утраты, подделки информации, а также неправомерных действий по уничтожению, модификации, искажению, несанкционированному копированию, блокированию информации, предотвращение других форм незаконного вмешательства в ИР и информационные системы обеспечения правового режима документированной информации как субъекта собственности.

2.3.2. Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах.

2.3.3. Сохранение конфиденциальности информации в соответствии с законодательством Российской Федерации.
2.3.4. Обеспечение прав сотрудников в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.
2.4. Сотрудники, получающие доступ к БД и другим ИР, должны изучить настоящую инструкцию и оставить письменное подтверждение (подпись) о неразглашении ими информации, к которой они имеют доступ, паролей, а также в том, что за нарушение правил информационной безопасности и данной инструкции они несут персональную ответственность в соответствии с законодательством Российской Федерации.
Форма регистрации ознакомления сотрудников с данной инструкцией и соблюдением правил, изложенных в ней, приведена в Приложении №1.
2.5. Лица, ответственные за информационную безопасность, назначаются приказом по КОУРК «ЛКШИ».

III. Обеспечение сохранности информации

3.1. Для обеспечения сохранности электронных ИР КОУРК «ЛКШИ» необходимо соблюдать следующие требования:

* руководитель подразделения, в ведении которого находятся системы управления БД и ИР ЛВС КОУРК «ЛКШИ», должны быть назначены лица, ответственные за резервное копирование конкретного вида информации;

- резервное копирование Ир должно производится в соответствии с документацией на используемое ПО;
- в случае сбоя или порчи восстановление ИР из резервных копий производится в соответствии с документацией на используемое ПО;
- на компьютерах локальных пользователей сети КОУРК «ЛКШИ» должны быть установлены средства защиты от компьютерных вирусов и других вредоносных программ;
- для копирования информации не должны использоваться непроверенные на наличие компьютерных вирусов и других вредоносных программ носители информации.

3.2. Сотрудникам запрещается:

* установка и использование при работе с ЭВТ вредоносных программ, ведущих к блокированию работы сети;
* самовольное изменение:

- IP-адресов;
-mac- адресов сетевого адаптера;
-других сетевых настроек;
-вскрытие блоков объектов ЭВТ, модернизация или модификация объектов

ЭВТ и ПО. При необходимости модернизация ЭВТ и ПО согласуется с Ответственным КОУРК «ЛКВШИ»;

- несанкционированная передача компьютеров с прописанными сетевыми настройками. Пересдача компьютеров из одного подразделения в другое производится только с предварительно удаленными сетевыми настройками и с обязательным уведомлением Ответственного КОУРК «ЛКШИ»;

3.3. Сведения, содержащиеся в электронных документах и БД КОУРК «ЛКШИ», должны использоваться только в служебных целях в рамках полномочий сотрудника, работающего с соответствующими материалами.

3.3.1. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации.

VI. Защита от несанкционированного доступа

4.1. Защита от несанкционированного доступа осуществляется:
4.1.1. Идентификацией и проверкой подлинности сотрудников при доступе к ИР (при несовпадении идентификаторов или паролей пользователей дальнейшая работа блокируется).
4.1.2. Разграничением доступа к обрабатываемым массивам данных, субъект доступа имеет доступ к там ИР, которые разрешены для него согласно приказа по КОУРК «ЛКШИ». Для осуществления доступа к ИР, ответственный назначает конкретному лицу идентифицирующее имя пользователя и персональный пароль доступа, устанавливает разрешенные согласно приказа по КОУРК «ЛКШИ» права доступа к ИР школы.
4.2. Ответственный должен осуществлять мероприятия по обеспечению защиты ИР от несанкционированного доступа и непреднамеренных изменений и разрешений, а также иметь в наличии средства восстановления, резервные копии, предусматривающие процедуру восстановления свойств информационных ресурсов после сбоев и отказов оборудования.

Приложение №1

С настоящей инструкцией ознакомлен, о неразглашении пароля и полученной информации при осуществлении доступа к базам данных и иных информационных ресурсам, а также о персональной ответственности, предусмотренной за нарушение правил информационной безопасности, в соответствии с законодательством Российской Федерации и за соблюдение требований данной инструкции предупрежден:

№п/п	Ф.И.О. сотрудника	Личная подпись