Муниципальное бюджетное общеобразовательное учреждение «Караванный казачий кадетский корпус Оренбургского района» Оренбургской области

(МБОУ «Караванный казачий кадетский корпус»)

СОГЛАСОВАНО

Педагогическим советом

МБОУ «Караванный казачий кадетский корпус»

Протокол № 5 от 12.02.2024

УТВЕРЖДАЮ

директор МБОУ «Караванный казачий кадетский корпус»

_____ Д.А. Позюбан

«12» 02 2024г.

Положение

об информационной безопасности МБОУ «Караванный казачий кадетский корпус»

1. Общие положения

1.1. Информационная безопасность является одним из составных элементов комплексной безопасности в МБОУ «Караванный казачий кадетский корпус» (далее— Корпус), порядок организации работ по её созданию и функционированию.

1.2. Данное положение разработано в соответствии с Федеральным законом Российской Федерации от 29 декабря 2012 г. № 273-ФЗ "Об образовании в Российской Федерации" п. 3 ст. 47 Трудовым кодексом РФ от 30.12.2001 № 197- ФЗ (с изм. и доп.), Федеральным законом от 29.12.2012 г. №273-ФЗ «Об образовании в Российской Федерации». 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" и имеет статус локального нормативного акта образовательной организации. Если нормами действующего законодательства РФ предусмотрены иные требования, чем настоящим Положением, применяются нормы законодательства РФ.

1.3. Под информационной безопасностью Корпуса следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности. Система информационной безопасности направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

1.4. Использование сети Интернет в образовательной организации подчинено следующим принципам:

-соответствие образовательным целям;

-способствование гармоничному формированию и развитию личности;

- «уважение закона, авторских и смежных прав, а также иных прав, чести и достоинства других граждан и пользователей сети Интернет;

-приобретение новых навыков и знаний;

-расширение применяемого спектра учебных и наглядных пособий;

-социализация личности, введение в информационное общество.

1.5. К объектам информационной безопасности в Корпусе относятся:

• информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных;

• информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. персональные данные;

• средства и системы информатизации — средства вычислительной и организационной техники, локальной сети, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации.

1.6. Система информационной безопасности (далее - СИБ) должна обязательно обеспечивать:

-конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата);

-целостность (точность и полноту информации и компьютерных программ);

-доступность (возможность получения пользователями информации в пределах их компетенции).

1.7. Обеспечение информационной безопасности осуществляется по следующим направлениям:

• правовая зашита - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

• организационная зашита - это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;

• инженерно-техническая защита - это использование различных технических средств, препятствующих нанесению ущерба.

2. Правовые нормы обеспечения информационной безопасности

2.1. *Корпус имеет право* определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных обучающихся, работников Корпуса, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз.

2.2. Корпус обязан обеспечить сохранность конфиденциальной информации.

2.3. Администрация корпуса:

• назначает ответственного за обеспечение информационной безопасности;

• издаёт нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
• имеет право включать требования по обеспечению информационной безопасности в коллективный договор;
• имеет право включать требования по защите информации в договоры по всем видам деятельности;
• разрабатывает перечень сведений конфиденциального характера;
• имеет право требовать защиты интересов школы со стороны государственных и судебных инстанций.
2.4. Организационные и функциональные документы по обеспечению информационной безопасности:
• приказ директора Корпуса о назначении ответственного за обеспечение информационной безопасности;
• должностные обязанности ответственного за обеспечение информационной безопасности;
• перечень защищаемых информационных ресурсов и баз данных;
• инструкция, определяющая порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников Корпуса и др.
2.5. Порядок допуска сотрудников корпуса к информации предусматривает:
• принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
• ознакомление работника с нормами законодательства РФ и Корпуса об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
• инструктаж работника специалистом по информационной безопасности;
• контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

3. Использование сети Интернет

3.1. Использование сети Интернет в Корпусе осуществляется в целях образовательного процесса. В рамках развития личности, ее социализации и получения знаний в области компьютерной грамотности лицо может осуществлять доступ к ресурсам не образовательной направленности.
3.2. Работники Корпуса вправе:
• размещать информацию в сети Интернет на интернет-ресурсах корпуса;
• иметь учетную запись электронной почты на интернет-ресурсах Корпуса.
3.3. Работникам Корпуса запрещено размещать в сети Интернет и на образовательных ресурсах информацию, противоречащую требованиям законодательства РФ и локальным нормативным актам Корпуса:
•не относящуюся к образовательному процессу и не связанную с деятельностью Корпуса;
•нарушающую нравственные и этические нормы, требования профессиональной этики.
3.4. Обучающиеся Корпуса вправе:
• использовать ресурсы, размещенные в сети Интернет, в том числе интернет-ресурсы Корпуса, в порядке и на условиях, которые предусмотрены настоящим Положением.

• размещать информацию и сведения на интернет-ресурсах Корпуса.

3.5. Обучающемся запрещено:

•находиться на ресурсах, содержание и тематика которых недопустима для несовершеннолетних и / или нарушает законодательство РФ;

•осуществлять любые сделки через интернет;

•загружать файлы на компьютер Корпуса без разрешения уполномоченного лица;

• распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.6. Запрет и снятие такого запрета на допуск пользователей к работе в сети Интернет устанавливает уполномоченное лицо, назначенное приказом директора Корпуса.

3.7. Если в процессе работы пользователем будет обнаружен ресурс, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить об этом уполномоченному лицу с указанием интернет-адреса (URL) и покинуть данный ресурс.

3.7.1. Уполномоченное лицо обязано:

• принять сообщение пользователя;

• принять меры по отключению выхода на данный ресурс с интернет ресурсов Корпуса;

• если обнаруженный ресурс явно нарушает законодательство РФ - сообщить о нем по специальной "горячей линии" для принятия мер в соответствии с законодательством РФ (в течение суток).

Передаваемая информация должна содержать:

в интернет-адрес (URL) ресурса;

• тематику ресурса, предположения о нарушении ресурсом законодательства РФ либо несовместимости с задачами образовательного процесса;

• дату и время обнаружения;

•информацию об установленных в образовательной организации технических средствах ограничения доступа к информации.

4. Мероприятия по обеспечению информационной безопасности

4.1. Для обеспечения информационной безопасности в Корпусе требуется проведение следующих первоочередных мероприятий:

• защита интеллектуальной собственности Корпуса;

• защита компьютеров, локальных сетей и сети подключения к системе Интернета;

• организация защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся Корпуса;

• учет всех носителей конфиденциальной информации.

5. О системном администрировании и обязанностях ответственного за информационную безопасность

5.1. Задачи, связанные с мерами системного администрирования, обеспечивающего информационную безопасность, являются частью работы технического специалиста (внесено в обязанности учителя информатики, технического специалиста) в МБОУ «Караванный казачий кадетский корпус».

5.2. Для решения задач информационной безопасности технический специалист обязан:

• следить за соблюдением требований по парольной защите, в том числе осуществлять

изменение паролей по мере необходимости (утрата пароля, появление новых пользователей в связи с изменением кадрового состава и пр.);

- обеспечивать функционирование программно-аппаратного комплекса защиты по внешним цифровым линиям связи;
- обеспечивать мероприятия по антивирусной защите, как на уровне серверов, так и на уровне пользователей;
- обеспечивать нормальное функционирование системы резервного копирования.

6. Антивирусная защита

6.1. Правила пользования внешними сетевыми ресурсами (Интернет, электронная почта и т.д.).

Основным способом проникновения компьютерных вирусов на компьютер пользователя в настоящее время является Интернет и электронная почта. В связи с этим не допускается работа без организации антивирусной защиты. Антивирусная защита организуется посредством лицензионного антивирусного программного обеспечения.

6.2. Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в день.

6.3. За своевременное обновление антивирусного программного обеспечения отвечает учитель информатики.