РАССМОТРЕНО И ПРИНЯТО

на заседании Общего собрания
работников и представителей
обучающихся, студентов

Протокол от 28 августа.2025 № 16

УТВЕРЖДАЮ

Директор ГБПОУ «ВКМиС им. Н. Сердюкова»

_____ Р.С. Лиховцов

28.08.2025

ПОЛОЖЕНИЕ

о службе (ответственном лице) информационной безопасности государственного бюджетного профессионального образовательного учреждения «Волгоградский колледж машиностроения и связи имени Героя Советского Союза Николая Сердюкова»

1. Общие положения

1.1 Настоящее Положение о службе (ответственном лице) информационной безопасности государственного бюджетного профессионального образовательного учреждения «Волгоградский колледж машиностроения и связи имени Героя Советского Союза Николая Сердюкова» (далее - колледж) разработано в соответствии:

- ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- ст. 9 Закона № 149-ФЗ, п. 5 - информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей подлежит защите в случаях, предусмотренных законом (государственная тайна);
- гл. 14 Трудового кодекса РФ (далее - ТК РФ) - защита персональных данных работника;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных;
- Постановлением Правительства РФ от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)».

1.2 Настоящее Положение определяет задачи, функции, обязанности, ответственность и права ответственных за информационную безопасность Колледжа.

1.3 Ответственный за информационную безопасность назначаются приказом директора Колледжа.

1.4 Ответственный за информационную безопасность подчиняются директору Колледжа.

1.5 Ответственный за информационную безопасность в своей работе руководствуется настоящим Положением.

1.6 Ответственный за информационную безопасность в пределах своих функциональных обязанностей обеспечивает безопасность информации, обрабатываемой, передаваемой и хранимой при помощи информационных средств Колледжа.

2. Основные задачи и функции ответственного за информационную безопасность

2.1 Основными задачами ответственного за информационную безопасность являются:

- Организация эксплуатации технических и программных средств защиты информации.
- Текущий контроль работы средств и систем защиты информации.

2.2 Ответственный за информационную безопасность выполняет следующие основные функции:

- Разработка и обновление инструкций по информационной безопасности: инструкции по организации антивирусной защиты (приложение 1), инструкций по безопасной работе в Интернете (приложение 2).
- Обучение персонала и пользователей ПК правилам безопасной обработки информации и правилам работы со средствами защиты информации.
- Организация антивирусного контроля носителей информации и файлов электронной почты, поступающих в Колледж.
- Текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации.
- Контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нем.
- Контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК.

3. Права ответственного лица за информационную безопасность

2.1 Требовать от сотрудников и пользователей компьютерной техники безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения и электронных платежей.

2.2 Готовить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов.

4. Обязанности ответственного лица за информационную безопасность

3.1 Обеспечение функционирования и поддержания работоспособности средств и систем защиты информации, в пределах, возложенных на них обязанностей.

3.2 Немедленное информирование директора Колледжа о выявленных нарушениях и несанкционированных действиях пользователей, в том числе о случаях несанкционированного доступа в Интернет, а также принятие необходимых мер по устранению нарушений.

3.3 Принятие мер совместно по восстановлению работоспособности средств и систем защиты информации.

3.4 Проведение инструктажей сотрудников и пользователей ПК по правилам работы используемыми средствами и системами защиты информации.

5. Ответственность за информационную безопасность

4.1 На ответственного за информационную безопасность возлагается персональная ответственность за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определенными настоящим Положением.

Приложение 1

Инструкция по организации антивирусной защиты

1. Общие положения

1.1 Настоящая Инструкция разработана в целях реализации мер по антивирусной защите, которые должны обеспечивать обнаружение в информационных системах (далее – ИС) государственного бюджетного профессионального образовательного учреждения «Волгоградский колледж машиностроения и связи имени Героя Советского Союза Николая Сердюкова» компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.
1.2 Контроль за исполнением настоящей Инструкции осуществляет ответственный за информационную безопасность.

2. Порядок организации антивирусной защиты

2.1 Для антивирусной защиты ИС допускаются к использованию только сертифицированные ФСТЭК России лицензионные антивирусные средства.
2.2 Права по администрированию средств антивирусной защиты предоставлены только ответственному за информационную безопасность
2.3 При загрузке, открытии или исполнении объектов (файлов) из внешних источников средствами антивирусной защиты проводится автоматическая проверка объектов (файлов).
2.4 Расширенный антивирусный контроль проводится ответственным за информационную безопасность ИС при необходимости в случае заражения или подозрения в заражении ИС вирусной программой.

3. Порядок проведения антивирусного контроля

3.1 При установке/обновлении программного обеспечения на ИС установочные пакеты проверяются на наличие вирусов.
3.2 При загрузке компьютера средствами антивирусной защиты проводится антивирусный контроль в автоматическом режиме.
3.3 При подключении внешнего носителя информации средствами антивирусной защиты проводится антивирусный контроль подключенного носителя в автоматическом режиме.
3.4 В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов, пользователю необходимо:
приостановить работу с файлами документов:
дождаться завершения антивирусной проверки;
в случае успешного устранения угрозы (по отчету антивирусной программы) повторно запустить проверку объекта на вирусы;
в случае невозможности автоматического устранения угрозы (по отчету антивирусной программы) немедленно поставить в известность о факте

обнаружения зараженных вирусом файлов ответственного за информационную безопасность, не производить никаких действий на ИС (не останавливать работу антивирусных средств, не отключать внешний носитель, не закрывать информационные сообщения и т.д.).

3.5 При получении сообщения пользователя об обнаружении вируса в случае невозможности лечения зараженных файлов ответственный за информационную безопасность обязан:

запретить использование внешнего носителя (если зараженные файлы находились на подключенном носителе) либо временно запретить использовать ИС;

определить возможный источник заражения;

в случае подозрения на заражение из внешних источников принять меры к нейтрализации возможности повторного заражения из этих источников;

при необходимости проверить сохранность конфиденциальной информации при повреждении обеспечить их восстановление из резервных копий.

4. Ответственность при организации антивирусной защиты

4.1 Ответственность за организацию антивирусной защиты ИС в соответствии с требованиями настоящей Инструкции возлагается на ответственного за информационную безопасность.

4.2 Ответственность за соблюдение требований настоящей Инструкции возлагается на всех сотрудников, эксплуатирующих ИС.

Приложение 2

Инструкция пользователей по безопасной работе в сети Интернет

1. Общие положения

1.1 Целью настоящей инструкции является регулирование работы пользователей, распределения сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации.
1.2 Работа в системе каждому сотруднику разрешена только на определенных компьютерах, в определенное время и только с разрешенными программами и сетевыми ресурсами. Если нужно работать вне указанного времени, на других компьютерах и с другими программами, необходимо получить разрешение директора.
1.3 По уровню ответственности и правам доступа к сети пользователи разделяются на следующие категории: системные администраторы и пользователи.
1.4 Пользователь подключенного к сети компьютера - лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.
1.5 Каждый работник должен пользоваться только своим именем пользователя и паролем для входа в сеть Интернет, передача их кому-либо запрещена.
1.6 Для работы на компьютере другому лицу, кроме пользователя, необходимо разрешение директора или работника, ответственного за Интернет.
1.7 В случае нарушения правил пользования сетью, пользователь сообщает сотруднику, ответственному за Интернет, который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений.
1.8 Работник, следящий за правильным функционированием сети, выдает IP-адрес компьютеру, создает учетную запись электронной почты для пользователя. Самовольное подключение является серьезнейшим нарушением правил пользования сетью.
1.9 Работник, ответственный за Интернет, информирует пользователей обо всех плановых профилактических работах, могущих привести к частичной или полной неработоспособности сети на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам сети.

2. Обязанности пользователей сети Интернет

Пользователи сети Интернет обязаны:
2.1 Соблюдать правила работы в сети, оговоренные настоящей инструкцией.
2.2 При доступе к внешним ресурсам сети, соблюдать правила, установленные системными администраторами для используемых ресурсов.
2.3 Немедленно сообщать работнику, ответственному за использование сети Интернет, об обнаруженных проблемах, а также о фактах нарушения настоящей инструкции кем-либо.