Приложение № 01 к приказу
от 27.09.2021. № 42/КАТ

	Профессиональное образовательное учреждение **«Северодвинский колледж управления и информационных технологий»**

УТВЕРЖДАЮ
Директор ПОУ «Северодвинский колледж управления и информационных технологий»
_____ С.В. Лукьяненко
«27» сентября 2021 г.

Инструкция №1/ИБ
Обеспечение информационной безопасности при использовании в работе персональных компьютеров, имеющих доступ к информационным ресурсам локальной сети и сети «Интернет»

1. Общие положения

1.1. Настоящая инструкция разработана в соответствии Постановления Правительства РФ от 02.08.2019 N 1006 "Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства просвещения Российской Федерации и объектов (территорий), относящихся к сфере деятельности Министерства просвещения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)" и определяет основные права, обязанности и ответственность работников ПОУ «Северодвинский колледж управления и информационных технологий» (далее - Колледж) - пользователей персональных компьютеров (далее - ПК), имеющих доступ к информационным ресурсам локальной сети Колледжа и сети «Интернет».
1.2. Основная цель обеспечения информационной безопасности - предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в компьютерных и телекоммуникационных системах Колледжа.

2. Обязанности работников, имеющих доступ к информационным ресурсам локальной сети и сети «Интернет»

2.1. Работники Колледжа - пользователи ПК, имеющие доступ к информационным ресурсам локальной сети Колледжа и сети «Интернет» обязаны:
— знать и соблюдать требования настоящей Инструкции и других документов

по информационной безопасности при работе с ПК, имеющими доступ к информационным ресурсам локальной сети Колледжа и сети «Интернет»;
— знать и уметь правильно использовать то аппаратно-программное обеспечение, которое установлено на его ПК, а также строго выполнять правила работы со средствами защиты информации, установленными на них;
— хранить в тайне свой пароль (пароли);
— выполнять следующие требования по антивирусному контролю:

а) антивирусный контроль всех дисков и файлов ПК должен проводиться ежедневно в начале работы при их загрузке в автоматическом режиме;

б) к использованию в структурных подразделениях Колледжа допускаются только лицензионные антивирусные средства.

в) обновление антивирусных баз должно проводиться в соответствии с периодичностью, указанной в руководствах по применению конкретных антивирусных средств.

г) в процессе работы обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Разархивирование и контроль входящей информации должен проводиться непосредственно после ее приема. Контроль исходящей информации должен проводиться непосредственно перед архивированием и отправкой (записью на съемный носитель);

д) файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц;

е) устанавливаемое (изменяемое) на ПК программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения на ПК лицом, установившим (изменившим) программное обеспечение, в присутствии пользователя ПК должна быть выполнена антивирусная проверка;

ж) при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник Колледжа должен провести внеочередной антивирусный контроль своего ПК;

з) в случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов работники обязаны:
- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов начальника АХО, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, немедленно приостановить работу и сообщить о данном факте начальнику АХО;

- по факту обнаружения зараженных вирусом файлов составить служебную записку начальнику АХО, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

— присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним ПК;

— немедленно вызывать начальнику АХО при подозрении компрометации личных паролей или их утери, а также при обнаружении:

а) нарушений целостности пломб, наклеек на аппаратных средствах ПК или иных фактов совершения в его отсутствие попыток несанкционированного доступа к ПК;

б) несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ПК;

в) отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ПК, выхода из строя или неустойчивого функционирования узлов ПК или периферийных устройств (дисководов, принтера и т.п.);

г) непредусмотренных формуляром ПК отводов кабелей и подключенных устройств.

— хранить значение своих паролей на бумажном или другом носителе информации только в сейфе у руководителя подразделения.

2.2. Работникам Колледжа категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ПК в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПК или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами ПК;
- осуществлять обработку конфиденциальной информации (персональных данных) в присутствии посторонних (не допущенных к данной информации) лиц;
- осуществлять обработку конфиденциальной информации (персональных данных) при подключенном ПК к сети Интернет;
- записывать и хранить конфиденциальную информацию (персональные данные) на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенными без присмотра свои ПК, не активировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры), если таковые имеются;
- оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие конфиденциальную информацию;
- предпринимать попытки несанкционированного доступа к недоступным информационным ресурсам, осуществлять намеренное изменение, уничтожение, чтение, или передачу информации неавторизованным способом;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут

привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок немедленно ставить в известность начальника АХО.

3. Права работников, имеющих доступ к информационным ресурсам локальной сети и сети «Интернет»

3.1. Работники Колледжа, пользователи ПК имеют право:
- давать начальнику АХО предложения по совершенствованию мер информационной безопасности в подразделении;
- обращаться к начальнику АХО для оказания необходимой технической и методологической помощи в своей работе.

3.2. Начальник АХО имеет право:
- требовать от работников Колледжа - пользователей ПК соблюдения установленных технологий обработки информации и выполнения инструкций и других документов по обеспечению безопасности и защите информации;
- обращаться к руководителю с требованием прекращения работы сотрудников
- пользователей ПК при несоблюдении ими установленных технологий обработки информации или невыполнении требований по обеспечению информационной безопасности;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи информации и технических средств.

4. Ответственность

4.1. Начальник АХО обеспечивает контроль за соблюдением работниками требований настоящей Инструкции.

4.2. Работники Колледжа, пользователи ПК, имеющие доступ к информационным ресурсам локальной сети Колледжа и сети «Интернет», несут персональную ответственность за обеспечение информационной безопасности при их использовании, и соблюдение требований настоящей Инструкции.