Министерство общего и профессионального образования
Свердловской области

государственное автономное профессиональное образовательное учреждение
Свердловской области
«Нижнетагильский строительный колледж»

УТВЕРЖДАЮ
Директор государственного автономного
профессионального образовательного
учреждения Свердловской области
«Нижнетагильский строительный колледж»

_____ О.В. Морозов
«12» 02 2018 г.

ПОЛОЖЕНИЕ

Об информационной безопасности в государственном автономном профессиональном образовательном учреждение Свердловской области «Нижнетагильский строительный колледж (ГАПОУ СО «НТСК»)

г. Нижний Тагил
2018 г.

Термины и определения

Сервер - аппаратно-программный комплекс, исполняющий функции хранения и обработки запросов пользователей и не предназначенный для локального доступа пользователей (выделенный сервер, маршрутизатор и другие специализированные устройства) ввиду высоких требований по обеспечению надежности, степени готовности и мер безопасности информационной системы колледжа.

Рабочая станция - персональный компьютер (терминал), предназначенный для доступа пользователей к ресурсам Автоматизированной системы колледжа, приема передачи и обработки информации.

Автоматизированная система (АС) - совокупность программных и аппаратных средств, предназначенных для хранения, передачи и обработки данных и информации и производства вычислений.

Системный администратор - должностное лицо, в обязанности которого входит обслуживание всего аппаратно-программного комплекса колледжа, управление доступом к сетевым ресурсам, а также поддержание требуемого уровня отказоустойчивости и безопасности данных, их резервное копирование и восстановление

Пользователь - сотрудник колледжа, использующий ресурсы информационной системы колледжа для выполнения должностных обязанностей.

Учетная запись - информация о сетевом пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (Адрес электронной почты, телефон и т.п.)

Пароль - секретная строка символов (букв, цифр, специальных символов), предъявляемая пользователем компьютерной системе для получения доступа к данным и программам. Пароль является средством защиты данных от несанкционированного доступа.

Изменение полномочий - процесс создания удаления, внесения изменений в учетные записи пользователей АС, создание, удаление изменение наименований почтовых ящиков и адресов электронной почты, создание, удаление изменение групп безопасности и групп почтовой рассылки, а также другие изменения, приводящие к расширению (сокращению) объема информации либо ресурсов доступных пользователю АС.

1. Назначение и область применения

1.1. Положение об информационной безопасности Государственного автономного профессионального образовательного учреждения Свердловской области «Нижнетагильский строительный колледж» (далее – Положение, колледж) регламентирует порядок организации и правила обеспечения информационной безопасности в колледже, распределение функций и ответственности за обеспечение информационной безопасности между подразделениями и сотрудниками колледжа, требования по информационной безопасности к информационным средствам, применяемым в колледже.

1.2. Положение является локальным нормативным актом колледжа. Требования настоящего Положения обязательны для всех структурных подразделений колледжа и распространяются на:

– автоматизированные системы колледжа;

– средства телекоммуникаций;

– помещения;

– сотрудников колледжа.

1.3. Положение утверждается приказом директора колледжа в установленном порядке.

2. Общие положения

2.1. Информационная безопасность является одним из составных элементов комплексной безопасности колледжа. Под информационной безопасностью колледжа понимается состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности

2.2. Информационная безопасность - деятельность, направленная на обеспечение защищенного состояния объекта информации, в том числе объектов автоматизированных и телекоммуникационных систем, противодействия техническим разведкам, включающая комплексные, криптографические, компьютерные, организационные, технические средства защиты.

2.3. Обеспечение информационной безопасности осуществляется по следующим направлениям:

– правовая защита – процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;

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

– инженерно-техническая защита – это использование различных техни-

ческих средств, препятствующих нанесению ущерба.

Информационная безопасность включает:

– защиту интеллектуальной собственности колледжа;

– защиту компьютеров, локальных сетей и сети подключения к системе Интернета;

– организацию защиты конфиденциальной информации, в т. ч. персональных данных работников и обучающихся;

– учет всех носителей конфиденциальной информации.

2.4. Информационная безопасность колледжа должна 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).

2.5. К объектам информационной безопасности колледжа относятся:

– информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;

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

– средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

2.6. Правовую основу Положения составляют:

– Конституция Российской Федерации;

– Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ;

– Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ;

– Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ;

– Федеральный закон «Об информации, информационных технологиях и о защите информации» от 26.07.2006 № 149-ФЗ;

– Федеральный закон «О персональных данных» от 27.07.06 № 152-ФЗ (в ред. от 27.07.2011)

– ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью" (утв. Приказом Ростехрегулирования от 29.12.2005 N 447-ст)

– другие законодательные акты, руководящие и нормативно-

методические документы Российской Федерации в области обеспечения информационной безопасности.

3. Цели и задачи обеспечения безопасности информации

3.1. Главная цель обеспечения безопасности информации, циркулирующей в колледже, является реализация положений законодательных актов Российской Федерации и нормативных требований по защите информации ограниченного доступа (далее по тексту - конфиденциальной или защищаемой информации) и предотвращение ущерба в результате разглашения, утраты, утечки, искажения и уничтожения информации, ее незаконного использования и нарушения работы информационно телекоммуникационной системы колледжа.

3.2. Основными целями обеспечения безопасности информации являются:

– предотвращение утечки, хищения, искажения, подделки информации, циркулирующей в колледже;

– предотвращение нарушений прав личности обучающихся, работников колледжа на сохранение конфиденциальности информации;

– предотвращение несанкционированных действий по блокированию информации;

3.3. Основными задачами обеспечения безопасности информации являются:

– соответствие положениям законодательных актов и нормативным требованиям по защите информации;

– своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба интересам колледжа, нарушению нормального функционирования и развития колледжа;

– создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции в системе информационных отношений;

– эффективное пресечение незаконных посягательств на информационные ресурсы, технические средства и информационные технологии, в том числе с использованием организационно-правовых и технических мер и средств защиты информации;

– координация деятельности структурных подразделений колледжа по обеспечению защиты информации;

– развитие системы защиты, совершенствование ее организации, форм, методов и средств предотвращения, парирования и нейтрализации угроз ин-

формационной безопасности и ликвидации последствий ее нарушения;

– развитие и совершенствование защищенного юридически значимого электронного документооборота.

– создание механизмов, обеспечивающих контроль системы информационной безопасности и гарантии достоверности выполнения установленных требований информационной безопасности

– создание механизмов управления системой информационной безопасности (СИБ).

4. Организация системы обеспечения информационной безопасности

4.1. Система обеспечения информационной безопасности распространяются на:

– автоматизированные системы колледжа.

– средства телекоммуникаций;

– помещения;

– сотрудников колледжа.

4.2. В целях реализации стоящих перед системой обеспечения информационной безопасности задач в колледже устанавливаются:

–защита персональных данных персонала и обучающихся;

– контроль за использованием электронных средств информационного обеспечения деятельности колледжа по прямому назначению;

– противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности колледжа нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами;

– внутрисетевой контроль за перемещением информации;

– принятие мер к воспрещению доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими;

– проверка целесообразности использования персоналом и обучающимися колледжа интернет - ресурса, предоставляемого им администрацией, анализ допускаемых нарушений и принятие мер к недопущению его нецелевого использования средствами технического противодействия;

– обучение персонала колледжа по вопросам обеспечения информационной безопасности;

– контроль за правильностью использования имеющихся в колледже средств телефонной и радиосвязи;

– защита персональных данных персонала и обучающихся - мероприятия по недопущению несанкционированного доступа к персональным данным персонала и обучающихся колледжа при их обработке с использованием средств автоматизации или без использования таких средств;

– контроль за использованием электронных средств информационного обеспечения деятельности колледжа по прямому назначению - плановые и внеплановые проверки в структурных подразделениях колледжа. Содержание проверок - сложившаяся практика использования персональных компьютеров, мультимедийных систем, интерактивных средств обучения, телевизионных приемников, копировально-множительной аппаратуры и сканирующих устройств, электронных средств проектирования и инженерной графики, телефонных аппаратов и радиостанций, а также программного обеспечения к указанным средствам и устранение выявленных в ходе проверок недостатков;

– противодействие фактам использования при работе на электронных средствах информационного обеспечения деятельности колледжа нелицензированных программных продуктов и электронных носителей информации способных произвести заражение программного обеспечения вирусами - контроль за используемым программным обеспечением и проверка его подлинности, ограничение в использовании съемных и компакт-дисков сотрудниками и обучающимися колледжа;

– принятие мер к воспрещению доступа к информационным материалам, признанным в соответствии с действующим законодательством экстремистскими постоянное ознакомление со сведениями об информационных материалах признанных в соответствии с действующим законодательством экстремистскими, доведение этих сведений до администрации и персонала колледжа и принятие мер к воспрещению доступа к этим материалам (мерами технического противодействия - в отношении материалов находящихся в сети Интернет, и путем изъятия – в отношении печатных изданий, хранящихся в библиотеке колледжа);

– проверка целесообразности использования персоналом и обучающимися колледжа интернет - ресурса, предоставляемого им администрацией, анализ допускаемых нарушений и принятие мер к недопущению его нецелевого использования средствами технического противодействия - установление и доведение в форме инструкций до персонала и обучающихся колледжа общедоступных требований об ограничениях при использовании- ресурса,

предоставляемого им администрацией колледжа, постоянный контроль за выполнением указанных ограничений, разработка, внедрение, и применение технических (программных) средств противодействия возникающим наруше-

ниям, либо злоупотреблениям;

– обучение персонала колледжа по вопросам обеспечения информационной безопасности - проведение занятий с персоналом в целях формирования у них соответствующих знаний, умений и навыков позволяющих соблюдать требования по обеспечению ин формационной безопасности колледжа.

– контроль за правильностью использования имеющихся в колледже средств телефонной и радиосвязи - выявление фактов нецелевого использования средств телефонной и радиосвязи и принятие мер технического и организационного характера по их недопущению.

4.3. Общее руководство системой информационной безопасности колледжа осуществляет заместитель директора по учебно-производственной работе. Руководители структурных подразделений колледжа обязаны участвовать в ее поддержании в надлежащем состоянии, дальнейшем развитии и совершенствовании по своим направлениям деятельности.

5. Порядок обеспечения информационной безопасности

5.1. Организационное и техническое обеспечение рабочего процесса сотрудников возлагается на сотрудников учебно-компьютерного центра.

5.2. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику учреждения, допущенному к работе с конкретной подсистемой АС, должно быть сопоставлено персональное уникальное имя - учетная запись пользователя и пароль, под которым он будет регистрироваться, и работать в системе. Использование несколькими сотрудниками при работе в АС одного и того же имени пользователя запрещено.

5.3. Основанием для изменения полномочий (предоставления, изменения либо прекращения действий прав доступа пользователя АС) является Письменная заявка сотрудника, для которого требуется изменить полномочия доступа к системе на имя руководителя учебно-компьютерного центра.

5.4. Проведение операций, указанных п. 4.2. сотрудниками, не уполномоченными на проведение подобных действий, запрещено и идентифицируется как факт несанкционированного доступа.

5.5. Правила использования сети Интернет (в том числе доступа обучающихся к Интернету) приведены в Приложении 1.

6. Порядок создания, изменения и удаления учетных записей, групп безопасности и почтовой рассылки

6.1. Оформленная заявка «На внесение изменений в списки пользователей» поступает руководителю учебно-компьютерного центра. Руководитель учебно-компьютерного центра в соответствии предоставленной в заявке информации дает задание системному администратору на внесение необходимых изменений. Проведение изменений системным администратором без наличия задания от руководителя учебно-компьютерного центра либо лица, его замещающего, запрещено.

6.2. Заявки с отметками об исполнении и подписью заявителя остается на хранении у руководителя учебно-компьютерного центра не менее 1 года.

7. Изменение полномочий учетных записей и состава групп безопасности и почтовой рассылки

7.1. После получения задания от руководителя учебно-компьютерного центра, системный администратор вносит соответствующие изменения в базу данных учетных записей и ставит отметку об исполнении задания на бланке заявки.

7.2. Все изменения в списках доступа должны быть выполнены системным администратором не позднее одного часа с момента получения задания на внесение изменений от руководителя учебно-компьютерного центра. Бланк заявки с отметкой об исполнении возвращается руководителю учебно-компьютерного центра.

7.3. По окончании процедур изменения списков доступа системный администратор вносит соответствующую запись в «Журнал изменения списков доступа».

8. Создание новых учетных записей пользователей групп безопасности и почтовой рассылки

8.1. Получив задание от руководителя учебно-компьютерного центра, системный администратор создает необходимые объекты безопасности, присваивает первичный пароль вновь созданной учетной записи, при необходимости создает почтовый ящик пользователя.

8.2. При задании первичного пароля учетной записи пользователя администратор обязан установить отметку «Потребовать смену пароля при первом

входе в систему» Допускается в качестве первичного пароля использовать простые или повторяющиеся комбинации.

8.3. После выполнения задания системный администратор ставит отметку об исполнении задания и передает бланк заявки, а также дополнительную информацию, необходимую для использования вновь созданного объекта безопасности (первичный пароль, «имя» учетной записи адрес электронной почты и т.п.) руководителю учебно-компьютерного центра.

8.4. Заявка «На внесение изменений в списки доступа» должна быть обработана и исполнена системным администратором не позднее одного часа с момента получения задачи от руководителя учебно-компьютерного центра.

8.5. По окончании процедур создания нового объекта в списках доступа системный администратор вносит соответствующую запись в «Журнал учета изменения списков доступа».

9. Удаление учетных записей пользователей групп безопасности и почтовой рассылки

9.1. Получив задание от руководителя учебно-компьютерного центра, системный администратор удаляет необходимые объекты безопасности из всех указанных в задании списков доступа.

9.2. После выполнения задания системный администратор ставит отметку об исполнении задания и передает бланк заявки, с отметкой об исполнении, руководителю учебно-компьютерного центра.

9.3. Бланк заявки с отметкой об исполнении возвращается руководителю учебно-компьютерного центра.

9.4. Задача «на внесение изменений в списки доступа», предполагающая удаление сокращение полномочий должна быть обработана и исполнена системным администратором не позднее 30 минут с момента получения задачи от руководителя учебно-компьютерного центра.

9.5. По окончании процедур удаления объекта в списках доступа системный администратор и администратор баз данных вносят соответствующую запись в «Журнал учета изменения списков доступа»

10. Служебные учетные записи и группы

10.1. Служебные учетные записи - объекты безопасности, содержащие реквизиты, необходимые для нормального функционирования некоторых служб и сервисов (например: задачи резервного копирования и восстановления,

служба автоматического обновления ОС и т.п.). Служебные учетные записи не предназначены для локального входа в систему, работа сотрудников учебно-компьютерного центра с использованием реквизитов служебных учетных записей запрещена.

10.2. Служебные группы безопасности и почтовой рассылки - объекты безопасности, необходимые для управления доступом к Служебному ПО и рассылки уведомлений, предназначенных техническому персоналу учебно-компьютерного центра.

10.3. Создание удаление и изменение служебных объектов безопасности производятся системным администратором либо администратором баз данных только по письменной (электронной) заявке руководителя учебно-компьютерного центра. Самостоятельное создание, изменение либо удаление служебных учетных записей системным администратором (администратором баз данных) запрещено.

10.4. Категорически запрещается использование встроенной учетной записей Administrator (SA для SQL сервера и т.п.) - для повседневной работы, для запуска служб и сервисов либо для доступа к сетевым ресурсам. Использование встроенных учетных записей допускается только в случаях, требующих реквизитов именно этой учетной записи (восстановление AD, восстановление поврежденных данных системы, в некоторых случаях проведение обновлений системы и т.п.).

10.5. Решение о необходимости применении реквизитов служебных учетных записей принимает системный администратор (администратор БД).

11. Локальные учетные записи

11.1 Локальные учетные записи компьютеров (Administrator, Guest) предназначены для служебного использования сотрудниками учебно-компьютерного центра при настройке системы и не предназначены для повседневной работы.

11.2. Создание и использование локальных учетных записей на рабочих станциях, подключенных к ВС колледжа запрещено.

11.3. Встроенная учетная запись Guest (Гость) должна быть заблокирована на всех рабочих станциях в составе ВС колледжа при первоначальном конфигурировании операционной системы.

12. Специальные учетные записи

12.1. К специальным учетным записям относятся - реквизиты доступа к активному

сетевому оборудованию, учетные записи для доступа к базам данным, а также все учетные записи, реквизиты которых не хранятся в едином каталоге AD.

12.2. Создание специальных учетных записей производится системным администратором при возникновении необходимости.

13. Требования к паролям

13.1. Первичный пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые системным администратором при создании новой учетной записи.

13.1.1. Установку первичного пароля производит системный администратор при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на системном администраторе.

13.1.2. Первичный пароль может содержать несложную комбинацию символов, либо повторяющиеся символы.

13.1.3. При создании первичного пароля, системный администратор обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

13.1.4. Первичный пароль также используется при сбросе забытого пароля на учетную запись. В любом случае, при использовании первичного пароля все требования настоящего документа сохраняются.

13.2. Основной пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику колледжа, используемая для подтверждения подлинности владельца учетной записи.

13.2.1. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

13.2.2. При выборе пароля необходимо руководствоваться следующими правилами:

– длина пароля должна составлять не менее 8 символов;

– при выборе пароля, рекомендуется использовать комбинацию из строчных и прописных букв, цифр, знаков препинания и специальных символов;

– запрещается использовать в качестве пароля название учетной записи,

фамилию пли имя пользователя, а также легко угадываемые сочетания символов.

13.2.3. Пользователь несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам, в том числе сотрудникам учебно-компьютерного центра, записывать его, а также пересылать открытым текстом в электронных сообщениях.

13.2.4. Пользователь обязан не реже одного раза в три месяца производить смену основного пароля, соблюдая требования настоящего Положения.

13.2.5. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом в учебно-компьютерный центр и изменить основной пароль.

13.2.6. Восстановление забытого основного пароля пользователя осуществляется системным администратором путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменной заявки пользователя.

13.2.7. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

13.2.8. Для предотвращения угадывания паролей системный администратор обязан настроить механизм блокировки учетной записи при трехкратном неправильном вводе пароля.

13.2.9. Разблокирование учетной записи пользователя осуществляется системным администратором на основании заявки владельца учетной записи.

13.3. Административный пароль – комбинация символов (буквы, цифры БД, администратору приложения), используемая при настройке служебных учетных записей, учетных записей служб и сервисов а также специальных учетных записей.

14. Доступ к ресурсам Интернет

14.1. Для исполнения задач, связанных с производственной деятельностью сотрудникам колледжа предоставляется доступ к ресурсам Интернет. Доступ к ресурсам Интернет в других целях запрещен.

14.2. Требуемый уровень доступа предоставляется сотруднику колледжа на основании заявки «на изменение списков доступа» на имя руководителя учебно-компьютерного центра.

14.3. Системный администратор учебно-компьютерного центра обязан предоставлять руководителю колледжа лимит использования Интернет на предстоящий месяц.

14.4. Системный администратор учебно-компьютерного центра обязан не

реже одного раза в месяц представлять отчет об использовании Интернет ресурсов сотрудниками колледжа руководителю учебно-компьютерного центра.

14.5. Доступ к ресурсам Интернет может быть блокирован системным администратором без предварительного уведомления при возникновении нештатных ситуаций либо в иных случаях, предусмотренных организационными документами.

14.6. Сотрудникам колледжа может быть предоставлен дополнительный объем трафика Интернет согласно заявлению на имя руководителя колледжа.

14.7. Сотрудникам колледжа может быть предоставлен платный доступ к сети Интернет согласно заявлению на имя руководителя учебно-компьютерного центра с вычетом оплаты из заработной платы по тарифам, установленным в колледже.

14.8. Правила использования сети Интернет (в том числе доступа обучающихся к Интернету) приведены в Приложении 1.

15. Электронная почта

15.1. Для исполнения задач, связанных с производственной деятельностью сотрудникам колледжа может быть предоставлен доступ к системе электронной почты. Использование системы электронной почты колледжа в других целях запрещено.

15.2. Доступ к системе электронной почты предоставляется сотруднику колледжа на основании заявки «на изменение списков доступа» на имя руководителя учебно-компьютерного центра.

15.3. Электронная почта является собственностью колледжа и может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

15.4. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководства.

15.5. В случае обнаружения значительных отклонений в параметрах работы средств обеспечения работы системы электронной почты, системный администратор обязан немедленно сообщить об этом руководителю учебно-компьютерного центра для принятия решений.

15.6. Доступ к серверу электронной почты может быть блокирован системным администратором без предварительного уведомления при возникновении нештатных ситуаций, либо в иных случаях предусмотренных организационными документами.

15.7. Правила работы с электронной почтой приведены в Приложении 2.

16. Антивирусная защита

16.1. К использованию в колледже допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

16.2. Установка средств антивирусного контроля на компьютерах (серверах ЛВС) колледжа осуществляется уполномоченными сотрудниками.

16.3. Настройка параметров средств антивирусного контроля осуществляется сотрудниками учебно-компьютерного центра в соответствии с руководствами по применению конкретных антивирусных средств. Изменение настроек другими сотрудниками запрещено.

16.4. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС – при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов РС.

16.5. 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 (магнитных дисках, лентах, CD-ROM и т.п.).

16.6. Антивирусная проверка должна проводиться:

– на компьютерах сотрудников - не реже одного раза в неделю;

– на серверах ЛВС - не реже двух раз в неделю.

16.7. 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.) сотрудник подразделения самостоятельно или вместе с сотрудником учебно-компьютерного центра должен провести внеочередной антивирусный контроль своей рабочей станции.

17. Хранение данных

17.1. Служебная информация сотрудников колледжа должна храниться в специально отведенных папках на серверах ЛВС колледжа. Хранение служебной информации на компьютерах сотрудников запрещено.

17.2. Для хранения личной информации сотрудников возможно выделение сетевых папок согласно заявке «На внесение изменений в списки пользователей». Хранение личной информации в служебных папках запрещено.

17.3. Для обеспечения целостности данных необходимо проводить ре-

зервное копирование не реже одного раза в сутки сотрудниками учебно-компьютерного центра. Резервное копирование личной информации сотрудниками руководителя учебно-компьютерного центра не предусмотрено.

17.4. Ответственность:

17.4.1. Ответственность за обеспечение целостности данных, хранимых на серверах колледжа в соответствии с требованиями настоящего положения возлагается на руководителя учебно-компьютерного центра.

17.4.2. Ответственность за обеспечение целостности данных, хранимых на локальных компьютерах сотрудников колледжа в соответствии с требованиями настоящего Положения возлагается на самих сотрудников.

18. Установка и обслуживание оборудования

18.1. Установка и обслуживание оборудования возможна только сотрудниками учебно-компьютерного центра. Установка и обслуживание оборудования сотрудниками других отделов запрещена.

18.2. Для определения несанкционированной замены оборудования вся техника колледжа должна быть опечатана в местах возможного вскрытия.

18.3. Ответственность за сбои в работе оборудования лежит на сотрудниках учебно-компьютерного центра.

19. Установка и обслуживание программ

19.1. Установка программ возможна только сотрудниками учебно-компьютерного центра. Установка программ сотрудниками других отделов запрещена.

19.2. Ответственность за сбои в работе программ лежит на сотрудниках отдела АСУ.

Приложение 1

Правила использования сети Интернет
(в том числе доступа обучающихся к Интернету) в ГАПОУ СО «НТСК»

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящие Правила регулируют условия и порядок использования сети Интернет в ГАПОУ СО «Нижнетагильский строительный колледж» (далее – Колледж) обучающимися и работниками Колледжа.

1.2 Правила имеют статус локального нормативного акта Колледжа.

Если нормами действующего законодательства РФ предусмотрены иные требования, чем настоящими Правилами, применяются нормы действующего законодательства РФ.

1.3 Использование сети Интернет в Колледже подчинено следующим принципам:

– соответствие образовательным целям;

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

– расширение применяемого спектра учебных и наглядных пособий;

– приобретение новых навыков и знаний;

– способствование гармоничному формированию и развитию личности;

– социализация личности, введение в информационное общество.

2 ПОЛИТИКА ИСПОЛЬЗОВАНИЯ (ДОСТУПА) СЕТИ ИНТЕРНЕТ В КОЛЛЕДЖЕ

2.1 Использование сети Интернет в Колледже возможно исключительно при условии ознакомления и согласия лица, пользующегося сетью Интернет в Колледже, с настоящими Правилами.

2.2 Ознакомление лиц, использующих сеть Интернет в Колледже с настоящими Правилами осуществляется:

– через размещение настоящих Правил на официальном сайте Колледжа по адресу http://www.ntst-edu.ru/tender/ , в разделах сайта «Сведения об образовательной организации» (подраздел «Документы»)

– в виде устного информирования обучающихся и родителей преподавателями и классных руководителей учебных групп на общих собраниях.

2.3 Руководитель Колледжа является ответственным за обеспечение эффективного и безопасного доступа к сети Интернет, а также за внедрение соответствующих технических, правовых и иных механизмов, обеспечивающих безопасный доступ к сети Интернет в Колледже.

2.4 Непосредственное определение политики доступа в Интернет осуществляет учебно-компьютерный центр Колледжа.

2.5 Учебно-компьютерный центр:

— принимает решение о разрешении / блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет, содержащим информацию, не совместимую с задачами образовательного процесса, с учетом социокультурных особенностей региона;

— определяет характер и объем информации, публикуемой на Интернет-ресурсах Колледжа;

— дает руководителю Колледжа рекомендации о назначении и освобождении от исполнения своих функций лиц, ответственных за непосредственный контроль безопасности работы в сети Интернет и соответствия ее целям и задачам образовательного процесса.

2.6 Контроль за использованием обучающимися сети Интернет в учебное и свободное от занятий время в соответствии с Правилами осуществляют ответственные лица.

2.6.1 Во время учебных занятий с использованием сети Интернет в учебных кабинетах и библиотеке ответственным лицом является преподаватель, ведущий занятие.

2.6.2 Во время свободной работы обучающихся в сети Интернет в библиотеке ответственными лицами являются:

— заведующий библиотекой;

—библиотекарь.

2.6.3 Ответственное лицо:

— определяет время и место для работы в сети Интернет обучающихся, педагогических и других работников Колледжа с учетом использования соответствующих технических мощностей Колледжа в образовательном процессе, а также длительность сеанса работы одного человека;

— наблюдает за использованием персонального компьютера и сети Интернет обучающимися;

— запрещает дальнейшую работу обучающегося в сети Интернет в случае нарушения настоящих Правил и иных нормативных документов, регламентирующих использование сети Интернет в Колледже;

— принимает предусмотренные Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу / группе ресурсов, не совместимых с задачами образования;

— не допускает обучающихся к работе в сети Интернет в предусмотренных Правилами случаях;

– принимает предусмотренные Правилами и иными нормативными документами меры для пресечения дальнейших попыток доступа к ресурсу / группе ресурсов, не совместимых с задачами образования.

2.7 При использовании сети Интернет в Колледже осуществляется доступ только к ресурсам, содержание которых не противоречит законодательству РФ и не является несовместимым с целями и задачами образования и воспитания.

Проверка такого соответствия осуществляется с помощью специальных технических средств и программного обеспечения контекстного ограничения доступа, установленного в Колледже или предоставленного оператором услуг связи.

Использование сети Интернет в Колледже без применения данных технических средств и программного обеспечения (например, в случае технического отказа) допускается только с индивидуального разрешения руководителя Колледжа в письменном виде.

Пользователи сети Интернет в Колледже понимают, что технические средства и программное обеспечение не могут осуществлять полную фильтрацию ресурсов сети Интернет в связи с высокой частотой обновления ресурсов и осознают возможную опасность столкновения с ресурсом, содержание которого противоречит законодательству РФ и является несовместимым с целями и задачами образовательного процесса.

2.8 Решение о политике доступа к ресурсам / группам ресурсов сети Интернет принимает руководитель учебно-компьютерного центра самостоятельно либо с участием внешних экспертов, в качестве которых могут привлекаться:

– педагогические работники Колледжа, и других учебных заведений;

– лица, имеющие специальные знания и профессиональные навыки либо опыт работы в рассматриваемой области;

– представители органов управления образованием;

– родители обучающихся.

При принятии решения руководитель учебно-компьютерного центра, эксперты руководствуются:

– действующим законодательством РФ;

– специальными познаниями, в т. ч. полученными в результате профессиональной деятельности;

– опытом организации образовательного процесса с использованием информационных технологий и возможностей сети Интернет;

– целями образовательного процесса;

– интересами обучающихся;

– рекомендациями профильных органов и организаций в сфере классифи-

кации ресурсов сети Интернет.

2.9 Отнесение определенных категорий и / или ресурсов в соответствующие группы, доступ к которым регулируется техническим средствами и программным обеспечением контекстного технического ограничения доступа к информации, технически осуществляется лицом, уполномоченным руководителем Колледжа по представлению отдела информационного обеспечения.

2.10 Категории ресурсов, в соответствии с которыми определяется политика использования сети Интернет в Колледжа, и доступ к которым регулируется техническими средствами и программным обеспечением контекстного технического ограничения доступа к информации, определяются в установленном порядке.

2.11 Принципами размещения информации на Интернет-ресурсах Колледжа являются:

– соблюдение действующего законодательства РФ, интересов и прав граждан;

– защита персональных данных обучающихся, поступающих, педагогических работников и других сотрудников;

– достоверность и корректность информации.

2.12 Порядок размещения персональных данных обучающихся, поступающих и работников Колледжа регулируется нормативным актом – Положением о защите персональных данных работников ГАПОУ МО «Мурманский технологический колледж сервиса», утвержденным руководителем образовательной организации.

3 ПОРЯДОК ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ В КОЛЛЕДЖЕ

3.1 Использование сети Интернет в Колледже осуществляется в целях образовательного процесса.

В рамках развития личности, ее социализации и получения знаний в области сети Интернет и компьютерной грамотности лицо может осуществлять доступ к ресурсам не образовательной направленности, не нарушающим нормы действующего законодательства.

3.2 По разрешению ответственного лица обучающиеся (с согласия родителей, законных представителей), педагогические работники и другие сотрудники вправе:

– размещать собственную информацию в сети Интернет на Интернет-ресурсах Колледжа;

– иметь учетную запись электронной почты на Интернет-ресурсах Колледжа.

3.3 Во время работы в сети Интернет с использованием технических

средств, принадлежащих Колледжу обучающимся и работникам Колледжа запрещается:

– находиться на ресурсах, содержание и тематика которых является недопустимой для несовершеннолетних и / или нарушающей законодательство РФ (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т. п. розни, иные ресурсы схожей направленности);

– использовать компьютеры и технические средства Колледжа для осуществления любых сделок через Интернет;

– распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы;

– осуществлять загрузку файлов на компьютеры Колледжа без разрешения ответственного лица.

3.4 Ответственное лицо проверяет, отстранен ли обучающийся от самостоятельной работы в сети Интернет.

3.5 При случайном обнаружении обучающимся или работником Колледжа, работающим в сети Интернет, ресурса, содержимое которого не совместимо с целями образовательного процесса, он обязан незамедлительно сообщить о нем ответственному лицу с указанием интернет-адреса (URL) и покинуть данный ресурс.

3.6 Ответственное лицо обязано:

– принять сообщение лица, работающего в сети Интернет;

– довести информацию до сведения руководителя учебно-компьютерного центра для оценки ресурса и принятия решения по политике доступа к нему;

– направить информацию о некатегоризированном ресурсе системному администратору средств и программного обеспечения технического ограничения доступа к информации (в течение суток);

– 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:

– 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 Колледже технических средствах и средствах технического ограничения доступа к информации.

Приложение 2

Правила работы с электронной почтой

1.Электронная почта является собственностью колледжа и может быть использована только в служебных целях. Использование электронной почты в других целях категорически запрещено.

2.Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию непосредственного либо вышестоящего руководителя.

3.При работе с корпоративной системой электронной почты сотрудникам колледжа запрещается:

3.1. использовать адрес корпоративной почты для оформления подписок и массовых рассылок;

3.2. публиковать свой адрес, либо адреса других сотрудников колледжа на общедоступных Интернет ресурсах (форумы, конференции и т.п.);

3.3. отправлять сообщения с вложенными файлами общий объем которых превышает 5 Мегабайт;

3.4. открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;

3.5. осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без их на то согласия. Данные действия квалифицируются как СПАМ и являются незаконными;

3.6. осуществлять массовую рассылку почтовых сообщений рекламного характера;

3.7. рассылка через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;

3.8. распространение защищаемых авторскими правами материалов, затрагивающих какой- либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права

третьей сторон;

3.9. распространять информацию содержание и направленность которой запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д. распространять информацию ограниченного доступа, представляющую коммерческую тайну;

3.10. предоставлять кому бы то ни было пароль для доступа к своему почтовому адресу.

СОГЛАСОВАНО
профсоюзный комитет
ГАПОУ СО «Нижнетагильский строительный колледж»
Председатель профкома
_____Н.В. Пермякова
«12» 02 2018 г.

СОГЛАСОВАНО

Руководитель учебно-компьютерного центра
_____О.В.Долгополов
«12» 02 2018 г.

Заместитель директора по учебной работе
_____О.И.Трубина
«12» 02 2018 г.

Заместитель директора по Учебно-производственной работе
_____А.В. Алленов
«12» 02 2018 г.

Юрисконсульт
_____Н.Л. Чернышева
«12» 02 2018 г.

РАЗРАБОТЧИК
Специалист по защите информации
_____А.Ю.Метелев
«12» февраля 2018 г

Протокол заседания совета колледжа
№ _27_ от _12.02.2018г.