Приложение
к приказу ГАПОУ МО «КИК»
от 20.02.2024 № 51

МИНИСТЕРСТВО ОБРАЗОВАНИЯ МУРМАНСКОЙ ОБЛАСТИ

Государственное автономное профессиональное образовательное учреждение Мурманской области «Кандалакшский индустриальный колледж» (ГАПОУ МО «КИК»)

ПОЛОЖЕНИЕ

об информационной безопасности государственном автономном профессиональном образовательном учреждении Мурманской области «Кандалакшский индустриальный колледж»

г. Кандалакша
2024 г.

Термины и определения

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

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.

Локальная сеть (ЛС) - комплекс сетевого оборудования, персональных компьютеров, серверов и программного обеспечения, обеспечивающий передачу, хранение и обработку информации с целью осуществление доступа к хранящимся данным, программам, сети Интернет, почтовому сервису и прочим ресурсам.

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.

Пользователь - сотрудник или обучающийся колледжа, использующий ресурсы автоматизированных систем и локальной сети колледжа, обладающий правом доступа в глобальную сеть Интернет .

Рабочая станция - персональный компьютер (терминал), предназначенный для доступа пользователей к ресурсам локальной сети, автоматизированных систем колледжа, приема передачи и обработки информации.

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.

Сервер хранения данных (СХД) - аппаратно-программный комплекс, исполняющий функции обработки данных, хранения данных и служебных документов пользователей, не предназначенный для локального доступа пользователей в целях обеспечения надежности сохранности данных, повышения отказоустойчивости и безопасности локальной сети и автоматизированных систем колледжа.

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.).

1. Назначение и область применения

1.1 Положение об информационной безопасности Государственного автономного профессионального образовательного учреждения Мурманской области «Кандалакшский индустриальный 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 сотрудников всех структурных подразделений колледжа и распространяются на:

- рабочие станции и автоматизированные системы колледжа;
- программные и аппаратные ресурсы;
- средства телекоммуникаций;
- помещения.

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 технических средств, препятствующих нанесению ущерба.

2.4. Информационная безопасность включает:

- защиту и сохранность 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;

- ограничение доступа в помещения, где расположены рабочие станции использующие автоматизированные системы обработки данных.

2.5. Информационная безопасность колледжа должна обеспечивать:

- конфиденциальность (защиту информации от несанкционированного раскрытия или перехвата) доступ к информации только авторизованных пользователей;

- целостность (достоверность и полноту информации, методов её обработки с использованием компьютерных программ);

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

2.6. 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.

2.7. Правовую основу Положения составляют:

- 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;

- федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 № 436-ФЗ;

- федеральный закон «О противодействии экстремистской деятельности» от 25.07.2002 № 114-ФЗ;

- постановление Правительства Российской Федерации «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)» от 02.08.2019 № 1006;

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

и 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, обрабатываемой в колледже;
- предотвращение нарушений прав личности обучающихся, сотрудников колледжа на сохранение конфиденциальности информации;
- предотвращение несанкционированных действий по незаконному использованию или блокированию информации;

3.2. 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 информационной 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 распро-страняются на:

- рабочие станции и автоматизированные системы колледжа;
- средства телекоммуникаций;
- помещения;
- сотрудников и обучающихся колледжа.

4.2. В целях реализации стоящих перед системой обеспечения информа-ционной безопасности задач в колледже устанавливаются:

- 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-ресурсов с помощью доступа в сеть Интернет, предоставляемого им администрацией, анализ допускаемых нарушений и принятие мер к недопущению его нецелевого использования средствами технического противодействия;
- контроль за правильностью использования имеющихся в колледже рабочих станций и электронных средств информационного обеспечения деятельности колледжа по прямому назначению;
- 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;
- плановые и внеплановые проверки в помещений колледжа в отношении сложившейся практики использования рабочих станций, мультимедийных систем, интерактивных средств обучения, телевизоров и проекторов, копировально-множительной аппаратуры и сканирующих устройств, телефонных аппаратов, а также программного обеспечения к указанным средствам и устранение выявленных в ходе проверок недостатков.
- контроль за используемым программным обеспечением и проверка его подлинности, ограничение в использовании съемных и компакт-дисков сотрудниками и обучающимися колледжа;
- 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);

- 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 нарушениям, 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 информационной безопасности колледжа.

4.3. Общее руководство системой информационной безопасности колледжа осуществляет заместитель директора по административно-хозяйственной деятельности (далее – зам.директора по АХР). 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 системного администратора.

5.2. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику учреждения, допущенному к работе с конкретной информационной системой (сайтом), 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 одного и того же имени пользователя запрещено.

5.3. Основанием для изменения полномочий, предоставления, изменения либо прекращения действий прав доступа пользователя к автоматизированной системе (далее - АС), является письменная заявка сотрудника, для которого требуется изменить полномочия доступа к системе на имя зам.директора по АХР.

5.4. Проведение операций, указанных п. 5.3 сотрудниками, не уполномоченными на проведение подобных действий, запрещено и идентифицируется как факт несанкционированного доступа.

5.5. Правила работы сотрудников колледжа и обучающихся в компьютерных сетях приведены в Приложении 1.

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

6.1. Служебная записка «На внесение изменений в списки

пользователей» поступает зам.директора по АХР, в случае отсутствия - директору. В соответствии предоставленной в заявке информации зам.директора по АХР дает задание системному администратору на внесение необходимых изменений. Проведение изменений системным администратором без наличия задания от зам.директора по АХР либо лица, его замещающего, запрещено.

6.2. Служебные записки с отметками об исполнении и подписью заявителя хранятся у зам.директора по АХР не менее 1 года.

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

7.1. После получения задания от зам.директора по АХР, системный администратор вносит соответствующие изменения в базу данных учетных записей и ставит отметку об исполнении задания на бланке служебной записки.

7.2. Все изменения в списках доступа должны быть выполнены системным администратором в течении двух рабочих дней после получения задания на внесение изменений. Служебная записка с отметкой об исполнении передается зам.директора по АХР.

7.3. По окончании процедур изменения списков доступа системный администратор вносит соответствующую запись в электронный список учета прав доступа пользователей.

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

8.1. Получив задание от зам.директора по АХР, системный администратор создает необходимые объекты безопасности, присваивает первичный пароль вновь созданной учетной записи, при необходимости создается 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 информирует об исполнении задания. Информация, необходимая для использования вновь созданного объекта безопасности (первичный пароль, «имя» учетной записи адрес электронной почты и т.п.), предоставляется пользователю указанному в служебной записке.

8.4. Заявка «На внесение изменений в списки доступа» должна быть обработана и исполнена системным администратором в течении двух рабочих дней после получения задания от зам.директора по АХР.

8.5. По окончании процедур создания нового объекта в списках доступа системный администратор вносит соответствующую запись в электронный список учета прав доступа.

9. Блокировка и удаление учетных записей пользователей, групп безопасности и почтовой рассылки

9.1. На период отсутствия сотрудника колледжа, по причине ухода на больничный, в отпуск или убытия в командировку более чем на 2 рабочих дня, специалист отдела кадров информирует системного администратора и зам.директора по АХР об этом. Системный администратор блокирует учетную запись указанного сотрудника на весь период отсутствия.

9.2. В случае увольнения сотрудника специалист отдела кадров информирует системного администратора и зам.директора по АХР об этом. Получив информацию системный администратор удаляет необходимые объекты безопасности и прекращает права доступа ко всем имеющимся в электронном списке учета информационным системам учетной записи указанного сотрудника.

9.3. После выполнения блокировки или удаления учетной записи пользователя системный администратор информирует об исполнении зам.директора по АХР.

9.4. Задача «на внесение изменений в списки доступа», предполагающая блокировку или удаление прав пользователя должна быть обработана и исполнена системным администратором в течении двух рабочих дней с момента информации.

9.5. По окончании процедур изменения, удаления объекта в списках доступа АС системный администратор вносит соответствующую запись в электронный список учета прав 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 пользователей или системного администратора 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 системному администратор.

10.3. Создание удаление и изменение служебных объектов безопасности производятся системным администратором по согласованию с зам.директора по АХР. Самостоятельное создание, изменение либо удаление служебных учетных записей системным администратором 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.

11. Локальные учетные записи

11.1. Локальные учетные записи компьютеров (Administrator, Guest) предназначены для служебного использования системным администратором 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 локальной сети 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. Первичный пароль может содержать несложную комбинацию символов, либо повторяющиеся символы.

13.1.2.Ответственность за сохранность первичного пароля лежит на системном администраторе.

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 или 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 системному администратору, записывать его, а также пересылать открытым текстом в электронных сообщениях.

13.2.4. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом системному администратору для изменения основного пароля.

13.2.5. Восстановление забытого основного пароля пользователя осуществляется системным администратором путем изменения (сброса) основного пароля пользователя на первичный пароль на основании обращения пользователя.

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

13.4. Разблокирование учетной записи пользователя осуществляется системным администратором на основании обращения владельца учетной записи.

13.5. 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. Правила работы с ресурсами Интернет приведены в Приложении 1.

14.2. Требуемый уровень доступа предоставляется сотруднику колледжа на основании заявки «на изменение списков доступа» на имя зам.директора по АХР.

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

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. Правила работы с электронной почтой приведены в Приложении 3.

15.2. Доступ к системе электронной почты предоставляется сотруднику колледжа на основании служебной записке «на изменение списков доступа» на имя зам.директора по АХР.

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 зам.директора по АХР 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.

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 ЛС) колледжа осуществляется системным администратором.

16.3. Настройка параметров средств антивирусного контроля осуществляется системным администратором 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 ЛС – 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 (USB-флешки,CD-ROM и т.п.).

16.6. Антивирусная проверка должна проводиться:

- на компьютерах сотрудников - не реже одного раза в неделю;
- на серверах ЛС - 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 системным администратором должен провести внеочередной антивирусный контроль своей рабочей станции.

17. Хранение данных

17.1. Служебная информация сотрудников колледжа должна храниться в специально выделенных папках на серверах хранения данных ЛС колледжа. Хранение служебной информации на компьютерах сотрудников, в целях обеспечения сохранности, не допускается.

17.2. Для хранения служебной информации сотрудникам предоставляется сетевая папка на СХД согласно заявке «На внесение изменений в списки пользователей». Хранение личной информации в служебных папках запрещено.

17.3. Для обеспечения целостности данных необходимо проводить резервное копирование не реже одного раза в сутки системным администратором. Резервное копирование личной информации хранящейся на рабочих станциях не предусмотрено.

17.4. Ответственность за целостность и сохранность обрабатываемых программных данных, служебной информации и документов возлагается:

- на серверах хранения данных колледжа возлагается на системного администратора.
- на служебных персональных компьютерах (локальное хранение) возлагается на самих сотрудников колледжа, использующих данные компьютеры.

18. Установка и обслуживание компьютеров, сетевого оборудования

18.1. Установка и обслуживание служебных компьютеров и сетевого оборудования возможна только системным администратором. Установка и обслуживание указанного оборудования прочими сотрудниками колледжа запрещена.

18.2. Для определения несанкционированной замены содержимого оборудования все компьютеры колледжа должны быть проинветаризированы и учтены в электронном журнале системным администратором, а в случае требования законодательства опечатана в местах возможного вскрытия.

18.3. Ответственность за технические сбои в работе оборудования лежит на системном администраторе.

18.4. Установка программ на служебные компьютеры возможна только системным администратором. Установка программ на служебные компьютеры прочими сотрудниками колледжа запрещена.

Разработал:
Заместитель директора по АХР А.В. Скворцов

Приложение 1

Правила работы сотрудников
и обучающихся колледжа в локальной сети

1. Данные правила регулируют права и обязанности обучающихся, связанные с работой в локальной сети колледжа и сети Интернет (далее Сетей), а также основные правила работы сотрудников колледжа. Правила призваны обеспечить и организовать использование образовательного потенциала Сетей в сочетании с системой мер по обеспечению охраны и безопасности обучающихся.

2. Основными принципами политики колледжа для работы в Сетях являются:

- равный доступ для всех обучающихся и сотрудников;
- использование Сетей сотрудниками и обучающимися только для служебных и образовательных целей.
- защита обучающихся от вредной или незаконной информации, содержащей: порнографию, пропаганду насилия и терроризма, этнической и религиозной нетерпимости, наркотиков, азартных игр и т.п.

3. Системный администратор обеспечивает:

- доступ обучающихся к ресурсам Сетей в соответствии с учебной программой и возможностями колледжа;
- доступ сотрудников к ресурсам Сетей в объеме необходимом для исполнения своих должностных обязанностей сотрудниками;
- помощь преподавателям и обучающимся в расширении образовательного процесса через доступ в Интернет;
- организацию мер, включая сотрудничество с провайдером, по ограничению доступа сотрудников и обучающихся к ресурсам вредного или незаконного содержания в Интернете в соответствии с действующим законодательством;
- обеспечивает контроль за соблюдением правил работы сотрудников и обучающихся в Сетях;
- технические возможности в области мониторинга трафика, передаваемого через Сеть колледжа в целях соблюдения безопасного использования Интернета сотрудниками и обучающимися;
- незамедлительно сообщает директору о выявлении нарушений и принимает меры по устранению нарушений.

4. Преподаватели компьютерных классов обязаны:

- объяснять обучающимся правила безопасного и ответственного поведения при работе в Сетях;
- использовать возможности Интернета в целях обогащения и расширения образовательной деятельности, для чего обучающимся назначать конкретные задания и приводить перечень соответствующих интернет-адресов;
- осуществлять непрерывный контроль работы обучающихся в Сетях в

учебное время;

- принимать незамедлительные меры для прекращения доступа обучающихся к ресурсам запрещенного содержания в Сетях;

- немедленно сообщать системному администратору или директору о нарушении правил или о создании незаконного контента в сети колледжа;

- не покидать учебный кабинет в учебное время, и не допускать обучающихся во время перемены к работе в Сетях;

- преподаватели несут ответственность за целостность оборудования колледжа, закрепленного за учебным кабинетом, в котором проводят занятия.

4. Обучающиеся обязаны:

- использовать Сети только для образовательных целей;

- запрещается выход на сайты, не включенные в перечень преподавателем для данного занятия;

- немедленно сообщить преподавателю при обнаружении материалов, содержащих порнографию, пропаганду насилия и терроризма, этнической и религиозной нетерпимости, наркотиков, азартных игр, и т.п.;

- не отправлять или отвечать на сообщения, оскорбительные, угрожающие или непристойные;

- избегать любой деятельности, которая угрожает целостности компьютерной сети колледжа или атаки на другие системы;

5. Сотрудникам запрещается:

- использование чужих имен пользователя, пароля и электронной почты;

- запрещено использование нелицензионного программного обеспечения, защищенных авторским правом материалов без разрешения, и любой другой деятельности, которая нарушает авторские права;

- использовать Сети в личных целях;

- выход на сайты запрещенные действующим законодательством;

- отправлять или отвечать на сообщения, оскорбительные, угрожающие или непристойные;

- любая деятельность, которая угрожает целостности компьютерной сети колледжа или атаки на автоматизированные системы;

- хранение личных сведений и файлов, не относящихся к служебной деятельности.

5. Ответственность за нарушения настоящих Правил:

- обучающиеся привлекаются к дисциплинарной ответственности в соответствии с правилами внутреннего распорядка колледжа;

- сотрудники колледжа несут ответственность в соответствии с Трудовым кодексом и привлекаются к дисциплинарной ответственности.

6. За нарушения, которые являются преступлениями, административными нарушениями или причиняют ущерб собственности, виновные несут ответственность в соответствии с законодательством РФ.

7. В целях обеспечения безопасности ресурсов локальной сети и проведения технологических мероприятий сетевой инфраструктуры используется ограничение работы пользовательских сеансов по времени.

7.1. Протяженность пользовательского сеанса устанавливается в

рабочие дни с 07 часов 30 минут до 17 часов 30 минут. Сотрудникам с ненормированным рабочим днем протяженность пользовательского сеанса устанавливается в рабочие дни с 07 часов 30 минут до 21 часов 00 минут. В выходные и праздничные дни все учетные записи блокируются.

7.2. В период нахождения на больничном или очередном отпуске учетная запись сотрудника блокируется.

8. В случае необходимости осуществления трудовой деятельности в отличное от установленного период времени, либо в отпускной период, заинтересованное лицо оформляет служебную записку на имя директора с указанием периода в который планируется осуществление трудовой деятельности, с указанием обоснования необходимости доступа к служебному компьютеру.

Приложение 2

Правила работы с ресурсами сети Интернет

1. Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. Руководство колледжа имеет право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к учебному процессу или исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых 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.

2. При работе с ресурсами сети Интернет недопустимо:

- разглашение коммерческой, служебной информации колледжа и персональных данных сотрудников и обучающихся, ставшей известной сотруднику колледжа по служебной необходимости либо иным путем;
- 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 стороны;
- публикация, загрузка и распространение материалов, содержащих 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 размещения ссылок на вышеуказанную информацию;
- загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом; использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой компании.

Возможность получить доступ к ресурсу не является гарантией того, что запрошенный ресурс является разрешенным политикой колледжа.

Вся информация о ресурсах, посещаемых сотрудниками колледжа, протоколируется и, при необходимости, может быть предоставлена руководству колледжа для детального изучения.

Приложение 3

Правила работы с электронной почтой

1. Служебная электронная почта является собственностью колледжа и должна использоваться только в целях исполнения трудовых функций сотрудника. Использование электронной почты в других целях категорически запрещено.

2. Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по решению руководства колледжа.

3. При работе со служебной электронной почты сотрудникам колледжа запрещается:

- предоставлять кому бы то ни было пароль для доступа к своему почтовому адресу;
- использовать адрес корпоративной почты для оформления подписок и массовых рассылок;
- открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, если отправитель письма неизвестен;
- осуществлять массовую рассылку почтовых сообщений (более 10) внешним адресатам без их на то согласия. Данные действия квалифицируются как СПАМ и являются незаконными;
- осуществлять массовую рассылку почтовых сообщений рекламного характера;
- 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;
- 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;
- 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.