СОГЛАСОВАНО:
Советом Учреждения
ГБПОУ
«Миасский медицинский колледж»
Протокол № 1
«11» 01 2021 г.

УТВЕРЖДЕНО:
Приказом директора Государственного бюджетного профессионального образовательного учреждения
«Миасский медицинский колледж»
от «11» 01 2021 г. № 10 ОД
Директор _____/ В.Л. Шульц

Положение
об информационной безопасности
в ГБПОУ «Миасский медицинский колледж»

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

Положение об информационной безопасности Государственного бюджетного профессионального образовательного учреждения «Миасский медицинский 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.

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.

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.

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.

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.

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).

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.

Правовую основу Положения составляют:

- Конституция Российской Федерации;
- Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»;
- Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»;
- Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Федеральный закон от 26.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью" (утв. Приказом от 29.12.2005 № 447-ст)

- другие законодательные акты, руководящие и нормативно-методические документы Российской Федерации в области обеспечения информационной безопасности.

3. Цели и задачи обеспечения безопасности информации

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.

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;

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

Система обеспечения информационной безопасности распространяются на:

- автоматизированные системы колледжа;
- средства телекоммуникаций;
- помещения;
- сотрудников колледжа.

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

5. Порядок обеспечения информационной безопасности

Организационное и техническое обеспечение рабочего процесса сотрудников возлагается на инженера по защите информации.

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.

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

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

6. Учетные записи

Локальные учетные записи компьютеров (Administrator, Guest) предназначены для служебного использования инженером по защите информации при настройке системы и не предназначены для повседневной работы.

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

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

7. Требования к паролям

Первичный пароль - комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые инженером по защите информации при создании новой учетной записи.

Установку первичного пароля производит инженер по защите информации при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на системном администраторе.

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

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.

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

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

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

Пользователь несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам, в том числе инженеру по защите информации, записывать его, а также пересылать открытым текстом в электронных сообщениях.

В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом инженеру по защите информации и изменить основной пароль.

Восстановление забытого основного пароля пользователя осуществляется инженером по защите информации путем изменения (сброса) основного пароля пользователя на первичный пароль.

8. Доступ к ресурсам Интернет

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

Доступ к ресурсам Интернет может быть блокирован инженером по защите информации без предварительного уведомления при возникновении нештатных ситуаций либо в иных случаях, предусмотренных организационными документами.

Правила работы с ресурсами Интернет приведены в приложении 2.

9. Антивирусная защита

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

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

9.3. Настройка параметров средств антивирусного контроля осуществляется инженером по защите информации в соответствии с руководствами по применению конкретных антивирусных средств. Изменение настроек другими сотрудниками запрещено.

9.4. 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.

9.5. Антивирусная проверка должна проводиться:

- на компьютерах сотрудников - не реже одного раза в неделю;
- на серверах - не реже двух раз в неделю.

9.6. 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 инженером по защите информации должен провести внеочередной антивирусный контроль своей рабочей станции.

10. Установка и обслуживание оборудования, программ

10.1. Установка и обслуживание оборудования возможна только инженером по защите информации. Установка и обслуживание оборудования сотрудниками других отделов запрещена.

10.2. Установка программ возможна только инженером по защите информации. Установка программ сотрудниками других отделов запрещена.

Приложение 1

Правила работы персонала и обучающихся колледжа в компьютерных сетях

1. Данные правила регулируют права и обязанности обучающихся, связанные с работой в компьютерной сети колледжа и сети Интернет (далее Сетей), а также основные правила работы и полномочия преподавателей и сотрудников колледжа. Правила призваны обеспечить и организовать использование образовательного потенциала Сетей в сочетании с системой мер по обеспечению охраны и безопасности студентов.
2. Основными принципами политики колледжа для работы в Сетях являются:

- равный доступ для всех обучающихся;
- использование Сетей обучающимися только для 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. Полномочия преподавателей и сотрудников.

Инженер по защите информации:

- организует и руководит всей деятельностью по реализации настоящих Правил;
- обеспечивает свободный и равный доступ обучающихся к Сетям в соответствии с учебной программой и возможностями колледжа;
- отвечает за организацию мер, включая сотрудничество с провайдером, по ограничению доступа обучающихся к ресурсам вредного или незаконного содержания в Сетях в соответствии с действующим законодательством;
- обеспечивает контроль за соблюдением правил работы обучающихся в сетях;
- организует поддержку и обновление сайта. Размещает на сайте только материалы, утвержденные директором;
- обеспечивать общую безопасность и эффективность работы в Сетях;
- предлагать и осуществлять меры по ограничению доступа обучающихся к вредным или незаконного содержания ресурсам в Сетях в соответствии с законодательством;
- периодически просматривать содержимое Сети колледжа с целью предотвращения любых возможных угроз и рисков безопасности для обучающихся;
- немедленно сообщать директору о выявлении нарушении Правил или о создании незаконного контента в сети колледжа и принимает меры по устранению нарушений.

Преподаватели компьютерных классов обязаны:

- объяснять обучающимся правила безопасного и ответственного поведения при работе в Сетях;
- использовать возможности Интернет в целях обогащения и расширения образовательной деятельности, для чего обучающимся назначать конкретные задания;
- 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 инженеру по защите информации или директору о нарушении правил или о создании незаконного контента в сети колледжа;
- не покидать учебный кабинет во время пары, 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. Права и обязанности обучающихся

Обучающиеся имеют право:

- на равный доступ к Сетям с учетом политики информатизации колледжа;
- на получение доступа к сети Интернет (только под наблюдением преподавателя);
- на грамотное и ответственное обучение работе в Сетях;

- быть информированным о правилах работы в Сетях.

Обучающиеся обязаны соблюдать следующие правила:

- 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.;
- запрещается проводить любую деятельность, которая угрожает целостности компьютерной сети колледжа или атаки на другие системы;
- запрещено использование нелицензионного программного обеспечения, защищенных авторским правом материалов без разрешения, и любой другой деятельности, которая нарушает авторские права.

5. Ответственность

Обучающиеся за нарушение положений настоящих Правил привлекаются к дисциплинарной ответственности в соответствии с правилами внутреннего распорядка колледжа.

Преподаватели и сотрудники за нарушение положений настоящих Правил несут ответственность в соответствии с Трудовым кодексом и привлекаются к дисциплинарной ответственности.

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

Приложение 2

Правила работы с ресурсами сети Интернет

Глобальная сеть Интернет предоставляет доступ к ресурсам различного содержания и направленности. Отдел по безопасности колледжа имеет право ограничивать доступ к ресурсам сети Интернет, содержание которых не имеет отношения к 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.

При работе с ресурсами сети Интернет недопустимо:

- разглашение коммерческой и служебной информации колледжа, 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.

При работе с ресурсами Интернет запрещается:

- 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.