Министерство образования Белгородской области
Областное государственное автономное
профессиональное образовательное учреждение
«Старооскольский медицинский колледж»

Утверждаю
Директор ОГАПОУ «СМК»
Н.С. Селиванов
«05» сентября 2022 г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат bead0cb8444fb6dc99073f9a7e5317746a43cdbd
Владелец Селиванов Николай Стефанович
Действителен с 04.01.2022 по 04.01.2027

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Областного государственного автономного Профессионального образовательного учреждения «Старооскольский медицинский колледж»

2022 г.

Содержание

1. Общие положения

В соответствии с Федеральным законом от 27.07.2006 г., № 149-ФЗ (с изменениями на 06.07.2016 г.) «Об информации, информационных технологиях и о защите информации», «Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации от 09.09.2000 г., решениями рабочей группы по развитию информационного общества при Совете Губернатора области ОГАПОУ «СМК» (далее - колледж) вводит отдельные *политики (правила),* направленные на обеспечение безопасности и приватности данных, управляемости информационной инфраструктурой. Политики вводятся для основных информационно-технологических (ИТ) ресурсов и процессов колледжа.

ИТ ресурсы являются неотъемлемой частью деятельности колледжа. Колледж предоставляет персоналу в пользование свои ИТ ресурсы. Руководство колледжа ожидает от персонала следования политикам, регламентам и процедурам колледжа, локальным нормативным документам, законодательству РФ при пользовании ИТ ресурсами. Неподчинение этим условиям влечет за собой ответственность соответствующих должностных лиц.

Термин "*персонал*" обозначает штатных сотрудников и других пользователей, кто имеет доступ к ИТ ресурсам колледжа в соответствии со своими должностными обязанностями.

Директор колледжа регулярно (ежегодно) корректирует политики ИТ безопасности, чтобы отражать изменения в индустриальных стандартах, законодательстве, технологиях и/или продуктах, сервисах и процессах колледжа. Политики объединены в настоящий документ, обязательны для ознакомления персоналом. Контроль исполнения политик возлагается на администратора информационной системы колледжа.

Приватность и риски персонала

ОГАПОУ «СМК» оставляет за собой право проводить мониторинг, копирование, запись и/или протоколирование всех действий персонала по использованию ИТ ресурсов без предупреждения. Это включает, но не ограничивается электронной почтой, ключами, логинами, паролями, доступом в Интернет и к файлам. Персонал не может рассчитывать на приватность при использовании ИТ ресурсов колледжа.

Ответственность и обязательства персонала

Эффективная информационная безопасность (ИБ) требует соответствующего участия персонала. Персонал несет ответственность за свои действия и, следовательно, отвечает за все события и последствия под своим идентификационным кодом пользователя (логин/пароль). Придерживаться политик и процедур доступа к сетям и системам - обязанность персонала.

Ответственность персонала включает, но не ограничивается следующим:

- считывать и передавать только данные, на которые у пользователя есть авторизованные права и которые положено знать, включая ошибочно адресованную электронную почту;
- сознательно придерживаться всех политик, законов и нормативных документов (локальных, федеральных), касающихся использованию компьютерных систем и программ;
- сообщать о нарушениях информационной безопасности ответственным за безопасность сотрудникам (инженеру-электронику/администратору информационной системы), сотрудничать в расследованиях злоупотреблений и неправомерных действий персонала с ИТ ресурсами;
- защищать назначенные имя и коды пользователя, пароли, другие ключи доступа от раскрытия;
- оберегать и содержать конфиденциальную печатную информацию, магнитные и электронные носители в предназначенных для этого местах,

когда они не в работе и размещать их в местах, обеспечивающих их безопасность;

- использовать только приобретенное колледжем лицензионное программное обеспечение, разрешенное для использования в колледже, устанавливать программы и сервисы только через инженера-электроника;
- выполнять все предписания и действия по информационной безопасности (например, по антивирусной защите, пользованию электронной почтой); не оставлять компьютер с включенным доступом в свое отсутствие - ставить экран на пароль или выходить из системы.

2. Политика пользования электронной почтой и доступа к ресурсам сети Интернет

Настоящая политика предоставляет персоналу разрешенные правила пользования ресурсами электронной почты (e-mail) и порядок доступа к ресурсам сети Интернет. Политика охватывает e-mail, приходящий или отправляемый через все принадлежащие колледжу персональные компьютеры, ноутбуки, сотовые телефоны и любые другие ресурсы, способные посылать или принимать e-mail.

Мониторинг

ИТ специалист контролирует использование e-mail, каналы доступа к ресурсам сети Интернет, чтобы гарантировать текущую доступность и надежность систем.

Политика

1. Персонал должен сохранять конфиденциальность своих паролей и, независимо от обстоятельств, *никогда не передавать в пользование и не раскрывать их никому.*
2. Персонал должен использовать электронную почту для любой переписки, касающейся деятельности колледжа.

3. Персонал должен ограничивать объемы пересылаемой по e-mail информации, чтобы по возможности не перегружать и не блокировать каналы связи.

4. Пересылаемая текстовая информация при необходимости должна сжиматься стандартными архиваторами.

5. Персонал должен готовить e-mail сообщения, соответствующие по виду и содержанию официальному статусу колледжа.

6. Персонал должен удалять подозрительные сообщения и сообщения от незнакомых адресатов, при этом заботиться о ежедневном обновлении антивирусной базы.

7. Приветствуется использование технологии считывания только заголовков почтовых сообщений, что резко сокращает вирусную опасность и трафик, связанный со спамом.

Этика поведения и ответственное пользование

Колледж обеспечивает персонал каналами доступа к сети Интернет для облегчения коммуникаций и поддержки ежедневных рабочих операций. *Этично и приемлемо:*

- связываться и обмениваться информацией согласно с целями, характером и задачами колледжа;
- использовать общепринятую лексику и ограничения в словесных описаниях, принятых в колледже;
- уважать легальную защиту, которую предусматривают различные права пользования и лицензии на ПО и данные;
- придерживаться грамотного ведения e-mail, удалять устаревшие сообщения.

Запрещено:

- нарушать требования, политики ИБ колледжа;
- публиковать, показывать или передавать любую информацию или данные, содержащие клевету, ложь, неточности, оскорбления, непристойности,

порнографию, богохульство, сексуальные домогательства, угрозы, расовые и национальные обиды и агрессивные комментарии, дискриминацию по полу, цвету волос и пр. или неверный материал;

- нарушать приватность персонала, данных и/или использовать информацию, содержащуюся в колледже, в личных интересах или выгоды;
- заниматься рассылкой и пересылкой писем других лиц, не связанной с исполнением должностных обязанностей, распространением недозволенной и другой рекламы и пр.;
- намеренное размножение, разработка или использование вредоносного программного обеспечения в любых формах (вирусы, черви, трояны и пр.);
- просмотр, перехват, раскрытие или помощь в просмотре, перехвате, раскрытии e-mail, не адресованной пользователю;
- использование для ведения служебных переговоров интернет-сервиса Skype, Zoom;
- посещать социальные сети «Одноклассники», «В контакте», «Facebook» и аналогичные при работе на компьютерах колледжа, если это не предусмотрено должностными обязанностями;
- просматривать, скачивать информацию развлекательного, рекламного характера, видео и музыкальные файлы, если это не предусмотрено должностными обязанностями или поручениями руководителя.

3. Антивирусная политика

Настоящая политика устанавливает требования, которым должны удовлетворять все компьютеры, подключенные к сети колледжа, требования к пользователям по антивирусной защите, гарантирующие эффективное определение и защиту от деструктивного воздействия вирусов.

Область применения

Настоящая политика применяется ко всем компьютерам сети

колледжа, каталогам общего пользования, к которым относятся персональные компьютеры, ноутбуки, терминалы, любое сетевое оборудование. Источниками вирусов могут быть e-mail, Интернет-сайты со скрытыми вредоносными активными элементами, носители информации (флоппи-диски, CD-диски, flash-диски и пр.), открытые для общего доступа папки и файлы и т. д.

Политика

Защита от внешних угроз и вирусов имеет несколько уровней:

а) защита от внешних вторжений, вирусов с Интернет-сайтов;

б) антивирусный контроль файлов и почтовых вложений с помощью антивирусных программ на рабочих местах пользователей;

в) стандартные средства операционных систем.

На всех компьютерах сети должно быть установлено антивирусное программное обеспечение, а в некоторых случаях в сочетании с персональным брэндмауэром. Антивирус контролирует жесткий диск и память компьютера на проникновение вируса, а брэндмауэр контролирует данные, попадающие и покидающие «внутренний периметр» через Интернет-соединение.

Это программное обеспечение должно выполняться постоянно, а также настроено для регулярного исполнения по расписанию для проверки всего содержимого жесткого диска. Кроме того, антивирусные базы должны обновляться в срок (автоматически) и содержаться в актуальном состоянии. Инфицированные вирусами компьютеры должны удаляться из сети до полного уничтожения вирусов. Работы по уничтожению вирусов, настройке запуска антивирусных процедур по расписанию выполняются специалистами системного администрирования (СА).

Все сотрудники, допущенные к работе с информационно - технологическими ресурсами колледжа, должны неукоснительно соблюдать требования инструкции по антивирусной защите, владеть навыками работы с антивирусными инструментами. Антивирусное сканирование конечные

пользователи выполняют самостоятельно.

Любая деятельность по намеренному созданию и/или распространению вредоносных программ внутри сети колледжа (вирусы, черви, трояны, почтовые бомбы и пр.) *запрещена.*

Ответственность

К сотруднику, нарушившему эту политику, применяются меры дисциплинарной ответственности.

Рекомендованные антивирусные процедуры

- НИКОГДА не открывать вложенные (присоединенные) к e-mail файлы или макросы от неизвестных, подозрительных или недостоверных источников особенно файлов в виде архива (расширения *.zip, *.rar, *.7z, *.cab) или исполняемого файла (*.exe, *.com, *.js, *.wbs, *.hta, *.bat, *.cmd), не переходить по ссылкам, указанным в письме. Удалять эти вложения немедленно, затем удалять их «физически» из «Корзины» (папки) удаленных. В противном случае возможно заражение компьютера с шифрованием данных пользователя на локальном ПК и данных на ПК других пользователей, подключенных к локально-вычислительной сети;
- удалять и не пересылать спам, рассылки и случайные e-mail сообщения;
- использовать технологии считывания только заголовков почтовых сообщений, что резко сокращает вирусную опасность и трафик, связанный со спамом;
- никогда не скачивать файлы с неизвестных, подозрительных и «зазывающих» Интернет-сайтов;
- **запретить** персоналу самостоятельно скачивать, устанавливать и запускать программы без согласования с ИТ специалистом;
- избегать предоставления дискового пространства для чтения/записи, кроме случаев абсолютной необходимости;
- **запретить** использование внешних носителей информации (флоппи-диски

CD- диски, flash-диски и пр.);

- при возникновении угроз, выявленных персональным брэндмауэром - НЕ разрешать доступ неизвестным Вам приложениям, обращаться к специалисту;

- при конфликтах в сети, замедлении работы, зависании и других необычных проявлениях в работе компьютера, всегда «останавливать», «закрывать» все программы, запускать сканирующие антивирусные программы для гарантированного лечения компьютера и информировать Ит специалиста.

4. Политика подготовки, обмена и хранения документов и данных

Настоящая политика устанавливает требования к содержанию, копированию, порядку обмена, хранению электронных и бумажных документов, файлов и информации внутри колледжа, между управлениями и их удаленными подразделениями, предоставлении прав пользования общими данными.

Область применения

Настоящая политика охватывает все подразделения, службы, отделы, чья деятельность связана с подготовкой, копированием, хранением, обменом документами, информацией, данными с использованием информационно-технологических ресурсов.

Политика

Персонал колледжа должен придерживаться следующих требований по подготовке, копированию, хранению, обмену документами, информацией, данными, файлами:

по содержанию:

- документы по виду и содержанию должны соответствовать официальному статусу колледжа, следует употреблять общепринятую деловую лексику;
- по хранению электронных документов:

- документы офисных, почтовых, графических и др. стандартных приложений (Word, Excel, PowerPoint или аналоги) должны создаваться и храниться в папках *Мои Документы (или аналогичной)*\ все папки должны иметь понятную вложенную структуру и наименования по темам;
- не допускается хранение файлов, информации **личного характера,** не относящейся к деятельности колледжа, на персональных компьютерах;

по обмену электронными документами:

- разрешено считывать, передавать, изменять только данные, на которые у пользователя есть права и которые пользователю положено знать, включая ошибочно доступные папки и электронную почту;
- внутриофисный обмен по электронной почте через Интернет не ограничивается;

по хранению электронных носителей информации:

- оберегать и содержать электронные носители, когда они не в работе, в предназначенных для этого контейнерах, полках, стеллажах, сейфах;
- не держать электронные носители на столе в пределах визуальной доступности во время отсутствия на рабочем месте.

Ответственность

К сотруднику, нарушившему эту политику, применяются меры дисциплинарной ответственности.

5. Политика информационно-технической поддержки

Настоящая политика устанавливает правила, уровни предоставления и получения персоналом информационно-технической поддержки своей работы. Доступ персонала к информационно-техническим ресурсам обеспечивается инженером-электроником на непрерывной основе, поддержкой всех технологических ресурсов в рабочем состоянии.

Поддержка требует:

а) работ по обслуживанию и развитию технологических ресурсов;

б) работ по реагированию и устранению причин этих заявок (инцидентов), т.е. работ непосредственно по поддержке. Повторяющиеся инциденты, переходят в разряд проблем и требуют выполнения внеплановых работ.

Область применения

Настоящая политика охватывает и описывает все уровни поддержки персонала, выполняемые специалистами системного администрирования.

Выделяется уровень самопомощи и три уровня поддержки:

Самопомощь - когда конечный пользователь самостоятельно выполняет действия по устранению проблемы, не нарушающие безопасность сети и других пользователей, такие как перезапуск приложения или компьютера, проверка подключения всех кабелей и сетевых ресурсов, антивирусное сканирование и пр.

Поддержка 1-го уровня - выполняется реализация работ *общего профиля:*

- решение оперативных проблем персонала, задач доступа и безопасности;
- первичная диагностика сложных проблем, причин неработоспособности программ;
- устранение проблемы или переадресация по сложности на следующий уровень.

Поддержка 2-го уровня - выполняется реализация по *работе приложений и систем.*

- углубленные, содержательные консультации и обучение;
- поиск решений имеющимися средствами (без вмешательства в логику приложений), помощь в выборке и восстановлении данных и документов, (раз)доработка отчетных форм:
- обслуживание контента и администрирование.

Поддержка 3-го уровня - выполняется реализация работ по развитию приложений, систем, инфраструктуры:

- работа с поставщиками приложений и разработчиками;
- планирование и развертывание новых приложений, реорганизация процессов и пр.

Политика

Поддержка закрепляется по уровням за техническими специалистами. Персонал должен использовать *Поддержку 1-го уровня* только после выполнения разрешенных процедур самопомощи. Многократное обращение за помощью по инцидентам, устраняемым самопомощью, указывает на несоответствие персонала занимаемой должности.

ИТ обслуживание персонала осуществляется по заявкам. Содержание заявки передается инженеру-электронику любым доступным способом (телефон, почта, бумажный носитель). Конечный пользователь должен быть информирован о порядке, времени исполнения заявки, ее движении, и, по возможности, обеспечен альтернативными ресурсами. Приоритет исполнения заявки устанавливается в связи с текущими задачами.

Работы по *Поддержке 3-го уровня* должны выполняться на проектной основе с привлечением специалистов, консультантов, подрядчиков. Внешние консультанты и подрядчики должны иметь максимально ограниченный доступ к информационно-техническим ресурсам колледжа, но достаточный для выполнения проектов. Для ведения проектов со стороны колледжа назначаются ответственные лица.

Ответственность

К сотруднику, нарушившему эту политику, применяются меры дисциплинарной ответственности.