Государственное бюджетное профессиональное образовательное учреждение Республики Марий Эл «Йошкар-Олинский медицинский колледж»
ИНН 1215039970, ОГРН 1021200755290, КПП 121501001
424037, г. Йошкар-Ола, ул. Пролетарская, д. 68

УТВЕРЖДЕНО
приказом директора ГБПОУ РМЭ
«Йошкар-Олинский медколледж»
№ 99-П от 18.09.2025
регистрационный номер 298

Положение
об информационной безопасности (защите информации) в ГБПОУ РМЭ «Йошкар-Олинский медколледж»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об информационной безопасности (защите информации) (далее – Положение) разработано в соответствии с:

- Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и защите информации";

- Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных";

- "ГОСТ Р 51583-2014. Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения" (утвержден и введен в действие Приказом Росстандарта от 28.01.2014 N 3-ст);

- "ГОСТ Р 56545-2015. Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей" (утвержден и введен в действие Приказом Росстандарта от 19.08.2015 N 1180-ст);

- "ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования" (принят и введен в действие Постановлением Госстандарта Российской Федерации от 09.02.1995 N 49);

- "ГОСТ Р 56938-2016. Национальный стандарт Российской Федерации. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения" (утвержден и введен в действие Приказом Росстандарта от 01.06.2016 N 457-ст);

- "ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности" (утв. Приказом Ростехрегулирования от 27.12.2007 N 513-ст);

- "ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции" (утвержден и введен в действие Приказом Росстандарта от 01.12.2011 N 683-ст);

- и иными нормами действующего законодательства Российской Федерации.

1.2. Положение обязательно к исполнению всеми работниками колледжа и обучающимися.

1.3. Положение подлежит применению по месту нахождения колледжа - адрес: _г. Йошкар-

Ола, ул. Пролетарская, 68 (основной корпус), а также по адресам: г.Йошкар-Ола, ул. Прохорова, 24 (корпус № 2), ул. Й. Кырли. 10 (корпус № 3), г. Волжск, ул. Советская, 29А (филиал).

1.4. Сокращения Положения:

- ИС - информационные системы;

- СВТ - средства вычислительной техники;

- НСД - несанкционированный доступ;

- КСЗ - комплекс средств защиты;

- ЗИ - защита информации;

- ВВС - виртуальные вычислительные системы;

- ПРД - правила разграничения доступа;

- ГРИИБ - группа реагирования на инциденты информационной безопасности.

1.5. Подразделением, отвечающим за реализацию настоящего Положения, является учебно-вычислительный отдел (далее - УВО).

1.6. Информационная безопасность обеспечивается реализацией следующих мер:

1.6.1. Выполнение технических требований.

1.6.2. Идентификация уязвимостей.

1.6.3. Защита при использовании технологий виртуализации.

1.6.4. Применение системы менеджмента инцидентов информационной безопасности.

1.6.5. Создание структурных подразделений, обеспечивающих информационную безопасность.

1.6.6. Обучение работников колледжа приемам информационной безопасности. Требование от работников их выполнения.

1.6.7. Использование КСЗ.

1.6.8. Мониторинг и проверка эксплуатации комплекса программных и технических средств и услуг.

1.6.9. Подготовка предложений по финансированию мероприятий по защите информации.

1.6.10. Оборудование помещений, предназначенных для размещения средств обработки информации ИС, системами инженерно-технического обеспечения (вентиляции, теплоснабжения, кондиционирования, охраны, сигнализации, пожаротушения, энергообеспечения) в соответствии с требованиями по защите информации.

1.6.11. Организация технического обслуживания и ремонта средств вычислительной техники, предназначенных для обработки информации ограниченного доступа, с учетом требований по защите информации.

II. ЗАЩИТА ИНФОРМАЦИИ

2.1. Защита информации в Колледже представляет собой принятие правовых,

организационных и технических мер, направленных:

1) на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2.2. Колледж как обладатель информации и/или оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязана обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации;

8) документирование доказательств неправомерного доступа к компьютерной информации, создания, использования и распространения вредоносных компьютерных программ, нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, нарушения правил защиты информации, незаконной деятельности в области защиты информации, разглашения информации с ограниченным доступом, воспрепятствования уверенной работе сайтов в сети Интернет, нарушения требований законодательства о хранении документов и информации, содержащейся в информационных системах;

9) сопровождение исполнения заключенных колледже договоров на закупку товаров, работ и услуг по темам развития и обеспечения защиты информации;

10) ведение реестра приобретенных средств защиты информации;

11) проведение служебных расследований по фактам нарушения требований защиты информации;

12) взаимодействие с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации по вопросам защиты информации в колледже;

13) обеспечение устойчивости и адаптивности ИС;

14) финансирование мероприятий по защите информации в колледже;

15) закупка товаров, работ и услуг, направленных на обеспечение защиты информации.

2.3. Информация, полученная работниками колледжа при исполнении ими профессиональных обязанностей или самой колледжем при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

2.4. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

2.5. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия колледжем или лица, предоставившего такую информацию о себе.

2.6. Порядок доступа к персональным данным граждан устанавливается Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных".

2.7. Документирование информации осуществляется в соответствии с установленными правилами делопроизводства.

2.8. Право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

2.9. Защита государственной тайны, коммерческой тайны, конфиденциальной информации обеспечивается в соответствии с федеральным законодательством и принятыми локальными нормативно-правовыми актами.

III. ВЫПОЛНЕНИЕ ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ

3.1. Защищенность от НСД к информации при ее обработке СВТ характеризуется тем, что только надлежащим образом уполномоченные лица или процессы, инициированные ими, будут иметь доступ к ознакомлению, созданию, изменению или уничтожению информации.

3.2. Защищенность обеспечивается выполнением трех групп требований к средствам защиты, реализуемым в СВТ:

а) требования к разграничению доступа, предусматривающие то, что СВТ должны поддерживать непротиворечивые, однозначно определенные правила разграничения доступа;

б) требования к учету, предусматривающие то, что СВТ должны поддерживать регистрацию событий, имеющих отношение к защищенности информации;

в) требования к гарантиям, предусматривающие необходимость наличия в составе СВТ технических и программных механизмов, позволяющих получить гарантии того, что СВТ обеспечивают выполнение требований к разграничению доступа и к учету.

3.3. Согласование требований к техническим характеристикам объектов закупки и технических заданий в части обеспечения защиты информации на закупку колледжем товаров, работ и услуг, направленных на развитие и обеспечение функционирования ИС обязательно.

3.4. Подготовка и утверждение требований к техническим характеристикам объектов закупки и технических заданий на закупку Колледжем товаров, работ и услуг, направленных на развитие и обеспечение защиты информации, выполняется УВО.

3.5. Мониторинг и систематическая проверка эксплуатации комплекса программных и технических средств и услуг выполняется УВО в течение всего срока их использования.

IV. 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 колледжапринятие

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 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 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 заведующий УВО. Руководители структурных подразделений колледжа обязаны участвовать в ее поддержании в надлежащем состоянии, дальнейшем развитии и совершенствовании по своим направлениям деятельности.

V. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ НА ОБУЧАЮЩЕМ ПОРТАЛЕ КОЛЛЕДЖА

5.1. Портал Колледжа относится к группе многопользовательских информационных систем разными правами доступа.
5.2. С учетом особенностей обрабатываемой информации, система соответствует требованиям, предъявляемым действующим в Российской Федерации законодательством, к информационным системам, осуществляющим обработку персональных данных.
5.3. Портал колледжа обеспечивает возможность защиты информации от потери и несанкционированного доступа на этапах её передачи и хранения.
5.4. Для настройки прав пользователей в системе созданы отдельные роли пользователей с назначением разрешений на выполнение отдельных функций и ограничений по доступу к информации, обрабатываемой на портале колледжа.
5.5. Регламент общих ограничений для участников образовательного процесса при работе с порталом колледжа, обеспечивающим предоставление Услуги.
5.6. Участники образовательного процесса, имеющие доступ к порталу колледжа, не имеют права передавать персональные логины и пароли для входа на портал другим лицам.
5.7. Передача персонального логина и пароля для входа на портал колледжа другим лицам влечет за собой ответственность в соответствии с законодательством Российской Федерации о защите персональных данных.
5.8. Участники образовательного процесса, имеющие доступ к порталу колледжа, соблюдают конфиденциальность условий доступа в свой личный кабинет (логин и пароль).
5.9. Участники образовательного процесса, имеющие доступ к порталу колледжа, в случае нарушения конфиденциальности условий доступа в личный кабинет, уведомляют в течение не

более чем одного рабочего дня со дня получения информации о таком нарушении службу технической поддержки портала.
5.10. Все операции, произведенные участниками образовательного процесса, имеющими доступ к порталу колледжа, с момента получения информации службой технической поддержки о нарушении, указанном в предыдущем абзаце, признаются недействительными.
5.11. При проведении работ по обеспечению безопасности информации в портале Колледжа участники образовательного процесса, имеющие доступ к порталу, обязаны соблюдать требования законодательства Российской Федерации в области защиты персональных данных.

VI. ДОСТУП К СЕТИ ИНТЕРНЕТ

6.1. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.
6.2. Сотрудникам Колледжа:
6.2.1. разрешается использовать сеть Интернет только в служебных целях;
6.2.2. запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения, пропаганду расовой ненависти, дискредитирующие заявления или иные материалы с оскорбительными, высказываниями по поводу чьего-либо возраста, религиозных или политических убеждений, национального происхождения или недееспособности;
6.2.3. запрещается использовать сеть Интернет для хранения конфиденциальных данных Колледжа;
6.2.4. разрешается использовать Интернет-ресурсы только режимом просмотра информации, исключая возможность передачи информации Колледжа в сеть Интернет, кроме специально регламентированных случаев.
6.2.5. перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
6.3. Руководство Колледжа и лицо, ответственное за информационную безопасность имеют право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.
6.4. Обучающимся и сотрудникам Колледжа запрещается
6.4.1 распространять (в том числе в социальных сетях) материалы, содержащие призыв к экстремистской деятельности, совершению самоубийства, а также материалы порнографического характера;
6.4.2. использовать на территории Колледжа, общежития, медицинских организаций мобильный телефон, планшет, компьютер для посещения сайтов, содержащих экстремистскую информацию, призывы к самоубийству, имеющие содержание порнографического характера.
6.4.3. Пользователь «точки доступа к Интернету» (сотрудник или обучающийся) в Колледже несет ответственность за содержание передаваемой, принимаемой и распечатываемой информации.
6.5. Лица, не соблюдающие настоящий регламент работ, лишаются права работы в «точке доступа к Интернету».
6.6. При нанесении любого ущерба «точке доступа к Интернету» (порча имущества, вывод оборудования из рабочего состояния) пользователь (сотрудник или обучающийся) несет материальную ответственность.
6.7. Обучающийся обязан подчиняться лицу, уполномоченному контролировать использование сети Интернет.
6.8. Обучающийся, использующий «точку доступа к Интернету» обязан:
6.8.1. Соблюдать тишину, порядок и чистоту в «точке доступа к Интернету», а также выполнять указания ответственного за «точку доступа к Интернету» по первому требованию.
6.8.2. Посещать Интернет-ресурсы только образовательной направленности.
6.8.3Сообщить ответственному лицу о случайном попадании на ресурс, явно не соответствующий образовательной направленности и/или нарушающий законодательство Российской Федерации с указанием Интернет-адреса ресурса, затем немедленно покинуть ресурс;
6.9. Обучающемуся - пользователю сети Интернет в Колледже запрещается:

6.9.1 Посещать сайты, содержащие необразовательную (порнографическую и антигосударственную информацию, информацию со сценами насилия и т. п.), участвовать в нетематических чатах, форумах, конференциях, общаться в любых социальных сетях.
6.9.2. Посещать сайты, содержащие необразовательную (порнографическую и антигосударственную информацию, информацию со сценами насилия и т. п.), участвовать в нетематических чатах, форумах, конференциях, общаться в любых социальных сетях.
6.9.3. Распространять, пересылать и записывать хакерскую, коммерческую, рекламную, непристойную, клеветническую, антигосударственную, угрожающую информацию, а также информацию, порочащую честь и достоинство граждан.
6.9.4. Устанавливать на компьютерах дополнительное программное обеспечение, как полученное в Интернете, так и любое другое;
6.9.5. Изменять конфигурацию компьютеров, в том числе менять системные настройки компьютера и всех программ, установленных на нем (заставки, картинку рабочего стола, стартовую страницу браузера).
6.9.6. Включать, выключать и перезагружать компьютер без согласования с ответственным за «точку доступа к Интернету».
6.9.7. Осуществлять действия, направленные на «взлом» любых компьютеров, находящихся как в «точке доступа к Интернету» Колледжа, так и за его пределами.
Использовать в качестве съемного носителя информации мобильные устройства.
6.10. Обучающиеся - пользователи «точки доступа к Интернету» в Колледже имеют право работать в сети Интернет в течение одного часа, если ответственный за использование Интернет не определит иначе. При необходимости время работы может быть увеличено по согласованию с ответственным за «точку доступа к Интернету» и при отсутствии иных лиц, желающих воспользоваться доступом к Интернет-ресурсам.
6.11. Иметь личную учетную запись электронной почты на самостоятельно выбранном Интернет-ресурсе.
6.12. Сохранять полученную информацию на съемном носителе информации (за исключением мобильных устройств). Любые съемные носители информации перед использованием на служебном компьютере должны в обязательном порядке предварительно проверяться антивирусной программой колледжа/филиала.

VII. ПРАВИЛА ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

7.1. Использование служебной электронной почты в личных целях не допускается
7.2. Использование сотрудниками Колледжа публичных и персональных почтовых ящиков электронной почты осуществляется только при согласовании с руководством Колледжа.
7.3. Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю.
7.4. Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.
7.5. Недопустимые действия сотрудников при использовании электронной почты:
7.5.1 групповая рассылка всем пользователям Колледжа сообщений/писем;
подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
7.5.2. поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
7.5.3 пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как

уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит корпоративным стандартам, в области этики.

7.6. Ко всем исходящим сообщениям, направляемым внешним пользователям, пользователь может добавлять уведомление о конфиденциальности.

7.7. Вложения, отправляемые вместе с сообщениями, следует использовать с должной осторожностью. Во вложениях всегда должна указываться дата их подготовки, и. они должны оформляться в соответствии с установленными в Колледже процедурами документооборота,

VIII. ЗАЩИТА ОБОРУДОВАНИЯ

8.1. Сотрудники Колледжа ДОЛЖНЫ ПОСТОЯННО ПОМНИТЬ о необходимости обеспечения физической безопасности оборудования, на котором хранятся информация Колледжа

8.2. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения может производить только ответственный сотрудник, либо специалисты, имеющие определенный допуск к аппаратному и программному обеспечению. Любые изменения в конфигурации аппаратного и программного обеспечения осуществляются только после согласования с руководством Колледжа.

8.3. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (принтеры и сканеры), аксессуары (манипуляторы типа «мышь», шаровые манипуляторы, дисководы для CO-дисков), коммуникационное оборудование (сетевые адаптеры и концентраторы), предоставленное Колледжем, является его собственностью и предназначено для использования исключительно в производственных целях.

8.4. Пользователи портативных компьютеров, содержащих информацию, принадлежащую Колледжу, обязаны обеспечить их хранение в физически защищенных помещениях, запираемых ящиках рабочего стола, шкафах, или. обеспечить их защиту с помощью аналогичного по степени эффективности защитного устройства, в случаях, когда данный компьютер не используется,

8.5. Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности, как в Колледже, так и по месту проживания. В ситуациях, когда возрастает степень риска кражи портативных компьютеров, например, в гостиницах, аэропортах и т.д, пользователи обязаны ни при каких обстоятельств не оставлять их без присмотра. Во время поездки в автомобиле портативный компьютер должен находиться в багажнике. На ночь его следует перенести из автомобиля в гостиничный номер.

8.6. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая, жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных.

8.7. Все программное обеспечение, установленное на предоставленном Колледжем компьютерном оборудовании, является собственностью Колледжа, и должно использоваться исключительно в производственных целях.

8.8. Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если, в ходе выполнения технического обслуживания, будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено руководству Колледжа.

IX. ОБЕСПЕЧЕНИЕ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

9.1. На всех компьютерах, принадлежащих Колледжу, должно быть установлено лицензионное антивирусное программное обеспечение.
9.2. Все компьютеры, подключенные к локальной сети, должны быть оснащены системой антивирусной защиты.
9.3. Сотрудники Колледжа не должны:
9.3.1. блокировать антивирусное программное обеспечение;
9.3.2. устанавливать другое антивирусное программное обеспечение;
9.3.3. изменять настройки и конфигурацию антивирусного программного обеспечения,
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 (магнитных дисках, флеш-носителях и т.п.). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съёмный носитель).
9.5. Файлы, помещаемые в электронный архив, в обязательном порядке должны подвергаться антивирусному контролю.
9.6. Ежедневно в начале работы при загрузке компьютера (для серверов локальной сети — при перезапуске) в автоматическом режиме должно выполняться обновление антивирусных баз и проводиться антивирусный контроль всех дисков и файлов персонального компьютера.
9.7. Периодические проверки электронных архивов проводятся не реже одного раза в неделю.
9.8. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера выполняется:
9.8.1. непосредственно после установки (изменения) программного обеспечения компьютера;
9.8.2. 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.).

X. СООБЩЕНИЕ ОБ ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РЕАГИРОВАНИЕ И ОТЧЕТНОСТЬ

10.1. Все пользователи должны сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.
10.2. В случае кражи переносного компьютера, принадлежащего Колледжу, следует незамедлительно сообщить об инциденте руководству Колледжа.
10.3. Пользователи должны знать способы информирования об известных или предполагаемых случаях нарушения информационной: безопасности с использованием телефонной связи, электронной почты и других методов. Необходимо обеспечить контроль и учет сообщений об инцидентах и принятие соответствующих мер.
10.4. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:
10.4.1. приостановить работу;
10.4.2. немедленно поставить в известность о факте обнаружения заражённых вирусом файлов ответственного за обеспечение информационной безопасности в Колледже;
10.4.3. не пользоваться и не выключать зараженный компьютер;
10.4.4. не подсоединять этот компьютер к компьютерной сети Колледжа до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование информационным отделом.

XI.УПРАВЛЕНИЕ ЛОКАЛЬНОЙ СЕТЬЮ

11.1. Уполномоченные сотрудники контролируют содержание всех потоков данных проходящих через локальную сеть Колледжа.

11.2. Сотрудникам Колледжа запрещается:
11.2.1. нарушать информационную безопасность и работу локальной сети Колледжа;
11.2.2. сканировать порты или систему безопасности;
11.2.3. контролировать работу сети с перехватом данных;
11.2.4. получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности,
11.2.5. использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;
11.2.6. передавать информацию о сотрудниках или списки сотрудников Колледжа посторонним лицам;
11.2.7. передавать информацию об обучающихся в Колледже посторонним лицам;
11.2.8. создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

XII. ЗАЩИТА И СОХРАННОСТЬ ДАННЫХ

12.1. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах Колледжа лежит на пользователях.
12.2. Необходимо регулярно делать резервные копии, всех основных служебных данных и. программного обеспечения.
12.3. Уполномоченное лицо на основании заявок руководителей подразделений может создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями, доступа к ним.
12.4. Сотрудники имеют право создавать/удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.
12.5. Информация, хранящаяся на предоставляемых Колледжем компьютерах и носителях информации, подлежит обязательной проверке на отсутствие вредоносного программного обеспечения.
12.6. Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется комиссионно с составлением акта.
12.7. В случае увольнения или перевода работника в другое структурное подразделение Колледжа, предоставленные ему компьютер и носители информации изымаются.

XIII. ОТВЕТСТВЕННОСТЬ

13.1. Обучающиеся за нарушение положений настоящих Правил привлекаются к дисциплинарной ответственности в соответствии с правилами внутреннего распорядка Колледжа.
13.2 Преподаватели и сотрудники за нарушение положений настоящих Правил несут ответственность в соответствии с Трудовым кодексом и привлекаются к дисциплинарной ответственности.
13.3. За нарушения, которые являются преступлениями, административными нарушениями или причиняют ущерб собственности, виновные несут ответственность в соответствии с законодательством РФ.

Заведующий УВО  В.И.Бурдин

СОГЛАСОВАНО:
Председатель профсоюза  М.Е. Криницына

Начальник отдела кадров  М.В. Елькина