ЧАСТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«МЕДИЦИНСКИЙ КОЛЛЕДЖ «ПРИЗВАНИЕ»

РАССМОТРЕНО И ОДОБРЕНО

на Общем собрании
трудового коллектива
Частного профессионального
образовательного учреждения
«Медицинский Колледж «Призвание»
Протокол № 1 от «5» июля 2017 г.

УТВЕРЖДАЮ

Директор
Частного профессионального
образовательного учреждения
«Медицинский Колледж «Призвание»
_____ М.С. Шогенова
«07» июля 2017 г.

ИНСТРУКЦИЯ
ПОЛЬЗОВАТЕЛЮ ПО СОБЛЮДЕНИЮ РЕЖИМА ЗАЩИТЫ ИНФОРМАЦИИ ПРИ РАБОТЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЧПОУ «МЕДКОЛЛЕДЖ «ПРИЗВАНИЕ»

г. Нальчик
2017 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение определяет порядок работы сотрудников Частного профессионального образовательного учреждения «Медицинский Колледж «Призвание» (далее – Колледж) в части:

- обеспечения безопасности конфиденциальной информации при её обработке, хранении и передаче в автоматизированных системах,
- использования средств защиты информации,
- разработки и принятия мер по предотвращению возможных опасных последствий таких нарушений,
- порядка обучения персонала практике работы с конфиденциальной информацией, предусмотренных эксплуатационной и технической документацией,
- порядка проверки электронного журнала обращений к АС,
- порядка контроля соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией,
- правил обновления общесистемного и прикладного программного обеспечения,
- правил организации антивирусной защиты и парольной защиты,
- порядка охраны и допуска посторонних лиц в защищаемые помещения.

II. ОРГАНИЗАЦИОННЫЕ ВОПРОСЫ БЕЗОПАСНОСТИ

2.1. Ответственным за разработку и реализацию политики информационной безопасности является администратор информационной безопасности, который отвечает за её реализацию и пересмотр в соответствии с установленной процедурой. Указанная процедура обеспечивает осуществление пересмотра политики информационной безопасности в соответствии с изменениями, влияющими на основу первоначальной оценки риска, появление новых уязвимостей или изменения организационной или технологической инфраструктуры. Периодические пересмотры должны осуществляться ежегодно и включать:

- проверку эффективности политики, исходя из характера, числа и последствий зарегистрированных инцидентов нарушения информационной безопасности;
- определение стоимости мероприятий по управлению информационной безопасностью и их влияние на эффективность бизнеса;
- оценку влияния изменений в технологиях.

2.2. Ответственность за организацию разработки и внедрения системы информационной безопасности, а также за оказание содействия в определении мероприятий по управлению информационной безопасностью возлагается на администратора информационной безопасности.

2.3. В повседневные обязанности администратора информационной безопасности входит обеспечение безопасности данного актива.

2.4. Приказом директора Колледжа определяются:

2.4.1. информационные активы и процессы (процедуры) безопасности, связанные с каждой отдельной автоматизированной системой;

2.4.2. ответственные за эксплуатацию и обеспечение безопасности каждой автоматизированной системы;

2.4.3. уровни полномочий (авторизации) пользователей автоматизированных систем.

2.5. Информационными активами, связанными с информационными системами, являются:

- информационные активы: базы данных и файлы данных, системная документация, руководства пользователя, учебные материалы, процедуры эксплуатации или поддержки (обслуживания), планы по обеспечению непрерывности функционирования информационного обеспечения, процедуры действий при сбоях, архивированная информация;
- активы программного обеспечения: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства разработки и утилиты;
- физические активы: компьютерное оборудование (процессоры, мониторы, переносные компьютеры, модемы), оборудование связи (маршрутизаторы, частные автоматические телефонные станции с выходом в сеть общего пользования, факсы, автоответчики), магнитные носители (ленты и диски), другое техническое оборудование (электропитание, кондиционеры), мебель, помещения;
- услуги: вычислительные услуги и услуги связи, основные коммунальные услуги (отопление, освещение, электроэнергия, кондиционирование).

III. КЛАССИФИКАЦИЯ ИНФОРМАЦИИ

3.1 С целью обеспечения защиты на надлежащем уровне информационных активов информацию следует классифицировать, чтобы определить её приоритетность, необходимость и степень её защиты.

Конфиденциальная информация требует дополнительного уровня защиты или специальных методов обработки.

Классификация информации позволяет определить, как эта информация должна быть обработана и защищена.

Система классификации информации используется для определения соответствующего множества уровней защиты и потребности в специальных методах обработки.

3.2 Для проведения классификации автоматизированных систем приказом директора Колледжа создаётся комиссия. Результатом работы комиссии является Акт классификации автоматизированной системы.

3.3 При проведении классификации и категорирования автоматизированных систем комиссия пользуется руководящими документами:

- руководящим документом ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;
- «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации по технической защите конфиденциальной информации (СТР-К)»;
- другими действующими нормативными документами в области информационной безопасности

IV. ДОСТУП К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

4.1. Система доступа представляет собой совокупность норм и правил, определяющих, кто из руководителей, кому из пользователей и с какими категориями документов можно давать разрешение на ознакомление.

4.2. Система доступа должна отвечать следующим требованиям:

доступ к конфиденциальным документам может предоставляться гражданским служащим, письменно оформившим с представителем нанимателя отношения о неразглашении ставших им известными конфиденциальных сведений. Письменное оформление отношений о неразглашении конфиденциальной информации (соблюдения

режима конфиденциальности) является обязательным условием для доступа исполнителей к документам;

доступ к конфиденциальным документам должен быть обоснованным, т.е. базироваться на служебной необходимости ознакомления с конкретным документом именно данного исполнителя;

система доступа должна давать возможность обеспечивать исполнителей всеми необходимыми им в силу служебных обязанностей документами, но только теми, которые действительно необходимы для выполнения конкретного вида работ;

доступ к документам должен быть санкционированным, т.е. осуществляться только по соответствующему разрешению уполномоченного на то должностного лица. При этом соответствующее должностное лицо может давать разрешение на ознакомление с документами только входящими в сферу его деятельности и только установленному кругу лиц;

доступ должен оформляться письменно по каждому конкретному конфиденциальному документу. При необходимости ознакомления исполнителя только с частью документа в разрешении на ознакомление должны быть указаны разделы (пункты или страницы), с которыми можно знакомить исполнителя;

доступ сотрудников к конфиденциальной информации осуществляется на добровольной основе. Эти отношения устанавливаются при приёме на работу или же при осуществлении трудовой деятельности лицом. При этом необходимо выполнить следующие условия:

- ознакомить сотрудника под подпись с перечнем конфиденциальной информации;
- ознакомить сотрудника под подпись с установленным в Колледжа режимом по охране конфиденциальности и с мерами ответственности за его нарушение;
- создать сотруднику необходимые условия для соблюдения им установленного режима по охране конфиденциальности.

4.3. Права гражданских служащих на доступ к конфиденциальной информации и работу с её носителями регулируются разрешениями полномочных должностных лиц, оформленными в письменном (документальном) виде.

4.4. Оформление таких разрешений осуществляется директором Колледжа.

4.5. Именные (должностные) списки сотрудников, допускаемых к конфиденциальной информации, в обязательном порядке содержат должности и фамилии, а также категории сведений (документов), к которым они допускаются.

4.6. Разрешение может оформляться:

непосредственно на документе (носителе информации) в виде резолюции (поручения), адресованного сотруднику;

либо посредством указания (перечисления) в организационно-плановых и иных документах Колледжа работников (их фамилий), которые при решении конкретных служебных и иных задач должны быть допущены к конфиденциальной информации.

4.7. Функции (роли) и ответственность в области информационной безопасности, должны быть документированы. В должностные регламенты включаются как общие обязанности по внедрению или соблюдению политики безопасности, так и специфические особенности по защите определенных активов или действий, касающихся безопасности.

Руководители структурных подразделений обязаны:

- ознакомить под расписку сотрудника, которому для выполнения его служебных обязанностей нужен доступ к информации, распространение которой в Российской Федерации ограничивается или запрещается, с перечнем информации, составляющей конфиденциальную информацию, обладателем которой является Колледж;
- ознакомить под расписку сотрудника с настоящим Положением и с мерами ответственности за его нарушение;

– создать сотруднику необходимые условия для соблюдения им установленного настоящим Положением порядка организации и проведения работ по защите конфиденциальной информации в Колледже.

4.8. Проверка достоверности представляемых гражданином персональных данных и иных сведений при трудоустройстве в Колледж осуществляется специалистом по кадрам в соответствии с действующим законодательством РФ.

V. СОГЛАШЕНИЯ О КОНФИДЕНЦИАЛЬНОСТИ

5.1 Все сотрудники Колледжа должны подписывать соглашение о конфиденциальности (неразглашении).

5.2 Соглашения о конфиденциальности или соглашения о неразглашении используются для уведомления сотрудников о том, что информация является конфиденциальной. Сотрудники должны подписывать такое соглашение как неотъемлемую часть условий трудового договора (соглашения).

5.3 Условия соглашения должны определять ответственность сотрудника в отношении информационной безопасности. Эта ответственность должна сохраняться и в течение определённого срока (три года) после увольнения. В соглашении указываются меры дисциплинарного воздействия, которые будут применимы в случае нарушения гражданским служащим требований безопасности.

5.4 С целью обеспечения уверенности в осведомленности пользователей об угрозах и проблемах, связанных с информационной безопасностью, и их оснащённости всем необходимым для соблюдения требований политики безопасности Колледжа при выполнении служебных обязанностей, пользователей необходимо обучать процедурам безопасности и правильному использованию средств обработки информации, чтобы свести к минимуму возможные риски безопасности.

VI. ПОРЯДОК РАБОТЫ СОТРУДНИКОВ КОЛЛЕДЖА В ЧАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В АС

6.1. При обработке данных в АС необходимо руководствоваться Положением по обеспечению безопасности конфиденциальной информации при её обработке в автоматизированных системах и защищаемых помещениях, утверждённым Колледжем.

6.2. Все сотрудники должны быть осведомлены о процедурах информирования о различных типах инцидентов нарушения информационной безопасности (нарушение безопасности, угроза, уязвимость системы или сбой), которые могли бы оказать негативное влияние на безопасность активов Колледжа.

Сотрудники должны немедленно сообщать о любых наблюдаемых или предполагаемых инцидентах своему непосредственному руководителю или администратору безопасности.

6.3. Перед началом работы в АС пользователи должны ознакомиться с инструкциями по использованию программных и технических средств, по использованию средств защиты информации под роспись.

6.4. Пользователи должны продемонстрировать администратору безопасности и (или) ответственному за защиту информации наличие необходимых знаний и умений для выполнения требований настоящего Положения.

6.5. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности конфиденциальных данных в соответствии с требованиями настоящего положения, к работе в АС не допускаются.

6.6. Ответственным за организацию обучения и оказание методической помощи в организации является администратор информационной безопасности.

VII. ТРЕБОВАНИЯ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

7.1. Система (подсистема) защиты информации, обрабатываемой в АС различного уровня и назначения, должна предусматривать комплекс организационных, программных, технических средств и мер по защите информации при её автоматизированной обработке, хранении и передаче по каналам связи.

7.2. Основными направлениями защиты информации являются:

обеспечение защиты информации от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней за счет НСД и специальных воздействий;

обеспечение защиты информации от утечки по техническим каналам при её обработке, хранении и передаче по каналам связи.

7.3. В качестве основных мер защиты информации необходимо:

документально оформить перечень сведений конфиденциального характера;

система допуска пользователей к информации и связанным с её использованием работам, документам должна осуществляться в соответствии с нормами настоящего Положения;

доступ сотрудников и посторонних лиц в ЗП и помещения, где размещены средства информатизации и коммуникационное оборудование должен быть ограничен;

действия пользователей АС, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц должен регистрироваться;

обеспечить учёт и надёжное хранение бумажных и машинных носителей конфиденциальной информации и их обращение, исключающее хищение, подмену и уничтожение;

ответственным за эксплуатацию АС назначаются руководители структурных подразделений Колледжа;

из числа сотрудников назначается администратор безопасности АС;

автоматизированные системы обработки конфиденциальной информации должны быть аттестованы по требованиям безопасности информации.

VIII. ЗАЩИТА ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

8.1 С целью обеспечения защиты целостности программного обеспечения и массивов информации должны быть приняты меры предотвращения и обнаружения внедрения вредоносного программного обеспечения.

8.2 Пользователи должны быть осведомлены об опасности использования неавторизованного или вредоносного программного обеспечения.

8.3 С целью обнаружения и предотвращения проникновения вредоносного программного обеспечения автоматизированные системы должны быть оснащены средствами защиты от вредоносного программного обеспечения.

8.4 Устанавливаются следующие мероприятия по управлению информационной безопасностью:

в автоматизированных системах используется программное обеспечение на основе лицензионных соглашений, запрещается использование неавторизованного программного обеспечения;

запрещается получать файлы и программное обеспечение из внешних сетей, через внешние сети или из любой другой среды;

должно быть установлено и регулярно обновляться антивирусное программное обеспечение для обнаружения и сканирования компьютеров и носителей информации, запускаемое в случае необходимости в качестве превентивной меры или рутинной процедуры;

должна обеспечиваться проверка всех файлов на носителях информации сомнительного или неавторизованного происхождения или файлов, полученных из общедоступных сетей, на наличие вирусов перед работой с этими файлами;

должна обеспечиваться проверка любых вложений электронной почты и скачиваемой информации на наличие вредоносного программного обеспечения до их использования.

IX. ПРАВИЛА АНТИВИРУСНОЙ ЗАЩИТЫ

9.1. При обеспечении антивирусной защиты необходимо руководствоваться нормами данного Положения по обеспечению безопасности конфиденциальной информации при ее обработке в автоматизированных системах и защищаемых помещениях, утверждённым Колледжем.

9.2. Резервное копирование важной служебной информации и программного обеспечения должно выполняться на регулярной основе.

9.3. Должны выполняться следующие мероприятия по управлению информационной безопасностью:

минимально необходимый объём резервной информации, вместе с точными и полными регистрационными записями по содержанию резервных копий, а также документация по процедурам восстановления во избежание любого повреждения от стихийных бедствий должны храниться в отдельном месте;

резервная информация должна быть обеспечена гарантированным уровнем физической защиты и защиты от воздействий окружающей среды;

резервное оборудование должно регулярно подвергаться тестированию для обеспечения уверенности в том, что в случае возникновения чрезвычайных ситуаций на его работу можно положиться;

процедуры восстановления следует регулярно актуализировать и тестировать для обеспечения уверенности в их эффективности, а также в том, что для выполнения этих процедур потребуется не больше времени, чем определено операционными процедурами восстановления;

ответственным за организацию резервирования назначается руководитель структурного подразделения.

X. БЕЗОПАСНОСТЬ НОСИТЕЛЕЙ ИНФОРМАЦИИ

10.1 С целью предотвращения повреждений активов использование носителей информации должно контролироваться, а также должна обеспечиваться их физическая безопасность.

10.2 Должны выполняться следующие мероприятия по управлению информационной безопасностью:

- если носители информации многократного использования больше не требуются и передаются за пределы организации, то их содержимое должно быть гарантированно уничтожено;
- в отношении всех уничтожаемых носителей информации должно быть принято соответствующее решение, а также должна быть сделана запись в регистрационном журнале;
- все носители информации следует хранить в надежном, безопасном месте в соответствии с требованиями изготовителей.

Носители информации по окончании использования следует надежно и безопасно утилизировать. Для этого необходимо предусматривать следующие мероприятия:

а) носители, содержащие важную информацию, следует хранить и утилизировать надежно и безопасно (посредством сжигания/измельчения). Если носители планируется

использовать в пределах Колледжа для других задач, то информация на них должна быть уничтожена;
б) перечень объектов, в отношении которых может потребоваться безопасная утилизация:
1) бумажные документы;
2) выводимые отчеты;
3) сменные диски;
4) оптические носители данных (все разновидности, в том числе носители, содержащие программное обеспечение, поставляемое производителями).

XI. БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ

11.1. Электронная почта используется для обмена служебной информацией. Правила использования электронной почты:

- доступ к официальному адресу электронной почты должен быть ограничен согласно настоящему Положению;
- должны выполняться мероприятия в части антивирусной защиты почтовых сообщений;
- пароль доступа в электронной почте хранится у администратора безопасности, смена производится по мере необходимости.

11.2. Пользователи обязаны соблюдать правила обеспечения безопасности при выборе и использовании паролей, должны быть осведомлены о необходимости:
а) сохранения конфиденциальности паролей;
б) запрещения записи паролей на бумаге, если только не обеспечено безопасное их хранение;
в) изменения паролей всякий раз, при наличии любого признака возможной компрометации системы или пароля;
г) выбора качественных паролей с минимальной длиной в девять знаков, которые: легко запомнить; не подвержены легкому угадыванию или вычислению с использованием персональной информации, связанной с владельцем пароля, например, имен, номеров телефонов, дат рождения и т.д.; не содержат последовательных идентичных символов и не состоят из полностью числовых или полностью буквенных групп;
д) изменения паролей через равные интервалы времени или после определенного числа доступов и исключения повторного или цикличного использования старых паролей;
е) изменения временных паролей при первой регистрации в системе;
ж) запрещения включения паролей в автоматизированный процесс регистрации, например, с использованием хранимых макрокоманд или функциональных клавиш;
з) исключения коллективного использования индивидуальных паролей.

XII. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВИЛ ОБРАЩЕНИЯ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

12.1 Требования настоящего Положения обязательны для всех пользователей, обрабатывающих конфиденциальную информацию.

12.2 Нарушения, связанные с выполнением требований руководящих документов по информационной безопасности, применению средств защиты информации и разграничения доступа, использованию технического, информационного и программного обеспечения, по степени их опасности делятся на нарушения первой, второй и третьей категории.

12.2.1. К нарушениям первой категории относятся нарушения, повлёкшие за собой разглашение (утечку) защищаемых сведений, утрату содержащих их машинных носителей информации и машинных документов, уничтожение (искажение) информационного и программного обеспечения, выведение из строя технических средств.

12.2.2. К нарушениям второй категории относятся нарушения, в результате которых возникают предпосылки к разглашению (утечке) защищаемых сведений или утрате содержащих их машинных носителей информации и машинных документов, уничтожению (искажению) информационного и программного обеспечения, выведению из строя технических средств.

12.2.3. Остальные нарушения относятся к нарушениям третьей категории.

12.3. Ответственность за разглашение конфиденциальной информации и утрату носителей информации.

Разглашение конфиденциальной информации — предание огласке этой информации гражданским служащим, допущенным к ней в связи с выполнением функциональных (должностных) обязанностей.

Под утратой носителей конфиденциальной информации (документов, материалов, изделий) понимается выход (в том числе на непродолжительное время) этих носителей из владения гражданского служащего, который в установленном порядке допущен к ним в связи с выполнением функциональных (должностных) обязанностей, в результате чего данные носители стали либо могли стать достоянием посторонних лиц.

За разглашение конфиденциальной информации, утрату носителей конфиденциальной информации и нанесение вследствие этих действий ущерба министерству виновные лица привлекаются к дисциплинарной, материальной, административной или уголовной ответственности.