КОПИЯ №_____

Утверждено решением Правления АО «Медицинский университет Астана» №_17_ от «_25_» _мая_ 2012г.

П О Л О Ж Е Н И Е

ИНТЕГРИРОВАННАЯ СИСТЕМА МЕНЕДЖМЕНТА

ПОЛОЖЕНИЕ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «МЕДИЦИНСКИЙ УНИВЕРСИТЕТ АСТАНА»

ПЛ-МУА-28-12

г.Астана

Содержание

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящее Положение по информационной безопасности (далее - Положение) учитывает современное состояние и ближайшие перспективы развития корпоративной сети передачи данных

(далее- КСПД) АО «Медицинский университет Астана» (далее –Университет), цели, задачи и правовые основы эксплуатации, режимы функционирования, а также анализ угроз безопасности для ее ресурсов.

1.2 Требования Положения распространяются на структурные подразделения Университета, подведомственные им организаций, в которых осуществляется автоматизированная обработка информации, в том числе информации с ограниченным распространением (служебная информация) или персональных данных, а также осуществляющих сопровождение, обслуживание и обеспечение функционирования Университета. Положение распространяется также на другие организации и учреждения, осуществляющих взаимодействие с университетом в качестве поставщиков и потребителей (пользователей) информации и услуг.

1.3 За непосредственную организацию (построение) и обеспечение эффективного функционирования системы защиты информации в Университете отвечают: отдел информационных технологий и отдел правового обеспечения.

1.4 Сотрудники отдела информационных технологий, главный юрисконсульт юридического отдела, начальник финансово экономического управления, начальник управления кадровой работы и правового обеспечения проводит необходимые технические и организационные мероприятия для обеспечения информационной безопасности .

1.5 Проректор по административной и экономической деятельности осуществляет мероприятия по защите корпоративных секретов, обеспечению информационной безопасности и режима секретности в Университете и подведомственных организациях.

1.6 Начальник, главный инженер отдела информационных технологий (далее-ОИТ) осуществляют организацию квалифицированной разработки (совершенствования) системы защиты информации и организационного (административного) обеспечения ее функционирования в Университете.

2 ОСНОВНАЯ ЧАСТЬ

2.1 Цели и задачи

2.1.1 Основной целью, на достижение которой направлены все пункты Положения, является надежное обеспечение информационной безопасности и как следствие недопущение нанесения материального, физического, морального или иного ущерба Университету в результате информационной деятельности.

2.1.2 Указанная цель достигается посредством обеспечения и постоянного поддержания следующего состояния корпоративной сети передачи данных:

- доступность обрабатываемой информации для зарегистрированных пользователей;
- устойчивое функционирование КСПД Университета;
- обеспечения конфиденциальности информации, хранимой, обрабатываемой средствами вычислительной техники (далее - СВТ) и передаваемой по каналам связи;
- целостность и аутентичность информации, хранимой и обрабатываемой информационной системой (далее - ИС) Университета и передаваемой по каналам связи.

2.1.2 Для достижения поставленной цели необходимо решить следующие задачи:

- защита от вмешательства посторонних лиц в процесс функционирования информационных ресурсов Университета;
- разграничение доступа зарегистрированных пользователей к информации, аппаратными, программными и криптографическими средствами защиты, используемыми в ИС;
- регистрация в системных журналах действий пользователей при использовании сетевых ресурсов;
- периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов специалистами информационной безопасности;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее вос-

становление в случае нарушения;

- защита информации от несанкционированной модификации, искажения;
- контроль целостности используемых программных средств, а также защиту системы от внедрения вредоносного программного обеспечения;
- защиту служебной тайны и персональных данных от утечки, несанкционированного разглашения или искажения при ее обработке, хранении и передаче по каналам связи;
- обеспечение авторизации и аутентификации пользователей, участвующих в информационном обмене;
- своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;
- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции;
- создание условий и инструкций для минимизации и локализации нанесенного ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности.
- создание и обеспечения бесперебойной работы электронного документооборота.
- постоянный аудит политики безопасности внутренним аудитом не реже 1 раза в полгода и внешним аудитом раз в год.

2.2 Пользователи информационных систем

2.2.1 К пользователям информационных систем относятся:

- сотрудники – служащие, осуществляющие свою деятельность в Университете и обладающие основными правами и обязанностями в соответствии с законодательством Республики Казахстан;
- вспомогательный персонал - обслуживающий и технический персонал подведомственных и сторонних организаций, осуществляющих взаимодействие с Университетом в качестве поставщиков и потребителей (пользователей) информации и услуг. В том числе:
- администраторы корпоративной сети передачи данных, ответственные за сопровождение телекоммуникационного оборудования;
- системные администраторы, ответственные за сопровождение общего и прикладного программного обеспечения;
- разработчики прикладного программного обеспечения;
- инженеры-системотехники, технические специалисты;
- специалисты по информационной безопасности (специальных средств защиты) и др.;
- потребители услуг – лица и/или сторонние организации, использующие информационные ресурсы Университета.
- студенты, интерны, резиденты, магистранты, магистранты MBA и докторанты.

2.3 Модели потенциальных нарушителей

2.3.1 В качестве потенциального нарушителя информационной безопасности рассматривается лицо или группа лиц, состоящих или не состоящих в сговоре, которые в результате умышленных или неумышленных действий могут реализовать разнообразные угрозы информационной безопасности, направленные на информационные ресурсы и нанести моральный и/или материальный ущерб интересам Университета.

2.3.2 Потенциальных нарушителей можно разделить на внутренних и внешних. Внутренними нарушителями могут быть практически все сотрудники Университета и вспомогательный персонал. Их можно разделить на следующие группы в зависимости от уровня доступа к информационным ресурсам корпоративной сети:

- лица, имеющие доступ к информации, составляющую персонифицированные и служеб-

ную тайну;

- лица, имеющие доступ к информации, составляющую служебную тайну и задействованные в технологии обработки, передачи и хранения информации;
- лица, не имеющие доступ к информации, составляющую персонифицированные секрет и служебную тайну, но задействованные в технологии обработки, передачи и хранения информации;
- обслуживающий персонал.

2.3.3 Чтобы построить реальную модель потенциального нарушителя необходимо принять во внимание виды выявленных нарушений, устремлений различных лиц и организаций, а также имеющиеся в Университете интересы других юридических лиц.

2.3.4 В Университете возможны следующие виды нарушений:

- несанкционированное использование программ, могущих негативно повлиять на работоспособность КСПД Университета, снизить ее производительность, а также мешающих корректной работе КСПД (сканеры сети, интенсивный широковещательный трафик и т.п.);
- использование прав локальных администраторов на рабочих станциях пользователей, что дает возможность установки обычному пользователю неограниченного количества программ.
- нарушения сотрудниками вследствие незнания требований информационной безопасности и нормативных правовых актов Университета.

2.3.5 Потенциальные внешние нарушители:

- бывшие сотрудники и вспомогательный персонал;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности (энерго-, водо-, теплоснабжения и т.п.);
- посетители (приглашенные представители организаций, граждане);
- представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.

2.4 Назначение, нормативная и правовая база Положения

2.4.1 Настоящее Положение детализирует требования по решению вопроса обеспечения информационной безопасности в единой информационной телекоммуникационной среде, объединяющей ИС Университета.

2.4.2 Положение информационной безопасности Университета является методологической базой:

- выработки и совершенствования комплекса согласованных нормативных, правовых, технологических и организационных мер, направленных на защиту информации;
- обеспечения информационной безопасности;
- координации деятельности территориальных и структурных подразделений при проведении работ по соблюдению требований обеспечения информационной безопасности.

2.4.3 Научно-методической основой Положения является системный подход, предполагающий проведение исследований, разработку системы защиты информации в процессе ее обработки в информационных системах с учетом всех факторов, оказывающих на нее влияние и комплексного применения различных мер и средств защиты.

2.4.4 Основные требования Положения базируются на качественном осмыслении вопросов информационной безопасности, не концентрируя внимание на экономическом (количественном) анализе рисков и обосновании необходимых затрат на защиту информации.

2.4.5 Нормативной и правовой базой Положения являются: Указ Президента Республики Казахстан от 14 ноября 2011 года № 174 «О Концепции информационной безопасности Республики Казахстан до 2016 года»,Законы Республики Казахстан «О национальной безопасности Республики Казахстан», «О государственных секретах», «О противодействии терроризму», «Об электронном документе и электронной цифровой подписи», «Об информатизации», «О техническом регулировании», «О лицензировании», «О средствах массовой информации», «О связи», Программа по развитию информационных и коммуникационных технологий в Республике Казахстан на 2010 - 2014 годы, утвержденная постановлением Правительства Республики Казахстан от 29 сентября

2010 года № 983 и иные акты Республики Казахстан и Университета, регламентирующие вопросы обеспечения информационной безопасности.

2.5 Средства и меры защиты информации

2.5.1 Средства и меры защиты от утечки информации по каналам связи

2.5.1.1 Защита информации от утечки по каналам их передачи из/в Университете достигается, путем применения комплексных программных, технических средств защиты и организационных мер.

2.5.1.2 Для выявления утечки информации необходим систематический контроль возможности образования каналов утечки и оценки их опасности в пределах контролируемой зоны. Закрытие и локализация каналов утечки обеспечивается организационно-техническими мерами.

2.5.1.3 В соответствии с используемыми каналами передачи электронной информации в Университете предусматриваются необходимые технические средства защиты (межсетевой экран и т.п.). Организуется система регистрации, передачи, приема и хранения носителей информации, предусматриваются надлежащие способы их уничтожения, с целью исключения возможности восстановления записанных на них сведений. Технические каналы передачи информации оснащаются соответствующими средствами защиты. Создается надежная система охраны зданий и сооружений, организуется пропускной режим в помещения Университета для предотвращения доступа посторонних лиц.

2.5.2 Меры по защите средств вычислительной техники

2.5.2.1 Защита СВТ от несанкционированного доступа в Университете строится по нескольким направлениям. Создаются автоматизированные средства регистрации пользователей, система блокирования учетных записей и оповещения сотрудников об угрозе или проникновении в СВТ, согласно Правилам регистрации пользователей в корпоративной сети передачи данных (ПР-МУА-08) и Плану по обеспечению непрерывной деятельности информационных систем Университета.

2.5.2.2 Определяются организационные меры по предотвращению несанкционорованного доступа (далее - НСД), в том числе в случае утраты/компрометации паролей и выхода из строя СВТ, согласно Политике организации парольной защиты (ПР-МУА-09).

2.5.2.3 В случае обнаружения фактов НСД к информационным ресурсам и системам Университета или выявления потенциальной угрозы информационной безопасности сотрудники ОИТ немедленно информирует руководителя, курирующего вопросы связи.

2.5.3 Защита от аппаратных спецвложений, нелегального внедрения и использования неучтенных программ

2.5.3.1 Для предотвращения аппаратных спецвложений используются меры физической защиты, устанавливаются средства видеонаблюдения и контроля доступа в серверное помещение Университета.

2.5.3.2 Для защиты от нелегального внедрения и использования неучтенных программ в Университете кроме мероприятий, включающих физическую защиту, проведение аудита обращения к СВТ и мониторинг системных журналов, устанавливается базовый комплекс программного обеспечения, который необходимо устанавливать на рабочие станции пользователей. В базовый комплекс включается лицензионное программное обеспечение (далее - ПО), необходимое для обеспечения работоспособности СВТ, согласно Правила пользователя по эксплуатации средств вычислительной техники и программного обеспечения Университета (ПР-МУА-10).

2.5.3.3 Использование для производственных целей прикладного ПО, внешних носителей информации не входящего в состав базового комплекса санкционируется ОИТ по согласованию с руководителем, курирующим вопросы связи, информатизации и телекоммуникаций.

2.5.4 Защита от несанкционированного копирования данных пользователем

2.5.4.1 Служебная и иная защищаемая информация, обрабатываемая и хранящаяся в информационных системах Университета подлежит копированию и передаче третьему лицу только с разрешения ректора по согласованию с руководителем, курирующим вопросы связи, информатизации и телекоммуникаций согласно Правила пользователя по эксплуатации средств вычислительной техники и программного обеспечения Университета (ПР-МУА-10).

2.5.4.2 За копирование и передачу служебной и иной защищаемой информации третьему лицу без разрешения, пользователь привлекается к дисциплинарной ответственности.*

2.5.6 Защита информации, отображаемой на мониторе средств вычислительной техники

2.5.6.1 Защита достигается путем ограничения физического доступа к средствам отображения информации, исключения наблюдения за отображаемой информацией посторонними лицами, согласно Правила пользователя по эксплуатации средств вычислительной техники и программного обеспечения Университета (ПР-МУА-10).

2.5.7 Защита от действий вредоносных программ, вирусов

2.5.7.1 В целях защиты от действий вредоносных программ и вирусов в Университете используются «иммуностойкие» программные средства, защищенные от возможности несанкционированной модификации, специальные программы-анализаторы, осуществляющие постоянный контроль за возникновением отклонений в деятельности прикладных программных продуктов, периодическую проверку наличия возможных следов вирусной активности, а также входной контроль новых программ перед их использованием.

2.5.7.2 Организационные меры изложены в Правилах по антивирусной защите компьютеров и серверов (ПР-МУА-11), Правила подключения и использования ресурсов сети Интернет (ПР-МУА-12) и Правил по работе с электронной почтой (ПР-МУА-13).

2.5.8 Защита от хищения носителей информации

2.5.8.1 В Университете устанавливается определенный порядок хранения и использования носителей информации, согласно Правила пользователя по эксплуатации средств вычислительной техники и программного обеспечения Университета (ПР-МУА-10).

2.5.8.2 При передаче носителя цифровой информации для повторного использования за пределами Университета проводится его очистка с целью исключения несанкционированного разглашения защищаемых сведений.

2.5.9 Защита информации в средствах вычислительной техники

2.5.9.1 За каждым СВТ закрепляется сотрудник Университета. На СВТ используется система авторизации и/или аутентификации сотрудника, работающего на нем. Передача СВТ в пользование другому сотруднику осуществляется с разрешения руководителя подразделения. Принимаются необходимые программно-технические средства защиты информации, обрабатываемой на СВТ.

2.5.10 Защита от умышленной модификации информации

*

2.5.10.1 Кроме средств регламентированного доступа к СВТ защита информации от модификации осуществляется программными, техническими и организационными мерами. Для своевременного выявления и обнаружения указанных посягательств используются журналы действий операторов и администраторов.

2.5.11 Защита от ошибок программно-аппаратных средств

2.5.11.1 С целью проверки работоспособности, перед вводом в эксплуатацию программные продукты и аппаратные средства подлежат тестированию в условиях максимально приближенных к реальным. Не пригодные к использованию программное обеспечение и аппаратные средства в эксплуатацию не принимаются**.**

2.5.12 Защита от некомпетентного использования, настройки или неправомерного отключения средств защиты

2.5.12.1 Средства защиты КСПД вводятся в эксплуатацию, сопровождаются и используются в соответствии с установленным регламентом. Контроль за этим процессом осуществляет ОИТ, обеспечивающий информационную безопасность.

2.5.12.2 Сопровождением серверов Университета занимается ОИТ.

2.5.12.3 При нарушении регламента причастные сотрудники привлекаются к ответственности в соответствии с законодательством Республики Казахстан.

2.5.13 Защита средств вычислительной техники от нарушений работоспособности или разрушения аппаратных, программных, информационных ресурсов

2.5.13.1 В результате возникновения аварий, стихийных бедствий и иных внештатных ситуаций могут возникнуть нарушения работоспособности СВТ, а также разрушение аппаратных, программных, информационных ресурсов в Университете. На такие случаи предусматриваются соответствующие меры защиты, согласно Плану по обеспечению непрерывной деятельности информационных систем Университета.

2.5.14 Защита от ввода ошибочных данных

2.5.14.1 Данные, вводимые в приложениях проверяются программными и техническими средствами, чтобы гарантировать их правильность и соответствующее использование. Ввод информации осуществляется уполномоченным на это персоналом.

2.5.15 Меры по защите коммуникационных средств

2.5.15.1 Основные и резервные телекоммуникационные сервисы соответствующим образом отделяются друг от друга, чтобы не подвергаться одним и тем же угрозам, согласно Плану по обеспечению непрерывной деятельности информационных систем Университета**,** Правилам по резервному копированию информации (ПР-МУА-14).

2.5.16 Защита от незаконного подключения к корпоративной сети передачи данных

2.5.16.1 Защита коммуникаций от незаконного подключения кроме средств санкционированного электронного и физического доступа, осуществляется программными, техническими средствами и организационными мерами. Проводятся необходимые мероприятия для своевременного выявления, предупреждения и пресечения неправомерных действий лиц по получению доступа к коммуникациям. За незаконное подключение и попытка незаконного подключения к линиям связи

и сетевому оборудованию лица несут ответственность в соответствии с законодательством Республики Казахстан.

2.5.17 Защита от повреждения, некорректного функционирования, частичного или полного отказа сетевого оборудования

2.5.17.1 Повреждение, некорректное функционирование, частичный, полный отказ сетевого оборудования Университета может быть, в первую очередь, в результате возникновения аварий, стихийных бедствий и иных внештатных ситуаций.

2.5.17.2 В Университете принимаются меры, связанные с внедрением средств защиты, которые будут использоваться в случае стихийных бедствий (пожаров, наводнений и землетрясений), а также в различных нештатных ситуациях.

2.5.17.3 Разрабатывается План обеспечения непрерывной работы и восстановления, согласно Плану по обеспечению непрерывной деятельности информационных систем Университета.

2.5.18 Защита от неправомерного включения, выключения оборудования

2.5.18.1 Сетевое оборудование КСПД Университета вводится в эксплуатацию, сопровождается и используется в соответствии с установленным регламентом. Включение и отключение оборудования производится уполномоченным техническим персоналом, по согласованию с ОИТ и руководителем, курирующим вопросы связи, информатизации и телекоммуникации.

2.5.19 Защита от неправомерной модификации передаваемых данных, технической и служебной информации

2.5.19.1 Кроме средств санкционированного доступа к коммуникационным средствам и сетевому оборудованию, защита передаваемых данных от модификации осуществляется программно-техническими и организационными мерами.

2.5.20 Меры по защите системы архивирования

2.5.20.1 Определяется порядок резервного копирования, хранения и восстановления программных продуктов и информационных систем. Хранилище резервных копий размещается в помещении специально оборудованным согласно Плану по обеспечению непрерывной деятельности информационных систем. Обеспечивается санкционированный доступ к хранилищу резервных копий для своевременного восстановления информации и информационных систем в случае сбоя, аварии и иных нештатных ситуациях.

2.5.20.2 Разрабатывается План по обеспечению непрерывной деятельности информационных систем, в котором также определяются меры по защите архивов на случай возникновения аварий, стихийных бедствий и других нештатных ситуаций, согласно Правилам по резервному копированию информации (ПР-МУА-14).

2.5.21 Прочие меры по защите информации

2.5.21.1 Следует принять исчерпывающие меры защиты информации на всех запоминающихся устройствах при передаче СВТ на ремонт сторонним организациям.

2.5.22 Пересмотр Положения информационной безопасности

2.5.22.1 Соблюдение требований Положения информационной безопасности обязательно для всех пользователей информационных систем Университета. Проведение планового аудита информационной безопасности является одним из основных методов проверки эффективности мер по защите информации. Результаты аудита могут служить основанием для пересмотра некоторых пунктов Положения и внесения в них необходимых корректировок.

2.5.22.2 Аудит информационной безопасности Университета целесообразно проводить ежегодно, по итогам которого ОИТ и главным специалистом по информационной безопасности должен проводиться пересмотр Положения на предмет соответствия предъявляемым требованиям, в случае возникновения необходимости вносить изменения и дополнения.

3 ПЕРЕСМОТР, ВНЕСЕНИЕ ИЗМЕНЕНИЙ, ХРАНЕНИЕ И РАССЫЛКА

3.1 Пересмотр, внесение изменений, хранение и рассылка настоящего положения Университета осуществляются в соответствии с требованиями стандарта Университета «Управление документацией» (СУ-МУА-02).

3.2 Оригинал настоящего положения Университета регистрируется и хранится в ОМК и СП.

3.3 Сканированная версия настоящего положения Университета размещается на серверном компьютере Университета в папке общего доступа.

3.4 Копии настоящего Положения рассылаются всем структурным подразделениям Университета.

Начальник отдела
информационных технологий **А. Маралов**

Лист согласования

№ п/п	Должность	Ф.И.О.	Дата согласования	Подпись
1	Проректор по образовательной деятельности	Жаксылыкова Г.А.	18.05.2012г	
2	Проректор по научной и клинической деятельности	Галицкий Ф.А.	21.05.2012.	
3	Проректор по воспитательной деятельности и связям с общественностью	Хайрли Г.З.	22.05.12	
4	Проректор по административной и экономической деятельности	Нуржаубай М.О.	19.05.12	
5	Начальник управления кадровой работы и правового обеспечения	Сыздыков Б.А.	16.05.2012г	
6	Начальник отдела менеджмента качества и стратегического планирования	Жумашева З.С.	15.05.12г	
7	Начальник юридического отдела	Устинович О.С.	14.05.2012.	

Лист регистраций изменений

№ п/п	Номера листов (страниц)				Всего листов	Номер раздела, подраздела, пункта стандарта, к которому относятся изменения	Подпись лица, внесшего изменения	Дата внесения изменения
	Измененных	Замененных	Новых	Аннулированных				

Лист ознакомления

№ п/п	Должность	Ф.И.О.	Дата согласования	Подпись