«Рассмотрено»
*На заседании Ученого Совета международного медицинского университета протокол № _4_*

«_24_»__май__ 2021 г.

«Утверждаю»
Ректор Ошского международного медицинского университета доцент Кенешбаев Б.К.

«_24_»__май__ 2021 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОШСКОГО МЕЖДУНАРОДНОГО МЕДИЦИНСКОГО УНИВЕРСИТЕТА

Общие положения

1. Концептуальная схема информационной безопасности Ошского международного медицинского университета направлена на защиту его информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Наибольшими возможностями для нанесения ущерба университету обладает ее собственный персонал. Внешний злоумышленник, скорее всего, может иметь сообщника внутри университета.

2. Политика информационной безопасности университета пре следует цель по обеспечению следующих прав граждан:

Каждый имеет право на неприкосновенность частной жизни, на защиту чести и достоинства

Каждый имеет право на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных, электронных и иных сообщений. Ограничение этих прав допускается только в соответствии с законом и исключительно на основании судебного акта.

Не допускается сбор, хранение, использование и распространение конфиденциальной информации, информации о частной жизни человека без его согласия, кроме случаев, установленных законом.

Каждому гарантируется защита, в том числе судебная, от неправомерного сбора, хранения, распространения конфиденциальной информации и информации о частной жизни человека, а также гарантируется право на возмещение материального и морального вреда, причиненного неправомерными действиями.

3. Информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют **врачебную тайну.** Гражданину должна быть подтверждена гарантия конфиденциальности передаваемых им сведений. Не допускается разглашение сведений, составляющих врачебную тайну, лицами, которым они стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей.

4. **Государственные секреты** - информация, хранящаяся и перемещаемая любыми видами носителей, затрагивающая обороноспособность, безопасность, экономические, научно-технические и политические интересы Кыргызской Республики, подконтрольная государству и ограничиваемая специальными перечнями и правилами, разработанными в соответствии нормативными правовыми актами Кыргызской Республики.

5. **Информация персонального характера (персональные данные)** - зафиксированная информация на материальном носителе о конкретном человеке, отождествленная с конкретным человеком или которая может быть отождествлена с конкретным человеком, позволяющаяидентифицировать этого человека прямо или косвенно, посредством ссылки на один или не- сколько факторов, специфичных для его биологической, экономической, культурной, гражданской или социальной идентичности.

К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном положении, финансовом положении, состоянии здоровья и прочее.

6. **Кибербезопасность** - сохранение свойств целостности (которая может включать аутентичность и отказоустойчивость), доступности и конфиденциальности информации в объектах информационной инфраструктуры, обеспечиваемое за счет использования совокупности средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками и страхования, профессиональной подготовки, практического опыта и технологий;

7. Под **коммерческой тайной** понимаются не являющиеся государственной тайной сведения, связанные с производством, технологией, управлением, финансовой и другой деятельностью университета, разглашение которых может нанести ущерб его интересам.

8. **Системное программное обеспечение** - совокупность программного обеспечения для обеспечения работы вычислительного оборудования;

9. **Средство криптографической защиты информации** - программное обеспечение или аппаратно-программный комплекс, реализующий алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами шифрования;

10. **Третьи лица** - все лица, кроме субъекта персональных данных, ректора, оператора (специалиста) обработчика персональных данных.

11. Настоящая Политика информационной безопасности (далее-политика) разработан с учетом следующих международных стандартов и документов:

- Статья 29, Конституции Кыргызской Республики;
- законы Кыргызской Республики «Об информации персонального характера», «Об электронной подписи», «Об электронном управлении», «О коммерческой тайне», «О защите государственных секретов Кыргызской Республики», «Об охране здоровья граждан в Кыргызской Республике» и «О наружном видеонаблюдении»;
- Требования к защите информации, содержащейся в базах данных государственных информационных систем, утвержденный Постановлением Правительства КР от 21 ноября 2017 года

12. Направление информационной безопасности создано в **отделе цифровизации и информационных технологий (далее - ОЦИТ)** соследующими задачами и функциями, определяемым Законом Кыргызской Республики "Об информации персонального характера":

- разработка и совершенствование нормативно-правовой базы обеспечения информационной безопасности;
- выявление, оценка и прогнозирование угроз информационной безопасности;
- организация технической защиты информации, участие в проектировании систем защиты;
- проведение периодического контроля состояния информационной безопасности, учет и - анализ результатов с выработкой решений по устранению уязвимостей и нарушений;
- контроль за использованием закрытых каналов связи и ключей с цифровыми подписями;
- организация плановых проверок режима защиты, и разработка соответствующей документации.анализ результатов, расследование нарушений;
- разработка и осуществление мероприятии по защите персональных данных;

- организация взаимодействия со всеми структурами, участвующими в их обработке, выполнение требований законодательства к информационным системам персональных данных, контроль действий операторов, отвечающих за их обработку.

Организационно-правовой статус сотрудников информационной безопасности: сотрудники имеют право беспрепятственного доступа во все помещения, где установлены технические средства с Информационными системами, право требовать от руководства подразделений и администраторов Информационной системы прекращения автоматизированней обработки информации, персональных данных, при наличии непосредственной угрозы защищаемой информации;имеют право получать от пользователей и администраторов необходимую информацию го вопросам применения информационных технологий, в части касающейся вопросов информационной безопасности;

руководитель Службы внутреннего аудита, и комплайнса (далее - комплайнс) имеет право проводить аудит действующих и вновь внедряемых Информационных систем, программного обеспечения, на предмет реализации требований защиты и обработки информации, соответствию требований законодательства, запрещать их эксплуатацию, если не отвечают требованиям или продолжение эксплуатации может привести к серьезным последствиям в случае реализации значимых угроз безопасности;

- сотрудники имеют право контролировать исполнение утвержденных нормативных и организационно-распорядительных документов, касающихся вопросов информационной безопасности.

Область действия

14. Требования настоящей Политики распространяются на всех сотрудников Университета (штатных, временных, работающих по контракту и т.п). Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах с контрагентами.

Порядок доступа пользователей к информационным системам, в которых обрабатывается информация персонального характера

15. Управление доступом к информационным системам реализовано с помощью штатных средств (операционных систем MS Windows) в целях идентификации и проверки подлинности субъектов доступа при входе в Информационную систему, а также для их регистрации входа (выхода) в систему (из системы).

16. Требование идентификации и аутентификации при входе в информационную систему определяется в законах Кыргызской Республики "Об информации персонального характера", Об электронной подписи", "Об электронном управлении".

17. В составе информационных систем персональных данных используются сертифицированные или разрешенные к применению средства защиты информации от несанкционированного доступа.

Все действий пользователей информационной системы регистрируются в журналах соответствий системного и прикладного программного обеспечения. Данные электронные журналы доступны для чтения, анализа и резервного копирования только администратору соответствующего программного обеспечения, который несет персональную ответственность за полноту и точность отражения в журнале имевших место событий. Он же, по запросу, выборочно передаетданные из журналов сотруднику ОЦИТ

При необходимости комплайнсу предоставляется административный доступ к серверам базам данных по служебной записке на имя директора ОЦИТ.

Запрещается доступ супер пользователей к серверам и базам данных под единой или предопределенной учетной записью.

Любой доступ к базам данных информационных систем без фиксации в соответствующих

журналах или логин-файлах запрещен. В случае увольнения сотрудника, имеющего права.пользователя, пароли доступа к серверам и базам данных меняются в тот же день.

Сетевая безопасность

22. Доступ изИнтернет в сеть университета:

- доступ во внутреннюю сеть осуществляется только через настроенный межсетевой экран;
- не допускается удаленный доступ в локальную сеть с использованием не персонифицированных, групповых и анонимных учетных записей;
- не допускается использование программ удаленного администрирования.

23. При администрировании удаленного доступа к ресурсам корпоративной сети Университета предъявляются следующие требования:

- удаленный доступ пользователей к ресурсам и сервисам компьютерной сети университета обеспечивается на основе зарегистрированных персональных учетных записей.

24. В целях обеспечения безопасности и нормального функционирования компьютерных сетей запрещается:

- самовольно подключать компьютерное оборудование (беспроводные точки доступа, маршрутизаторы, компьютеры и др.) к сети университета и присваивать ему сетевое имя и адрес без согласования с ОЦИТ;
- перемещать компьютеры между сетевыми розетками и другими коммуникационными устройствами без согласования с ОЦИТ;
- использовать информационные ресурсы университета для сетевых игр, распространения коммерческой рекламы;

26. Для анализа защищенности Информационных систем комплайнсом применяются специализированные программно-аппаратные средства - сканеры безопасности.

Функционал подсистемы реализуется программными и программно-аппаратными средствами.на межсетевых экранах. Администратор сети ведет протоколирование и регулярныймониторинг доступа, контролирует содержание трафика с использованием специализированного программного обеспечения, проводит анализ логин-файлов.

31. Приобретение и установка средств и систем защиты информационных систем осуществляются по согласованию с комплайнсом. Сеть информационных систем персональных данных выделена в отдельный сегмент и защищена межсетевым экраном.

Ограничение прав доступа к информационным системам и системам хранения данных, защита от несанкционированного доступа

42. Для доступа к информационным системам университета сотрудник должен ввести логин -пароль.

43. В целях защиты информации организационно и технически разделяются подразделения университета,имеющие доступ и работающие с различной информацией (в разрезе ее конфиденциальности и смысловой направленности).

44. Данная задача решается с использованием возможностей конкретных информационных систем, где в целях обеспечения защиты данных и права пользователей ограничивается набором прав и ролей. В случае обработки информации конфиденциального характера права назначаются администратором информационных

45. Администратором информационных систем проводится анализ журналов доступа к ресурсам информационных систем, фиксируются попытки несанкционированного доступа, о которых докладывается комплансу.

47. Не допускается использование учетных записей уволенных сотрудников.