Приложение 1
Для служебного пользования
Коммерческая тайна

Утверждено приказом ректора
Ошского государственного университета
от «25» 02 2020 г. № 001/НПА

Политика информационной безопасности Ошского государственного университета

Общие положения

1. Концептуальная схема информационной безопасности Ошского государственного 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 Ошского государственного университета преследует 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, позволяющая

идентифицировать этого человека прямо или косвенно, посредством ссылки на один или несколько 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»;
- ISO/IEC 15408-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий;
- ISO/IEC 12207-99 Информационная технология. Процессы жизненного цикла программных средств;
- ISO/IEC TO 15271-2002 Информационная технология. Руководство по применению ISO/IEC 12207 (Процессы жизненного цикла программных средств);
- ISO/IEC 17799-2000 Информационная технология. Кодекс установившейся практики для менеджмента информационной безопасностью;
- ISO/IEC 13335 Информационная технология. Методы и средства обеспечения безопасности. Руководство для менеджмента безопасностью информационных технологий;
- ISO/IEC 18044 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентами информационной безопасности;
- ISO/IEC 15288-2002 Информационная технология. Менеджмент на жизненном цикле. Процессы жизненного цикла систем;
- ISO/IEC 15504-98 Информационная технология. Оценка процессов программных средств;
- ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования";
- ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки ЭЦП";

- ГОСТ Р 34.11-2012 "Информационная технология. Криптографическая защита информации. Функция хэширования";
- ГОСТ Р 34.12-2015 "Информационная технология. Криптографическая защита информации. Блочные шифры";
- ГОСТ Р 34.13-2015 "Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров";
- ГОСТ 34.310-2004 "Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма";
- ГОСТ 34.311-2004 "Информационная технология. Криптографическая защита информации. Функция хеширования";
- RFC 3647 Certificate Policy and Certification Practices Framework (серии международных стандартов IETF);
- RFC 5280 из серии международных стандартов IETF (регулирующий требования к структуре регистрационных свидетельств и списку отозванных регистрационных свидетельств);
- RFC 3280 из серии международных стандартов IETF (Certificate and Certificate Revocation List (CRL) Profile);
- RFC 1422 из серии международных стандартов IETF;
- RFC 3029 Data Validation and Certification Server Protocols серии международных стандартов IETF;
- Серия стандартов ITU-T X.500 версии 3 (ITU-T X.509, ITU-T X.501);
- RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP);
- RFC 5816 - update of RFC 3161;
- RFC 6960 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP;
- RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2;
- RFC 4346 - The Transport Layer Security (TLS) Protocol Version 1.1;
- (RFC 4033, RFC 4034, RFC 4035) DNSSEC;
- Associated Signature Containers (ASiC) (ETSI EN 319 162-1 V1.1.1 (2016-04);
- XML Advanced Electronic Signatures ETSI EN 319 132-1 V1.1.0;
- RFC 4253 SSH;
- RFC 3447 - (PKCS) #1: RSA Cryptography Specifications Version 2.1;
- ISO/IEC 18033-3:2005 для AES;
- ISO/IES 10118-3 для SHA-1, SHA-256, SHA-384, SHA-512;
- RFC 2104 HMAC (для имитовставок);
- ISO/IEC 9797-1 CMAC, CBC-MAC (для имитовставок);
- ISO/IEC 14888-3:2016.
- Требования к защите информации, содержащейся в базах данных государственных информационных систем, утвержденный Постановлением Правительства КР от 21 ноября 2017 года № 762

12. Направление информационной безопасности создано в **департаменте (отделе) информационных технологий и технического обслуживания компьютеров (далее – ОИТТОК)** со следующими 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 мероприятий 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.

13. 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 автоматизированной обработки информации, персональных данных, при наличии непосредственной угрозы защищаемой информации;
- имеют право получать от пользователей и администраторов необходимую информацию по вопросам применения информационных технологий, в части касающейся вопросов информационной безопасности;
- руководитель Службы внутреннего аудита, риск-менеджмента 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 Server, Linux и используемых ими СУБД) в целях идентификации и проверки подлинности субъектов доступа при входе в Информационную систему, а так же 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.

18. Все действий пользователей информационной системы регистрируются в журналах событий 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 передает данные из журналов сотруднику ОИТТОК.

19. При необходимости комплайнсу предоставляется административный доступ к серверам и базам данных по служебной записке на имя директора ОИТТОК. Запрещается доступ суперпользователей к серверам и базам данных под единой или предопределенной учетной записью.

20. Повышение привилегий администратором для ранее существовавших учетных записей или создание новых административных групп согласовывается с комплайнсом.

21. Любой доступ к базам данных информационных систем без фиксации в соответствующих журналах или лог-файлах запрещен. В случае увольнения сотрудника, имеющего права суперпользователя, пароли доступа к серверам и базам данных меняются в тот же день.

Сетевая безопасность

22. Доступ из Интернет в сеть университета:

- доступ во внутреннюю сеть осуществляется только через настроенный межсетевой экран;
- доступ из вне периметра сети разрешен только по распоряжению директора ОИТТОК с согласованием у комплайнс, по определенному порту и на определенное время;
- не допускается удаленный доступ в локальную сеть с использованием не персонифицированных, групповых и анонимных учетных записей;
- не допускается использование программ удаленного администрирования типа TeamViewer. Как исключение, по согласованию с комплайнс возможно подключение для удаленной настройки программного обеспечения на ограниченное время.
- Настройка и конфигурация средств обнаружения вторжений, межсетевых экранов должны обеспечивать оперативное обнаружение несанкционированного доступа к ресурсам сети для принятия мер блокирования проникновения нейтрализации последствий.

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, с использованием технологии VPN, других протоколов шифрования;
- доступ предоставляется сроком на 3 месяца, при необходимости продлевается с разрешения директора ОИТТОК;
- делается соответствующая запись в Журнале учета предоставления удаленного доступа;
- список сотрудников, которым предоставлен удаленный доступ поддерживается в актуальном состоянии и передается в комплайнс по запросу.

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 ОИТТОК;
- перемещать компьютеры между сетевыми розетками и другими коммуникационными устройствами без согласования с ОИТТОК;
- использовать информационные ресурсы университета для сетевых игр, распространения коммерческой рекламы; организации СПАМа.
- сканировать узлы сети неуполномоченными на то сотрудникам.

25. В Университете используется система межсетевого экранирования, которая реализует функции фиксации во внутренних журналах информации о проходящем IP-трафике, фильтрацию пакетов служебных протоколов, блокирования доступа не идентифицированного объекта.

26. Для анализа защищенности Информационных систем комплайнсом применяются специализированные программно-аппаратные средства – сканеры безопасности. Проводится выявление и анализ уязвимостей и несоответствия в настройках операционной системы, программного обеспечения, системы управления базами данных, сетевого оборудования. Выявленные уязвимости протоколируются и передаются в ОИТТОК для устранения в установленные сроки. Запрещается использовать программное обеспечение, снятое с поддержки, имеющее уязвимости, с просроченными сертификатами.

27. Подсистема обнаружения вторжений, обеспечивает выявление сетевых атак на элементы информационных систем подключенные к сетям общего пользования и (или) международного обмена.

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

29. На межсетевом экране заводится лог-файл, куда записываются все обращения к ресурсам (попытки создания соединений). Доступ к лог-файлам имеют администратор сети и комплайнс.

30. Анализ лог-файлов проводится с применением соответствующего программного обеспечения (анализатор логов) комплайнсом. Комплайнс должен иметь независимый доступ к элементам системы защиты для контроля настроек конфигураций, просмотра системных журналов.

31. Доступ из одного сегмента сети в другой ограничивается и разделяется маршрутизаторами. Настройкой маршрутизаторов занимается сектор сетевого и системного администрирования.

32. 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.

Локальная безопасность

33. Исходя из Требования к защите информации, содержащейся в базах данных государственных информационных систем, утвержденный Постановлением Правительства КР от 21 ноября 2017 года № 762, антивирусная защита предназначена для обеспечения антивирусной защиты серверов и автоматизированном рабочем месте пользователей Университета.

34. На каждом работающем компьютере, или сервере при вводе в эксплуатацию или после переустановки операционной системы сотрудниками ОИТТОК в обязательном порядке устанавливается и активируется антивирусная программа. Установка средств антивирусного контроля (в том числе настройка параметров средств антивирусного контроля) на автоматизированном рабочем месте, серверах, осуществляется специалистами структурных подразделений и ОИТТОК в соответствии с руководствами по применению конкретных антивирусных средств. Отключение или не обновление антивирусных средств не допускается. Установка и обновление антивирусных средств в университет контролируется централизованно ответственным сотрудником ОИТТОК.

35. Не допускается присутствие и использование в электронно-вычислительной машине и автоматизированной информационной системе программного обеспечения и данных, не связанных с выполнением конкретных функций в бизнес-процессах университета. Устанавливаемое или изменяемое программное обеспечение должно быть предварительно проверено на отсутствие вирусов. После установки или изменения программного обеспечения должна быть выполнена антивирусная проверка.

36. При обнаружении компьютерного вируса необходимо приостановить работу, проинформировать руководство и организовать устранение последствий вирусной атаки.

37. Отключение или не обновление антивирусных средств не допускается. Установка и обновление антивирусных средств в университете должны контролироваться комплайнсом.

38. Ответственность за выполнение требований инструкции по антивирусной защите должна быть возложена на специалиста ОИТТОК, а обязанности по выполнению мер антивирусной защиты должны быть возложены на каждого сотрудника университета, имеющего доступ к электронно-вычислительной машине и/или автоматизированной информационной системе.

Уровни безопасности средств криптографической защиты информации

39. В зависимости от криптографической стойкости для средств криптографической защиты информации устанавливаются четыре уровня безопасности:

первый: средства криптографической защиты информации первого уровня безопасности предназначены для защиты информации, вред от разглашения которой или нарушения конфиденциальности, целостности, доступности информации, защищенной с использованием одного и того же средства криптографической защиты информации (одних и тех же средств криптографической защиты информации) не может быть причинен (не влечет негативных последствий в социальной, политической, международной, экономической, финансовой или иных областях деятельности) (коэффициент 0);

второй: средства криптографической защиты информации второго уровня безопасности предназначены для защиты информации, вред от изменения которой или конфиденциальности, целостности, доступности информации, защищенной с использованием одного и того же средства криптографической защиты информации (одних и тех же средств криптографической защиты информации) незначителен - менее 1000 расчетных показателей (влечет незначительные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности), легко компенсируем оператором информационной системы и/или обладателем информации, которые могут выполнять возложенные на них функции с недостаточной эффективностью или выполнение функций возможно только с привлечением дополнительных сил и средств (коэффициент 1);

третий: средства криптографической защиты информации третьего уровня безопасности предназначены для защиты информации, вред от изменения которой или конфиденциальности, целостности, доступности информации, защищенной с использованием одного и того же средства криптографической защиты информации (одних и тех же средств криптографической защиты информации) значителен - от 1000 до 5000 расчетных показателей (влечет умеренные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности), который может быть компенсирован оператором информационной системы и/или обладателем информации, которые могут выполнять хотя бы одну из возложенных на них функций (коэффициент 2);

четвертый: средства криптографической защиты информации четвертого уровня безопасности предназначены для защиты информации, вред от изменения которой или конфиденциальности, целостности, доступности информации, защищенной с использованием одного и того же средства криптографической защиты информации (одних и тех же средств криптографической защиты информации) является критическим - более 5000 расчетных показателей (влечет существенные негативные последствия в социальной, политической, международной, экономической, финансовой или иных областях деятельности), не может быть компенсирован оператором информационной системы и/или обладателем информации, которые не могут выполнять возложенные на них функции (коэффициент 3).

40. Средства криптографической защиты информации не могут быть признаны соответствующими первому, второму, третьему или четвертому уровню безопасности, если вычислительная сложность существующих алгоритмов вскрытия криптографической защиты, обеспечиваемой ими, составляет менее 2^{50}, 2^{80}, 2^{120} или 2^{160} возможных комбинаций для перебора соответственно.

41. Общие технические требования к средствам криптографической защиты информации по уровням безопасности университета должны соответствовать Требованию к защите информации, содержащейся в базах данных государственных информационных систем, утвержденный Постановлением Правительства КР от 21 ноября 2017 года № 762.

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

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

43. При предоставлении доступа к операционным система, приложениям информационной системе, реализуется принцип минимума привилегий доступа.

44. В целях защиты информации организационно и технически разделяются подразделения Университета, имеющие доступ и работающие с различной информацией (в разрезе ее конфиденциальности и смысловой направленности). Данная задача решается с использованием возможностей конкретных информационных систем, где в целях обеспечения защиты данных доступ и права пользователей ограничивается набором прав и ролей. В случае обработки информации конфиденциального характера права назначаются администратором информационных систем по ролевой матрице доступа, в соответствии с функциональными обязанностями, определяемыми должностью и по служебной записке руководителя подразделения согласованной с комплайнсом.

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

46. Для защиты от несанкционированного доступа на компьютерах в сегментах сети, где обрабатывается информация конфиденциального характера используются продукты линейки Dallas Lock, Secret Net, с администрированием в Центре безопасности, развернутом в домене. Администратором Центра безопасности является администратор домена.

47. Не допускается использование учетных записей уволенных сотрудников.

Использование электронной почты, сети Интернет

48. Не допускается распространять материалы, использование и распространение которых ограничено действующим законодательством Кыргызской Республики.

49. Пересылка информации конфиденциального характера осуществляется только с использованием корпоративной почты.

50. Электронная почта на рабочем месте сотрудника используется только для служебной, и иной, предусмотренной должностными обязанностями переписки.

51. Логин и пароль к корпоративной электронной почте для сотрудников выдает ответственный сотрудник ОИТТОК по служебной записке на имя руководителя ОИТТОК, для студентов – по студенческому билету.

52. Запрещается открывать письма с подозрительными вложениями, с незнакомого адреса и т.п., о получении подобных писем сообщается комплайнсу.

53. Запрещается публиковать информацию конфиденциального характера в социальных сетях, пересылать через системы мгновенного обмена сообщениями (Skype, ICQ, Jabber и. т. п.).

54. Запрещается использование облачных сервисов на рабочих местах сотрудников, обрабатывающих информацию конфиденциального характера.

55. Доступ через беспроводную сеть разрешается только к общедоступным ресурсам сети. Беспроводные точки устанавливают и администрируют сотрудники ОИТТОК.

56. Самостоятельно скачивать и устанавливать программное обеспечение разрешается только уполномоченным на то сотрудникам ОИТТОК.

57. Запрещается несогласованная с ОИТТОК установка роутеров WiFi.

Физическая безопасность

58. Серверное оборудование аппаратно-программного комплекса и системы хранения данных размещаются в серверном помещении.

59. Серверное помещение располагается в отдельных, непроходных помещениях без оконных проемов. При наличии оконных проемов они закрываются или заделываются негорючими материалами.

60. Для поверхности стен, потолков и пола применяются материалы, не выделяющие и не накапливающие пыль. Для напольного покрытия применяются материалы с антистатическими свойствами. Серверное помещение защищается от проникновения загрязняющих веществ.

61. Стены, двери, потолок, пол и перегородки серверного помещения обеспечивают герметичность помещения. Двери серверного помещения составляют не менее 1,2 метра в ширину и 2,2 метра в высоту, открываются наружу или раздвигаются. Конструкция рамы двери не предусматривает порога и центральной стойки.

62. Серверное помещение оборудуется фальшполом и (или) фальшпотолком для размещения кабельных систем и инженерных коммуникаций.

63. Через серверное помещение исключается прохождение любых транзитных коммуникаций. Трассы обычного и пожарного водоснабжения, отопления и канализации выносятся за пределы серверного помещения и не размещаются над серверным помещением на верхних этажах.

64. Монтаж коммуникационных каналов для прокладки силовых и слаботочных кабельных сетей здания выполняется в отдельных или разделенных перегородками кабельных лотках, коробах или трубах, разнесенных между собой. Слаботочные и силовые шкафы устанавливаются раздельно и закрываются на замок. Прокладка кабелей через перекрытия, стены, перегородки осуществляется в отрезках несгораемых труб с герметизацией негорючими материалами.

65. Серверное помещение надежно защищается от внешнего электромагнитного излучения.

66. При размещении оборудования в серверном помещении:

- обеспечивается исполнение правил технической эксплуатации электроустановок потребителей, утвержденных уполномоченным органом в сфере энергетики;
- обеспечивается исполнение требований поставщиков и (или) производителя оборудования к установке (монтажу), нагрузке на перекрытия и фальшпол, с учетом веса оборудования и коммуникаций;
- обеспечивается наличие свободных служебных проходов для обслуживания оборудования;
- учитывается организация воздушных потоков системы обеспечения микроклимата;
- учитывается организация системы фальшполов и фальшпотолков.

67. При техническом сопровождении оборудования, установленного в серверном помещении, подразделением компетентным в вопросах информационных технологий документируются:

- обслуживание оборудования;
- устранение проблем, возникающих при работе аппаратно-программного обеспечения;
- факты сбоев и отказов, а также результаты восстановительных работ;
- послегарантийное обслуживание критически важного оборудования по истечении гарантийного срока обслуживания.

68. Обслуживание критически важного оборудования выполняется сертифицированным техническим персоналом.

69. В непосредственной близости от серверного помещения создается склад запасных частей для критически важного оборудования, содержащий запас комплектующих и оборудования для выполнения оперативной замены при проведении ремонтно-восстановительных работ.

70. Вмешательство в работу находящегося в эксплуатации оборудования возможно только с разрешения руководителя ОИТТОК либо лица, его замещающего.

71. Основные и резервные серверные помещения располагаются на безопасном расстоянии в удаленных друг от друга зданиях. Требования к резервным серверным помещениям идентичны требованиям к основным серверным помещениям.

72. Для обеспечения кибербезопасности, отказоустойчивости и надежности функционирования:

1) в серверном помещении применяются способы расположения оборудования, обеспечивающие снижение рисков возникновения угроз, опасностей и возможностей несанкционированного доступа;

2) поддерживается в актуальном состоянии список лиц, авторизованных для осуществления сопровождения объектов критической информационной инфраструктуры, установленных в серверном помещении;

3) серверное помещение оборудуется системами:

- контроля и управления доступом;
- обеспечения микроклимата;
- охранной сигнализации;
- видеонаблюдения;
- пожарной сигнализации;
- пожаротушения;
- гарантированного электропитания;
- заземления;

4) отказоустойчивость инфраструктуры серверного помещения должна составлять не менее 99,7 процента.

73. Система контроля и управления доступом обеспечивает санкционированный вход в серверное помещение и санкционированный выход из него. Преграждающие устройства и конструкция входной двери должны предотвращать возможность передачи идентификаторов доступа в обратном направлении через тамбур входной двери.

74. Устройство центрального управления системы контроля и управления доступом устанавливается в защищенных от доступа посторонних лиц отдельных служебных помещениях, в том числе в помещении поста охраны.

75. Доступ персонала охраны к программным средствам системы контроля и управления доступом, влияющим на режимы работы системы, должен быть исключен.

76. Электроснабжение системы контроля и управления доступом осуществляется от свободной группы щита дежурного освещения. Система контроля и управления доступом обеспечивается резервным электропитанием.

77. Система обеспечения микроклимата должна включать системы кондиционирования, вентиляции и мониторинга микроклимата. Системы обеспечения микроклимата серверного помещения не должна объединяться с другими системами микроклимата, установленными в здании.

78. Температура в серверном помещении поддерживается в диапазоне от 20 °С до 25 °С при относительной влажности от 45 до 55 процентов.

79. Мощность системы кондиционирования воздуха должна превышать суммарное тепловыделение всего оборудования и систем. Система кондиционирования воздуха обеспечивается резервированием. Электропитание кондиционеров серверного помещения осуществляется от системы гарантированного электропитания или системы бесперебойного электропитания.

80. Система вентиляции обеспечивает приток свежего воздуха с фильтрацией и подогревом поступающего воздуха в зимний период. В серверном помещении давление создается избыточным для предотвращения поступления загрязненного воздуха из соседних помещений. На воздуховодах приточной и вытяжной вентиляции устанавливаются защитные клапаны, управляемые системой пожаротушения. Системы кондиционирования и вентиляции отключаются автоматически по сигналу пожарной сигнализации.

81. Система мониторинга микроклимата контролирует климатические параметры в серверных шкафах и телекоммуникационных стойках:

- температуру воздуха;
- влажность воздуха;
- запыленность воздуха;
- скорость потока воздуха;
- задымленность воздуха;
- открытие (закрытие) дверей шкафов.

82. Система охранной сигнализации серверного помещения выполняется отдельно от систем безопасности здания. Сигналы оповещения выводятся в помещение круглосуточной охраны в виде отдельного пульта. Контролю и охране подлежат все входы и выходы серверного помещения, а также внутренний объем серверного помещения. Система охранной сигнализации имеет собственный источник резервированного питания.

83. Расположение камер системы видеонаблюдения выбирается с учетом обеспечения контроля всех входов и выходов в серверное помещение, пространства и проходов возле оборудования. Угол обзора и разрешение камер должны обеспечить распознавание лиц. Изображение с камер выводится на отдельный пульт в помещение круглосуточной охраны.

84. Система пожарной сигнализации серверного помещения выполняется отдельно от пожарной сигнализации здания. В серверном помещении устанавливаются два типа датчиков: температурные и дымовые.

85. Датчиками контролируются общее пространство серверного помещения и объемы, образованные фальшполом и (или) фальшпотолком. Сигналы оповещения системы пожарной сигнализации выводятся на пульт в помещение круглосуточной охраны.

86. Система пожаротушения серверного помещения оборудуется автоматической установкой пожаротушения, независимой от системы пожаротушения здания.

87. Установка пожаротушения размещается непосредственно в серверном помещении или вблизи него в специально оборудованном для этого шкафу. Запуск системы пожаротушения производится от датчиков раннего обнаружения пожара, реагирующих на появление дыма, а также ручных датчиков, расположенных у выхода из помещения. Время задержки выпуска огнегасителя составляет не более 30 секунд. Оповещение о срабатывании системы пожаротушения выводится на табло, размещаемые внутри и снаружи помещения. Система пожаротушения выдает команды на закрытие защитных клапанов системы вентиляции и отключение питания оборудования. Серверное помещение, оборудованное системой пожаротушения, оснащается вытяжной вентиляцией.

88. Система гарантированного электропитания предусматривает наличие двух вводов электропитания от разных источников внешнего электропитания на напряжение ~400/230 В, частотой 50 Гц и автономного генератора. Все источники электроэнергии подаются на автомат ввода резерва, осуществляющий автоматическое переключение на резервный ввод электропитания при превращении, перерыве подачи электропитания на основном вводе. Параметры линий электропитания и сечение жил определяются исходя из планируемой суммарной потребляемой мощности оборудования и подсистем серверного помещения. Линии электропитания выполняются по пятипроводной схеме.

89. Система гарантированного электропитания предусматривает электроснабжение оборудования и систем серверного помещения через источники бесперебойного питания. Мощность и конфигурация источников бесперебойного питания рассчитываются с учетом всего запитываемого оборудования и запаса для перспективного развития. Время автономной работы от источников бесперебойного питания рассчитывается с учетом потребностей, а также необходимого времени для перехода на резервные линии и времени запуска генератора в рабочий режим.

90. Система заземления серверного помещения выполняется отдельно от защитного заземления здания. Все металлические части и конструкции серверного помещения заземляются с общей шиной заземления. Каждый шкаф (стойка) с оборудованием заземляется отдельным проводником, соединяемым с общей шиной заземления. Открытые токопроводящие части оборудования обработки информации должны быть соединены с главным заземляющим зажимом электроустановки. Заземляющие проводники, соединяющие устройства защиты от перенапряжения с главной заземляющей шиной, должны быть самыми короткими и прямыми (без углов).

Обработка персональных данных

91. Необходимая нормативная и организационно-регламентирующая документация размещена на сайте Университета.

92. Все сотрудники Университета, являющиеся пользователями информационной системы персональных данных, должны четко знать и строго выполнять установленные законами Кыргызской Республики "Об информации персонального характера", "Об электронной подписи", "Об электронном управлении" и «О наружном видеонаблюдении» правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности обработки персональных данных.

93. Компетентность пользователей в области обеспечения информационной безопасности достигается обучением правилам безопасной (с точки зрения информационной безопасности) работы, осведомленности об источниках потенциальных угроз и периодическими проверками их знаний и навыков. Занятия с пользователями проводятся комплайнс и/или уполномоченным государственным органом в области государственной и национальной безопасности (КГНБ КР) на регулярной основе не реже двух раз в год.

94. Все действия пользователей компьютеров и обязанности по соблюдению требований информационной безопасности определяются Соглашением (договором) о неразглашении конфиденциальной информации (Приложение 1), который они изучают, имеют распечатанный экземпляр с подписью сотрудника об ознакомлении.

95. При допуске сотрудника к выполнению обязанностей связанных с обработкой персональных данных непосредственный начальник подразделения, в которое он поступает, организует ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите персональных данных, подает служебную записку руководителю ОИТТОК о предоставлении доступа к информационным система персональных данных с указанием предполагаемой роли сотрудника.

96. Далее сотрудник проходит инструктаж у администратора безопасности информационных систем персональных данных, и расписывается об ознакомлении с Соглашением (договором) о неразглашении конфиденциальной информации (Приложение 1), получает у администратора информационной системы персональных данных, логин и пароль к учетной записи с правами, согласно ролевой матрицы доступа.

97. Порядок работы с запросами на предоставление сведений по персональным данным определяется Порядком получения согласия субъекта персональных данных на сбор и обработку его персональных данных, порядок и форму уведомления субъектов персональных данных о передаче их персональных данных третьей стороне, утвержденным Постановлением Правительства КР от 21 ноября 2017 года № 759.

98. С согласия субъекта персональных данных общедоступными персональными данными сотрудников являются фамилия, имя, отчество, занимаемая должность, подразделение, а студентов, аспирантов, докторантов, слушателей - фамилия, имя, отчество, группа, специальность.

99. Сотрудники Университета должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.

100.Сотрудникам, обрабатывающим персональные данные, запрещается устанавливать любое программное обеспечение, подключать личные мобильные устройства и отчуждаемые незарегистрированные в Службе внутреннего аудита носители информации, а так же записывать на них защищаемую информацию, за исключением случаев, предусмотренных функциональными обязанностями.

101.Сотрудникам запрещается разглашать содержание защищаемой информации, которая стала им известна при работе с информационными системами Университета, третьим лицам, согласно законами Кыргызской Республики "Об информации персонального характера", "Об электронной подписи", "Об электронном управлении" и «О наружном видеонаблюдении».

102.Запрещается хранение информации конфиденциального характера локально на компьютере, не оснащенном программными средствами предотвращения несанкционированного доступа (SecretNet, DallasLock и др.)

103.Допуск к Информационным системам персональных данных третьих лиц для осуществления ими договорных обязательств осуществляется при выполнении требований, предъявляемых к защите информации и соблюдения конфиденциальности, отражаемых в договоре, согласованном с Службой внутреннего аудита на этапе заключения.

104.Средства криптографической защиты информации при обработке персональных данных в университете не используются.

Дублирование, резервное копирование и хранение информации

105.Для обеспечения физической целостности данных, во избежание умышленного или неумышленного уничтожения или искажения защищаемой информации и конфигураций информационных систем организуется резервное копирование баз данных, конфигураций, файлов настроек, конфигурационных файлов.

106.Порядок резервного копирования, дублирования, хранения архивов и восстановления информации определен Требованием к защите информации, содержащейся в базах данных государственных информационных систем, утвержденный Постановлением Правительства КР от 21 ноября 2017 года № 762.

107.Для обеспечения гарантированного восстановления особо важной информации, которая может быть утеряна вследствие аппаратных сбоев, воздействия вирусов-шифровальщиков производится ежедневное резервное копирование содержимого дисков. Данный процесс запускается по служебной записке сотрудника на имя руководителя ОИТТОК. Ответственными за организацию резервного копирования, хранения копий и восстановления информации являются администраторы информационных систем, ответственные сотрудники ОИТТОК.

108. Доступ к резервным копиям организуется по протоколу ftps и SMB для Acronis Storage Server. Еженедельно архивная копия базы данных информационных систем персональных данных дублируется сотрудником ОИТТОК с использованием соответствующего оборудования на отчуждаемый носитель.

Ответственность за соблюдение положений Политики информационной безопасности

109.Общее руководство обеспечением информационной безопасности осуществляет руководитель Службы внутреннего аудита, риск-менеджмента и комплайнса.

110.Ответственным за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение и внесение изменений в процессы информационной безопасности является руководитель ОИТТОК.

111.Нарушение требований Политики, локальных нормативных актов по обеспечению информационной безопасности является чрезвычайным происшествием и влечет за собой последствия, предусмотренные действующим законодательством Кыргызской Республики, локальными нормативными актами, договорами, заключенными между университетом и сотрудниками (студентами, аспирантами).

112.Степень ответственности за нарушение требований локальных нормативных актов в области информационной безопасности определяется в каждом конкретном случае

113.Руководители структурных подразделений, несут персональную ответственность за обеспечение информационную безопасность в возглавляемых ими подразделениях, обязаны незамедлительно сообщать в Службу внутреннего аудита, риск-менеджмента и комплайнса о всех инцидентах, связанных с нарушениями требований информационной безопасности.

114.Руководители структурных подразделений ОИТТОК обязаны незамедлительно сообщать в Службу внутреннего аудита, риск-менеджмента и комплайнса о всех происшествиях и нештатных ситуациях в сфере их деятельности связанных с информационной безопасностью.

115.Виды ответственности, предусмотренные законами Кыргызской Республики:

- гражданско-правовая ответственность;
- дисциплинарная ответственность;
- уголовная ответственность;
- административная ответственность.

Порядок пересмотра Политики информационной безопасности

116.Пересмотр Политики информационной безопасности производится не реже одного раза в три года и имеет целью приведение в соответствие определенных Политикой защитных мер реальным условиям и текущим требованиям к защите информации.

117.Внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

118.Изменения и дополнения в Политику утверждает ректор Университета.

Приложение 1.

Соглашение (договор) о неразглашении конфиденциальной информации

г.Ош "___"_____ 20___ г.

Учреждение «Ошский государственный университет» (далее-университет), в лице Кожобекова К.Г., действующего на основании Устава и Политики информационной безопасности, и гражданин:

_____

(фамилия, имя, отчество)

действующий от своего имени, именуемые в дальнейшем сторонами, заключили настоящее соглашение о нижеследующем:

Я, _____

(фамилия, имя, отчество)

будучи поставлен(а) в известность о том, что по роду своей служебной деятельности и должностным обязанностям буду допущен(а) к сведениям ограниченного распространения (персональные данные, коммерческая тайна, государственная тайна, секретные научные исследования, врачебная тайна, военная тайна, и т.п.) в университете, принимаю на себя добровольные обязательства:

- не разглашать сведения ограниченного распространения, которые мне будут доверены (станут известны) по ходу службы;
- не передавать третьим лицам и не раскрывать публично сведения ограниченного распространения, без соответствующей санкции (разрешения) руководства;
- выполнять относящиеся ко мне требования приказов, инструкций и положений по защите сведений ограниченного распространения;
- в случае попытки посторонних лиц получить от меня сведения ограниченного распространения, немедленно сообщить об этом факте руководству своего подразделения;
- сохранять сведения ограниченного распространения сторонних организаций, с которыми университет связан договорными отношениями;
- не использовать знания сведений ограниченного распространения, для занятия какой-либо деятельностью, которая может нанести ущерб интересам университета;
- в случае моего увольнения, все носители сведений ограниченного распространения, которые находились в моем распоряжении в связи с исполнением своих служебных обязанностей, передать по указанию руководителя подразделения;
- об утрате или недостаче носителей сведений ограниченного распространения, что может привести к несанкционированному распространению конфиденциальных сведений, немедленно сообщать руководителю своего подразделения.

Обязуюсь добросовестно выполнять свои обязательства по настоящему соглашению.

Я предупрежден(а), что, в случае невыполнения взятых на себя обязательств, могу быть привлечен(а) к ответственности в соответствии с действующим законодательством Кыргызской Республики и другими нормативными документами, действующими в университете.

Руководство обязуется, в случае допуска гр.:

_____

(фамилия, имя, отчество)

к сведениям ограниченного распространения, создавать необходимые условия для работы с такими сведениями.

_____ "___" _____ 20__ г.

(подпись лица, заключившего соглашение)

Ректору Ошского государственного университета
к.ф.-м.н., доценту Кожобекову К.Г.

Уведомление №2

Уважаемый Кудайберди Гапаралиевич!

Руководствуясь Законом КР «О внутреннем аудите», постановлением Правительства Кыргызской Республики «Об утверждении Стандартов внутреннего аудита в Кыргызской Республике» от 3 июня 2014 года № 296, постановлением Правительства Кыргызской Республики «О Совете по внутреннему аудиту» от 9 сентября 2013 года № 498, постановлением Правительства Кыргызской Республики «Об утверждении Положения о финансовом управлении и контроле в бюджетных учреждениях» от 31 декабря 2013 года № 722, приказом Министерства финансов Кыргызской Республики «Об утверждении Руководства по составлению программы гарантии и повышения качества внутреннего аудита» от 28 декабря 2016 года № 212-П и приказом Министерства финансов Кыргызской Республики «Руководство по внутреннему аудиту (методическое пособие)» от 17 марта 2008 года N 54-П

Рекомендуем:

1. Типовые штаты университета должны быть приведены в соответствии Постановлению Правительства Кыргызской Республики от 20 ноября 2015 года № 788 «Об утверждении типовых штатов организаций среднего и высшего профессионального образования системы Министерства образования и науки Кыргызской Республики, так как деятельность университета, кроме специальных средств, также финансируется за счет республиканского бюджета, несмотря на то что эти средства составляют малую сумму;
2. В соответствии Постановлении Правительства Кыргызской Республики от 29 мая 2012 года № 346 «Об утверждении нормативных правовых актов, регулирующих деятельность образовательных организаций высшего и среднего профессионального образования Кыргызской Республики» департаменты (отделы) должны быть реорганизованы согласно пункту 1 настоящего уведомления.
3. Утвердить Политику информационной безопасности в целях исполнения требований:
   - Закона Кыргызской Республики "Об информации персонального характера";
   - Постановления ПКР от 21 ноября 2017 года № 762 «Об утверждении Требований к защите информации, содержащейся в базах данных государственных информационных систем»;
   - Постановления ПКР от 21 ноября 2017 года № 759 «Об утверждении Порядка получения согласия субъекта персональных данных на сбор и обработку его персональных данных, порядка и формы уведомления субъектов персональных данных о передаче их персональных данных третьей стороне» .

С уважением,
и.о.руководителя Службы внутреннего комплайнса ОшГУ
Шукур Тегин Замир