НЕКОММЕРЧЕСКОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»

Утверждаю

Ректор Некоммерческого акционерного общества «Алматинский университет энергетики и связи имени Гумарбека Даукеева»

_____ Сагинтаева С.С.

«_24_» ____04_____2020 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕКОММЕРЧЕСКОГО АКЦИОНЕРНОГО ОБЩЕСТВА «АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»

ИЗДАНИЕ 1
Введено в действие с даты подписания

Алматы, 2020 г.

Содержание

Паспорт документа 3

Лист согласования 4

1. Общие положения 5

2. Цели и задачи 6

3. Организационно-правовой статус работников ДИТ 6

4. Область действия 7

5. Порядок доступа пользователей к информационным системам, в которых обрабатывается информация конфиденциального характера 7

6. Сетевая безопасность 7

7. Обработка персональных данных 8

8. Дублирование, резервное копирование и хранение информации 9

9. Ответственность за соблюдение положений Политики 9

10. Порядок пересмотра Политики 10

Лист ознакомления

Паспорт документа	
Тип документа	Организационная документация Политика
Наименование документа	Политика информационной безопасности Некоммерческого акционерного общества «Алматинский университет энергетики и связи имени Гумарбека Даукеева»
Цель документа	Общие положения; цели и задачи; Организационно-правовой статус работников ДИТ; область действий; Порядок доступа пользователей к информационным системам, в которых обрабатывается информация конфиденциального характера; Сетевая безопасность; Обработка персональных данных; Дублирование, резервное копирование и хранение информации; Ответственность за соблюдение положений Политики; Порядок пересмотра Политики
Разработка	Директор департамента информационных технологий
Согласование	Проректор по академической деятельности Юрисконсульт Ведущий специалист отдела системы менеджмента качества
Утверждение	Ректор
Исполнители документа	Все работники Университета
Контроль за исполнением	Директор департамента информационных технологий
Приложения к документу	Да
Исключения	Нет
Нормативные ссылки	Закона Республики Казахстан от 24 ноября 2015 года «Об информатизации» Закон Республики Казахстан от 21 мая 2013 года N 94-V «О персональных данных и их защите» Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности». Трудовой кодекс РК Закон «Об образовании» РК от 27 июля 2007г.
Владелец оригинала	Отдел системы менеджмента качества

Лист согласования

Политика согласована:

Проректор по академической деятельности
_Коньшин С.В._____ _____
«_24_» _____05_____ 2020г.

Юрисконсульт
_Абдешова А._____ _____
«_24_» _____05_____ 2020 г.

Ведущий специалист отдела системы менеджмента качества
_Елашкина Н.В._____ _____
«_24_» _____05_____ 2020 г.

Разработано:

Директор департамента информационных технологий
_Каткаев В._____ _____
«_24_» _____05_____ 2020 г.

1. Общие положения

1.1 Настоящее Политика информационной безопасности (далее - Политика) Некоммерческого акционерного общества «Алматинский университет энергетики и связи имени Гумарбека Даукеева» (далее – университет) является официальным документом.

1.2 Политика Университета разработана в соответствии с требованиями действующего законодательства и нормативных актов Республики Казахстан: Закона Республики Казахстан от 24 ноября 2015 года «Об информатизации», Закон Республики Казахстан от 21 мая 2013 года N 94-V «О персональных данных и их защите», Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

1.3 Предметом настоящего документа является:

1.3.1 порядок доступа к информационным системам;

1.3.2 сетевая безопасность;

1.3.3 локальная безопасность;

1.3.4 физическая безопасность;

1.3.5 обеспечение защиты персональных данных;

1.3.6 дублирование, резервирование и хранение информации;

1.3.7 ответственность за соблюдение положений Политики ИБ.

1.4 Для целей настоящих Политик информационной безопасности используются следующие определения:

1.4.1 техническая документация по информационной безопасности (далее - ТД ИБ) - документация, устанавливающая политику, правила, защитные меры, касающиеся процессов обеспечения ИБ объектов информатизации и (или) организации;

1.4.2 рабочая станция - стационарный компьютер в составе локальной сети, предназначенный для решения прикладных задач;

1.4.3 системное программное обеспечение - совокупность программного обеспечения для обеспечения работы вычислительного оборудования;

1.4.4 журналирование событий - процесс записи информации о происходящих с объектом информатизации программных или аппаратных событиях в журнал регистрации событий;

1.4.5 локальная сеть (далее - ЛС) - локальная сеть Университета, отнесенная к внешнему контуру телекоммуникационной сети Университета, имеющая соединение с Интернетом, доступ к которому для Университета предоставляется операторами связи только через единый шлюз доступа к Интернету.

1.5 Для целей настоящих Политик информационной безопасности используются следующие сокращения:

1.5.1 АПК - аппаратно-программный комплекс;

1.5.2 ИБ - информационная безопасность;

1.5.3 ИС - информационная система;

1.5.4 ИКИ - информационно-коммуникационная инфраструктура;

1.5.5 ИКТ - информационно-коммуникационные технологии;

1.5.6 ПО - программное обеспечение;

1.5.7 МИО - местные исполнительные органы;

1.5.8 СПО - свободное программное обеспечение;

1.5.9 ЕШДИ - единый шлюз доступа к Интернету;

1.5.10 ИР - интернет-ресурс;

1.5.11 ЕТС ГО - единая транспортная среда государственных органов;

1.5.12 ЕПИР ГО - единая платформа интернет-ресурсов государственных органов;

1.5.13 СПП - сервисный программный продукт;

1.5.14 ЭИР - электронные информационные ресурсы;

1.5.15 ИКП ЭП - информационно-коммуникационная платформа «электронного правительства»;
1.5.16 АРМ - автоматизированное рабочее место;
1.5.17 ДИТ – Департамент информационных технологий;
1.5.18 ОС - операционная система
1.5.19 ПДн – персональные данные
1.5.20 Университет - Некоммерческого акционерного общества «Алматинский университет энергетики и связи имени Гумарбека Даукеева»
1.5.21 ЭЦП - электронная цифровая подпись.

2. Цели и задачи

2.1 Политика 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.
2.2 Направление информационной безопасности действует в Департаменте информационных технологий со следующими задачами и функциями:
2.2.1 выявление, оценка и прогнозирование угроз информационной безопасности;
2.2.2 организация технической защиты информации, участие в проектировании систем защиты;
2.2.3 проведение периодического контроля состояния ИБ, учет и анализ результатов с выработкой решений по устранению уязвимостей и нарушений;
2.2.4 организация плановых проверок режима защиты, и разработка соответствующей документации, анализ результатов, расследование нарушений;
2.2.5 разработка и осуществление мероприятий по защите персональных данных;
2.2.6 организация взаимодействия со всеми структурами, участвующими в их обработке, выполнение требований законодательства к информационным системам персональных данных, контроль действий операторов, отвечающих за их обработку;
2.2.7 разработка и совершенствование нормативно-правовой базы обеспечения информационной безопасности (совместно с ОПО).

3. Организационно-правовой статус работников ДИТ

3.1 Работники имеют право беспрепятственного доступа во все помещения, где установлены технические средства с Информационными системами, право требовать от руководства подразделений и администраторов ИС прекращения автоматизированной обработки информации, персональных данных, при наличии непосредственной угрозы защищаемой информации.
3.2 Имеют право получать от пользователей и администраторов необходимую информацию по вопросам применения информационных технологий, в части касающейся вопросов информационной безопасности.
3.3 Имеют право проводить аудит действующих и вновь внедряемых ИС, ПО, 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.
3.4 Имеют право контролировать исполнение утвержденных нормативных и организационно-распорядительных документов, касающихся вопросов информационной безопасности.

4. Область действия

4.1 Требования настоящей Политики распространяются на всех работников Университета (штатных, временных, работающих по контракту и т.п), а также всех прочих лиц (подрядчики, аудиторы и т.п.).
4.2 Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах с контрагентами.

5. Порядок доступа пользователей к информационным системам, в которых обрабатывается информация конфиденциального характера

5.1 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 ИС, а так же для их регистрации входа (выхода) в систему (из системы).
5.2 Все действия пользователей ИС регистрируются в журналах событий системного и прикладного ПО. Данные электронные журналы доступны для чтения, анализа и резервного копирования только администратору соответствующего ПО, который несет персональную ответственность за полноту и точность отражения в журнале имевших место событий. Он же, по запросу, выборочно передает данные из журналов работнику ДИТ.
5.3 При необходимости работнику ДИТ предоставляется административный доступ к серверам и базам данных по служебной записке на имя ректора Университета.
5.4 Запрещается доступ суперпользователей к серверам и базам данных под единой или предопределенной учетной записью.
5.5 Порядок доступа, получения логинов и паролей, определяется *Порядком предоставления прав доступа*.

6. Сетевая безопасность

6.1 Доступ из Интернет в сеть университета:

6.1.1 доступ во внутреннюю сеть осуществляется только через настроенный межсетевой экран;
6.1.2 доступ из вне периметра сети разрешен только по распоряжению директора ДИТ, по определенному порту и на определенное время;
6.1.3 не допускается удаленный доступ в локальную сеть с использованием не персонифицированных, групповых и анонимных учетных записей;
6.1.4 не допускается использование программ удаленного администрирования (TeamViewer, Anydesk…). Как исключение, по согласованию с директором ДИТ возможно подключение для удаленной настройки ПО на ограниченное время.
6.1.5 При администрировании удаленного доступа к ресурсам корпоративной сети Университета предъявляются следующие требования:
6.1.6 удаленный доступ пользователей к ресурсам и сервисам компьютерной сети Университета обеспечивается на основе зарегистрированных персональных учетных записей, с использованием технологии VPN, других протоколов шифрования;
6.1.7 доступ предоставляется сроком на 3 месяца, при необходимости продлевается с разрешения директора ДИТ;
6.1.8 делается соответствующая запись в Журнале учета предоставления удаленного доступа;
6.1.9 список работников, которым предоставлен удаленный доступ поддерживается в актуальном состоянии.

6.2 В целях обеспечения безопасности и нормального функционирования проводных компьютерных сетей запрещается:

6.2.1 самовольно подключать компьютерное оборудование (беспроводные точки доступа, маршрутизаторы, компьютеры и др.) к сети Университета и присваивать ему сетевое имя и адрес без согласования ДИТ;

6.2.2 перемещать компьютеры между сетевыми розетками и другими коммуникационными устройствами без согласования с ДИТ;

6.2.3 использовать информационные ресурсы университета для сетевых игр, распространения коммерческой рекламы, организации СПАМа;

6.2.4 использовать любые почтовые сервисы кроме корпоративного;

6.2.5 сканировать узлы сети неуполномоченными на то работниками.

6.3 Средства защиты, маршрутизаторы и межсетевые экраны:

6.3.1 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;

6.3.2 для анализа защищенности ИС работниками ДИТ применяются специализированные программно-аппаратные средства – сканеры безопасности. Проводится выявление и анализ уязвимостей и несоответствия в настройках ОС, ПО, СУБД и сетевого оборудования. Запрещается использовать ПО снятое с поддержки, имеющее уязвимости, с просроченными сертификатами;

6.3.3 подсистема обнаружения вторжений, обеспечивает выявление сетевых атак на элементы ИС подключенные к сетям общего пользования;

6.3.4 функционал подсистемы реализуется программными и программно-аппаратными средствами, на межсетевых экранах. Работниками ДИТ ведут регулярный мониторинг доступа, контролируют содержание трафика с использованием специализированного ПО, проводит анализ лог-файлов;

6.3.5 на межсетевом экране заводится лог-файл, куда записываются все обращения к ресурсам (попытки создания соединений). Доступ к лог-файлам имеют администраторы сети;

6.3.6 доступ из одного сегмента сети в другой ограничивается и разделяется маршрутизаторами;

6.3.7 сеть ИС с доступом из вне периметра, выделена в отдельный сегмент и защищена межсетевым экраном;

6.3.8 в контролируемых зонах университета ведется видеонаблюдение;

6.3.9 на территории университета действует пропускной режим, порядок которого определяется локальным нормативным актом Университета.

7. Обработка персональных данных

7.1 Все работники Университета, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные внутренними нормативными документами правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности обработки ПДн.

7.2 Компетентность пользователей в области обеспечения ИБ достигается обучением правилам безопасной (с точки зрения ИБ) работы, осведомленности об источниках потенциальных угроз и периодическими проверками их знаний и навыков. Занятия с пользователями проводятся работниками ДИТ на регулярной основе не реже двух раз в год.

7.3 Все действия пользователей компьютеров и обязанности по соблюдению требований ИБ определяются *Порядком действий пользователя информационной системы по обеспечению информационной безопасности* в Университете, который они изучают, имеют распечатанный экземпляр с подписью работника об ознакомлении.

7.4 При допуске работника к выполнению обязанностей связанных с обработкой персональных данных подписывает Обязательство о неразглашении персональных данных. Бумажная версия Обязательство передается в ДИТ.
7.5 Далее работник проходит инструктаж у администратора ДИТ, и расписывается об ознакомлении с Положением о защите персональных данных и Порядком обеспечения конфиденциальности при обработке персональных данных, получает у администратора ИС ПДн логин и пароль к учетной записи с правами, согласно ролевой матрицы доступа.
7.6 Порядок работы с запросами на предоставление сведений по персональным данным определяется утвержденными локальными нормативными документами.
7.7 Общедоступными персональными данными работников являются фамилия, имя, отчество, занимаемая должность, подразделение, а студентов, аспирантов, слушателей - фамилия, имя, отчество, группа, специальность.
7.8 Работники Университета должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.
7.9 Работникам, обрабатывающим ПДн, запрещается устанавливать любое программное обеспечение, подключать личные мобильные устройства и отчуждаемые носители информации, а также записывать на них защищаемую информацию, за исключением случаев, предусмотренных функциональными обязанностями.
7.10 Работникам запрещается разглашать содержание защищаемой информации, которая стала им известна при работе с информационными системами Университета, третьим лицам, согласно Положения о защите персональных данных.
7.11 Допуск к ИС ПДн третьих лиц для осуществления ими договорных обязательств осуществляется при выполнении требований, предъявляемых к защите информации и соблюдения конфиденциальности, отражаемых в договоре, согласованном с ОПО на этапе заключения.
7.12 СКЗИ при обработке персональных данных в университете не используются.
7.13 Текст Политики в отношении обработки персональных данных размещается на сайте Университета в свободном доступе.

8. Дублирование, резервное копирование и хранение информации

8.1 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.
8.2 Порядок резервного копирования, дублирования, хранения архивов и восстановления информации определен Порядком резервирования и восстановления информации.
8.3 Для обеспечения гарантированного восстановления особо важной информации, которая может быть утеряна вследствие аппаратных сбоев, воздействия вирусов-шифровальщиков производится ежедневное резервное копирование важных ИС. Данный процесс запускается по служебной записке работника на имя директора ДИТ.
8.4 Ответственными за организацию резервного копирования, хранения копий и восстановления информации являются администраторы ИС, ответственные работники ДИТ.

9. Ответственность за соблюдение положений Политики

9.1 Общее руководство обеспечением информационной безопасности осуществляет директор ДИТ.
9.2 Ответственным за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение и внесение изменений в процессы информационной безопасности является директор ДИТ.

9.3 Нарушение требований Политики, локальных нормативных актов по обеспечению ИБ является чрезвычайным происшествием и влечет за собой последствия, предусмотренные действующим законодательством Республики Казахстан, локальными нормативными актами, договорами, заключенными между университетом и работниками (обучающимися).
9.4 Степень ответственности за нарушение требований локальных нормативных актов в области ИБ определяется в каждом конкретном случае.
9.5 Руководители структурных подразделений, несут персональную ответственность за обеспечение ИБ в возглавляемых ими подразделениях, обязаны незамедлительно сообщать в ДИТ о всех инцидентах, связанных с нарушениями требований информационной безопасности.
9.6 Виды ответственности, предусмотренные законами об обращении с информацией конфиденциального характера:

9.6.1 гражданско-правовая ответственность;
9.6.2 дисциплинарная ответственность;
9.6.3 уголовная ответственность;
9.6.4 административная ответственность.

10. Порядок пересмотра Политики

10.1 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.
10.2 Внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов ИБ, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, результатам проведения внутренних аудитов ИБ и других контрольных мероприятий
10.3 Пересмотр Политики осуществляется рабочей группой и утверждается на Ученом совете Университета.

Лист ознакомления

ФИО	Дата получения копии	Роспись	Дата изъятия копии	Роспись