Утверждаю
Президент – ректор
АО «Казахский университет технологии и бизнеса»
д.т.н., профессор
_____ Байбеков С.Н.
«28» февраля 2023 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АО «КАЗАХСКИЙ УНИВЕРСИТЕТ ТЕХНОЛОГИИ И БИЗНЕСА»

Астана - 2023

ПРЕДИСЛОВИЕ

1 РАЗРАБОТАНО И ВНЕСЕНО Рабочей группой (РГ) совместно с отделом технического обеспечения и цифровизации

Руководитель РГ: Проректор по учебно-методической работе, PhD., Жамангарин Д.С.

Председатель РК: Проректор по учебно-методической работе, PhD., Жамангарин Д.С.

2 УТВЕРЖДЕНО И ВВЕДЕНО В ДЕЙСТВИЕ решением Ученого Совета №_7_ протокола, от «_28_» _февраля_ 2023 г.

3 РАЗРАБОТЧИК: отделом технического обеспечения и цифровизации

4 ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 3 года

5 ВВЕДЕНО ВПЕРВЫЕ

СОДЕРЖАНИЕ

1 ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Политика информационной безопасности (далее – Политика) Акционерное общество «Казахский университет технологии и бизнеса» (далее – АО «КазУТБ») определяет систему взглядов на проблему обеспечения информационной безопасности (далее – ИБ). Представляет собой систематизированное изложение высокоуровневых целей и задач защиты, которыми необходимо руководствоваться в своей деятельности, а также основных принципов построения системы управления информационной безопасностью (далее – СУИБ) АО «КазУТБ».

Обеспечение информационной безопасности – необходимое условие для успешного осуществления уставной деятельности университета. Обеспечение информационной безопасности включает в себя любую деятельность, направленную на защиту информационных ресурсов и/или поддерживающей инфраструктуры. Политика охватывает все автоматизированные и телекоммуникационные системы, владельцем и пользователем которых является АО «КазУТБ».

Реализация Политики должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищённости информационных ресурсов не только с помощью отдельного средства, но и с помощью их простой совокупности. Необходимо их системное, согласованное между собой применение, а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищённом исполнении при оптимальном соотношении технических и организационных мероприятий

2 НОРМАТИВНЫЕ ССЫЛКИ

№	Наименование документов	Сведения об утверждении (№, дата)	Изменения и дополнения в нормативный документ (№, дата)
1	Закон РК «Об образовании»	№ 319-III от 27 июля 2007 года	с изменениями и дополнениями 26.02.2023 г.
3	Об утверждении государственных общеобязательных стандартов высшего и послевузовского образования	Приказ МНиВО РК №2 от 20.07.2022 года	Приказ МНиВО РК №66 от 20.02.2023 г.
4	Об утверждении Правил организации учебного процесса по кредитной технологии обучения	Приказ МОН РК №152 от 20 апреля 2011года	с изменениями и дополнениями №79 от 23.09.2022 г.
5	Об утверждении Типовых правил деятельности организаций высшего и (или) послевузовского образования	Приказ МОН РК №595 от 31 октября 2018 года	Приказ МНиВО №145 от 20.01.2023 г.

3 ОСНОВНЫЕ ТЕРМИНЫ, СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

3.1 Основные термины

Автоматизированная система	система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.
Авторизация	предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ.
Аутентификация	проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.
Безопасность информации	защищённость информации от её нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного её тиражирования.
Бизнес-процесс	последовательность технологически связанных операций по предоставлению продуктов, услуг и/или осуществлению конкретного вида деятельности Учреждения
Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения	субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом.
Документ	зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать.
Доступность информации	состояние, характеризуемое способностью ИС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.
Защита информации	деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию и средства доступа к ней.
Идентификация	присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.
Информационная безопасность (ИБ)	состояние защищённости интересов Учреждения.
Информационная система	совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
Информационный ресурс (актив)	всё, что имеет ценность и находится в распоряжении Учреждения.

Инцидент	непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).
Коммерческая тайна	конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.
Конфиденциальная информация	информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством.
Конфиденциальность информации	состояние защищённости информации, характеризуемое способностью ИС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.
Несанкционированный доступ	доступ к информации иди действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.
Политика	общие цели и указания, формально выраженные руководством.
Привилегии	это права доверенного объекта на совершение каких-либо действий по отношению к объектам системы.
Риск	сочетание вероятности события и его последствий.
Система управления информационной безопасностью (СУИБ)	часть общей системы управления, основанная на оценке рисков, предназначенная для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ.
Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения	субъект, в полном объёме реализующий полномочия владения, пользования, распоряжения указанными объектами.
События информационной безопасности	идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности.
Угроза	Опасность, предполагающая возможность потерь (ущерба).

Целостность информации	устойчивость информации к несанкционированному доступу или случайному воздействию на неё в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации

4 СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

Сокращение	Полное наименование
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ГБУ	Государственное бюджетное учреждение
ИБ	Информационная безопасность
ИР	Информационный ресурс
ИС	Информационная система
ИТ	Информационные технологии
НСД	Несанкционированный доступ
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СУИБ	Система управления информационной безопасностью

5 ОТВЕТСТВЕННОСТЬ И ПОЛНОМОЧИЯ

5.1 Настоящая Политика разработана на основе требований законодательства Республики Казахстан, накопленного в АО «КазУТБ» опыта в области обеспечения ИБ, интересов и целей Учреждения.

5.2 Настоящая Политика утверждается решением Ученого совета АО «КазУТБ» и вводится в действие со дня утверждения.

5.3 Выполнение требований Политики контролируют проректор по НРиВС, руководитель ОТОиЦ, руководитель ЦОС, деканы факультетов и заведующие кафедрами.

5.4 Изменения к Политике разрабатываются по результатам его применения в деятельности АО «КазУТБ» или при изменении нормативных актов, регулирующих образовательную деятельность в Республике Казахстан, Устава АО «КазУТБ» и стратегии.

6 ЦЕЛЬ

6.1 Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация рисков ИБ.

6.2 Для достижения основной цели необходимо обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз ИБ;
- создание механизма оперативного реагирования на угрозы ИБ;
- предотвращение и/или снижение ущерба от реализации угроз ИБ;
- защита от вмешательства в процесс функционирования ИС посторонних лиц;

- соответствие требованиям законодательства, нормативно- методических документов и договорным обязательствам в части ИБ;
- обеспечение непрерывности критических бизнес-процессов;
- достижение адекватности мер по защите от угроз ИБ;
- выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников;
- повышение деловой репутации и корпоративной культуры.

7 ОБЛАСТЬ ДЕЙСТВИЯ

7.1 Настоящая Политика распространяется на все бизнес-процессы АО «КазУТБ» и обязательна для применения всеми сотрудниками и руководством АО «КазУТБ», а также пользователями его информационных ресурсов.

7.2 Настоящая политика распространяется на информационные системы учреждения. Лица, осуществляющие разработку внутренних документов АО «КазУТБ», регламентирующих вопросы информационной безопасности, обязаны руководствоваться настоящей Политикой.

7.3 Настоящая Политика является внутренним нормативным документом по ИБ первого уровня. Документы второго уровня – инструкции, порядки, регламенты и прочие документы, описывающие действия сотрудников АО «КазУТБ» по реализации документов первого и второго уровня. Документы третьего уровня – отчётные документы о выполнении требований документов верхних уровней.

8 ОТВЕТСТВЕННОСТЬ ЗА ОБЕСПЕЧЕНИЕ ИБ

8.1 Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности в АО «КазУТБ» функции обеспечения ИБ возложены на Центр информационных технологий (ЦИТ). На это подразделение возлагается решение следующих основных задач:

- проведение в жизнь Политики ИБ;
- определение требований к защите информации;
- организация мероприятий и координация работ всех подразделений по вопросам комплексной защиты информации;
- контроль и оценка эффективности принятых мер и применяемых средств защиты;
- оказание методической помощи сотрудникам в вопросах обеспечения информационной безопасности;
- регулярная оценка и управление рисками информационной безопасности в соответствии с установленными процедурами в области управления рисками;
- выбор и внедрение средств защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения СУИБ;
- обеспечение минимально-необходимого доступа к информационным ресурсам, основываясь на требованиях бизнес-процессов;
- информирование, обучение и повышение квалификации работников Учреждения в сфере информационной безопасности;
- расследования инцидентов информационной безопасности;
- сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности;

- обеспечение необходимого уровня отказоустойчивости ИТ-сервисов и доступности данных для подразделений.

Для решения задач, возложенных на ЦИТ, его сотрудники имеют следующие права:

- определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей информационной системы в указанной области;
- получать информацию от пользователей информационных систем по любым аспектам применения информационных технологий;
- участвовать в проработке технических решений по вопросам обеспечения безопасности информации при проектировании и разработке новых информационных технологий;
- участвовать в испытаниях разработанных информационных технологий по вопросам оценки качества реализации требований по обеспечению безопасности информации;
- контролировать деятельность пользователей по вопросам обеспечения ИБ;
- готовить предложения руководству по обеспечению требований ИБ.

9 ОБЪЕКТ ЗАЩИТЫ

9.1 В АО «КазУТБ» должны быть выявлены и оценены с точки зрения их важности все информационные ресурсы. Для всех ценных ресурсов должен быть составлен реестр (перечень). Благодаря информации о ресурсах Учреждения реализуется защита информации, степень которой соразмерна ценности и важности ресурсов.

9.2 В ИС АО «КазУТБ» присутствуют следующие типы ресурсов:

- информационные ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой деятельности АО «КазУТБ»;
- открыто распространяемая информация, необходимая для работы АО «КазУТБ», независимо от формы и вида её представления;
- информационная инфраструктура, включая системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

9.3 Для каждого ресурса должен быть назначен владелец, который отвечает за соответствующую классификацию информации и ресурсов, связанных со средствами обработки информации, а также за назначение и периодическую проверку прав доступа и категорий, определённых политиками управления доступа.

9.4 В учреждении должны быть определены требования к безопасности путём методической оценки рисков. Оценки рисков должны выявить, определить количество и расположить по приоритетам риски в соответствии с критериями принятия рисков и бизнес-целями учреждения. Результаты оценки должны определять соответствующую реакцию руководства, приоритеты управления рисками ИБ и набор механизмов контроля для защиты от этих рисков.

9.5 Оценка рисков предполагает системное сочетание анализа рисков и оценивания рисков. Кроме того, оценка рисков и выбор механизмов контроля должны производиться периодически, чтобы:

- учесть изменения бизнес-требований и приоритетов;
- принять во внимание новые угрозы и уязвимости;

- убедиться в том, что реализованные средства сохранили свою эффективность.

9.6 Перед обработкой каждого риска АО «КазУТБ» должно выбрать критерии для определения возможности принятия этого риска. Риск может быть принят, если его величина достаточно мала и стоимость обработки нерентабельна для АО «КазУТБ».

Для каждого из оцененных рисков должно приниматься одно из решений по его обработке:

- применение соответствующих механизмов контроля для уменьшения величины риска до приемлемого уровня;
- сознательное и объективное принятие риска, если он точно удовлетворяет Политике АО «КазУТБ» и критериям принятия рисков;
- уклонение от риска путём недопущения действий, могущих быть его причиной;
- передача рисков другой стороне (аутсорсинг, страхование и т.п.).

10 ОТВЕТСТВЕННОСТЬ РУКОВОДСТВА

10.1 Руководство АО «КазУТБ» должно требовать от всех сотрудников, подрядчиков и пользователей сторонних организаций принятия мер безопасности в соответствии с установленными в АО «КазУТБ» политиками и процедурами. Уполномоченные руководством АО «КазУТБ» сотрудники имеют право в установленном порядке, без уведомления пользователей, производить проверки:

- Выполнения действующих инструкций по вопросам ИБ;
- Данных, находящихся на носителях информации;
- Порядка использования сотрудниками информационных ресурсов;
- Содержания служебной переписки.

11 ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

11.1 Средства обработки информации, поддерживающие критически важные и уязвимые ресурсы Учреждения, должны быть размещены в защищённых областях. Такими средствами являются: серверы, магистральное телекоммуникационное оборудование, телефонные станции, кроссовые панели, оборудование, обеспечивающее обработку и хранение конфиденциальной информации. Защищённые области должны обеспечиваться соответствующими средствами контроля доступа, обеспечивающим возможность доступа только авторизованного персонала. Запрещается приём посетителей в помещениях, когда осуществляется обработка информации ограниченного доступа. Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами, металлическими шкафами или шкафами, оборудованными замком. Помещения должны быть обеспечены средствами уничтожения документов. Места доступа, через которые неавторизованные лица могут попасть в помещения АО «КазУТБ», должны контролироваться и, если это возможно, должны быть изолированы от средств обработки информации с целью предотвращения несанкционированного доступа. Все вспомогательные службы, такие как электропитание, водоснабжение, канализация, отопление, вентиляция и кондиционирование воздуха должны обеспечивать гарантированную и устойчивую работоспособность компонентов ИС АО «КазУТБ».

12 КОНТРОЛЬ ДОСТУПА

12.1 Основными пользователями информации в информационной системе

АО «КазУТБ» являются сотрудники структурных подразделений. Уровень полномочий каждого пользователя определяется индивидуально. Каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями. Допуск пользователей к работе с информационными ресурсами должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться в установленном порядке, согласно регламента предоставления доступа пользователей. Каждому пользователю, допущенному к работе с конкретным информационным активом АО «КазУТБ», должно быть сопоставлено персональное уникальное имя (учётная запись пользователя), под которым он будет регистрироваться и работать с ИА. В случае производственной необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имён (учётных записей). Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе). В общем случае запрещено создавать и использовать общую пользовательскую учётную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учётной записи должно сопровождаться отметкой в журнале учёта машинного времени, которая должна однозначно идентифицировать текущего владельца учётной записи в каждый момент времени. Одновременное использование одной общей пользовательской учётной записи разными пользователями запрещено.

12.2 Регистрируемые учётные записи подразделяются на:

- Пользовательские – предназначенные для аутентификации пользователей ИР Учреждения;
- Системные – используемые для нужд операционной системы;
- Служебные – предназначенные для функционирования отдельных процессов или приложений.

Системные учётные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему. Служебные учётные записи используются только для запуска и работы сервисов или приложений. Использование системных или служебных учётных записей для регистрации пользователей в системе категорически запрещено.

12.3 Процедуры регистрации и блокирования учётных записей пользователей должны применяться с соблюдением следующих правил:

- использование уникальных идентификаторов (ID) пользователей для однозначного определения и сопоставления личности с совершёнными ей действиями;
- использование групповых ID разрешать только в случае, если это необходимо для выполнения задачи;
- предоставление и блокирование прав должны быть санкционированы и документированы;
- предоставление прав доступа к ИР, только после согласования с владельцем данного ИР;
- регистрация и блокирование учётных записей допускается с отдельного разрешения руководства Учреждения;
- уровень предоставленных полномочий должен соответствовать производственной

необходимости и настоящей Политике и не ставить под угрозу разграничение режимов работы;

- согласование изменения прав доступа с отделом ИС СМТ;
- документальная фиксация назначенных пользователю прав доступа;
- ознакомление пользователей под подпись с письменными документами, в которых регламентируются их права доступа;
- предоставление доступа с момента завершения процедуры регистрации;
- обеспечение создания и поддержания формального списка всех пользователей, зарегистрированных для работы с ИР или сервисом;
- немедленное удаление или блокирование прав доступа пользователей, сменивших должность, форму занятости или уволившихся из АО «КазУТБ»;
- аудит ID и учетных записей пользователей на наличие неиспользуемых, их удаление и блокировка;
- обеспечение того, чтобы лишние ID пользователей не были доступны другим пользователям;
- обеспечить возможность предоставления пользователям доступа в соответствии с их должностями, основанными на производственных требованиях, путем суммирования некоторого числа прав доступа в типовые профили доступа пользователей.

13 УПРАВЛЕНИЕ ПРИВИЛЕГИЯМИ

13.1 Доступ сотрудника к информационным ресурсам АО «КазУТБ» должен быть санкционирован руководителем структурного подразделения, в котором числится согласно штатному расписанию данный сотрудник, и владельцами соответствующих информационных ресурсов. Управление доступом осуществляется в соответствии с установленными процедурами. Наделение привилегиями и их использование должно быть строго ограниченным и управляемым. Контроль и периодический пересмотр прав доступа пользователей к информационным ресурсам АО «КазУТБ» осуществляется в процессе аудита ИБ в соответствии с Правилами аудита ИБ и установленными процедурами.

13.2 Управление паролями

Пароли – средство проверки личности пользователя для доступа к ИС или сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю.

Предоставление паролей должно контролироваться посредством официальной процедуры, отвечающей следующим требованиям:

- все пользователи должны быть ознакомлены под роспись с требованием сохранения в тайне личных и групповых паролей;
- при наличии возможности, необходимо настроить систему таким образом, чтобы при первом входе пользователя с назначенным ему временным паролем система сразу же требовала его сменить;
- временные пароли должны назначаться пользователю только после его идентификации;
- необходимо избегать передачи паролей с использованием третьих лиц или незашифрованной электронной почтой;
- временные пароли не должны быть угадываемыми и повторяющимися от пользователя к пользователю;
- пользователь должен подтвердить получение пароля;
- пароли должны храниться в электронном виде только в защищенной форме;

- назначенные производителем ПО пароли должны быть изменены сразу после завершения инсталляции;
- необходимо установить требования к длине пароля, набору символов и числу попыток ввода;
- необходимо изменять пароля пользователя не реже одного раза в 90 дней.

При необходимости можно рассмотреть возможность использования других технологий идентификации и аутентификации пользователей, в частности, биометрических технологий, проверки подписи и аппаратных средств (смарт-карты, e-Token/ruToken, чипы и т.п.).

13.3 Контроль прав доступа

Чтобы обеспечить эффективный контроль доступа необходимо ввести официальный процесс регулярной проверки прав доступа пользователей, отвечающий следующим требованиям:

- права доступа пользователей должны проверяться через регулярные интервалы (не реже одного раза в полгода), а также после внесения каких-либо изменений в ИС;
- права доступа пользователей должны проверяться и переназначаться при изменении их должностных обязанностей в АО «КазУТБ», а также при переходе с одной работы на другую в пределах Учреждения;
- проверка прав пользователей, имеющих особые привилегии для доступа в систему, должна проводиться чаще (не реже одного раза в 3 месяца);
- необходимо регулярно проверять адекватность назначенных привилегий, во избежание получения кем-либо из пользователей излишних прав;
- изменение привилегированных учетных записей должно протоколироваться.

13.4 Использование паролей

Идентификатор и пароль пользователя в ИС являются учётными данными, на основании которых сотруднику АО «КазУТБ» предоставляются права доступа, протоколируются производимые им в системе действия и обеспечивается режим конфиденциальности, обрабатываемой (создаваемой, передаваемой и хранимой) сотрудником информации. Не допускается использование различными пользователями одних и тех же учётных данных. Первоначальное значение пароля учетной записи пользователя устанавливает Администратор безопасности.

Личные пароли устанавливаются первый раз сотрудниками отдела ЦИТ. После первого входа в систему и в дальнейшем пароли выбираются пользователями автоматизированной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля должны присутствовать три из четырёх видов символов:
- буквы в верхнем регистре;
- буквы в нижнем регистре;
- цифры;
- специальные символы (! @ # $ % ^ & * ( ) - _ + = ~ [ ] { } | \ : ; ' " < > , . ? /);
- пароль не должен содержать легко вычисляемые сочетания символов, например,
- имена, фамилии, номера телефонов, даты;
- последовательно расположенные на клавиатуре символы («12345678»,
- «QWERTY», и т.д.);
- общепринятые сокращения («USER», «TEST» и т.п.);
- повседневно используемое слово, например, имена или фамилии друзей, коллег, актёров или сказочных персонажей, клички животных;

- компьютерный термин, команда, наименование компаний, web сайтов, аппаратного или программного обеспечения;
- что-либо из вышеперечисленного в обратном написании;
- что-либо из вышеперечисленного с добавлением цифр в начале или конце;
- при смене пароля значение нового должно отличаться от предыдущего не менее чем в 4 позициях;
- для различных ИС необходимо устанавливать собственные, отличающиеся пароли.

14 СОТРУДНИКУ ЗАПРЕЩАЕТСЯ

14.1 Сообщать свой пароль кому-либо;

14.2 Указывать пароль в сообщениях электронной почты;

14.3 Хранить пароли, записанные на бумаге, в легко доступном месте;

14.4 Использовать тот же самый пароль, что и для других систем (например, домашний интернет провайдер, бесплатная электронная почта, форумы и т.п.);

14.5 Использовать один и тот же пароль для доступа к различным корпоративным ИС.

14.6 Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место пользователь обязан заблокировать компьютер (используя комбинации Win + «L» или Ctrl + Alt + Delete → «Блокировать компьютер»).

14.7 Сотрудник обязан:

- в случае подозрения на то, что пароль стал кому-либо известен, поменять пароль и сообщить о факте компрометации сотруднику отдела ИС СМТ;
- немедленно сообщить сотруднику отдела ЦИТв случае получения от кого-либо просьбы сообщить пароль;
- менять пароль каждые 90 дней;
- менять пароль по требованию Администратора ИБ.

14.8 Учреждение оставляет за собой право:

- осуществлять периодическую проверку стойкости паролей пользователей, используемых сотрудниками для доступа к ИС;
- принимать меры дисциплинарного характера к сотрудникам, нарушающим положения настоящей политики.

14.9 Сотрудники Учреждения обязаны:

- сохранять известные им пароли в тайне;
- закрывать активные сеансы по завершении работы, если только их нельзя защитить подходящим блокирующим механизмом, например, защищённый паролем хранитель экрана;
- по завершении сеанса выходить из системы у универсальных ЭВМ, серверов и офисных ПК.

14.10 Запрещается вести запись паролей (например, на бумаге, в программном файле или в карманном устройстве), за исключением случаев, когда запись может храниться безопасно, а метод хранения был утверждён. Документы и носители с конфиденциальной информацией должны убираться в запираемые места (сейфы, шкафы и т.п.), особенно при уходе с рабочего места. Компьютеры и терминалы должны быть оставлены в состоянии выполненного выхода из системы, когда они находятся без присмотра. Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место пользователь обязан заблокировать компьютер (используя комбинации Win + «L» или Ctrl + Alt + Delete «Блокировать компьютер»). Документы, содержащие конфиденциальную информацию, должны изыматься из печатающих устройств немедленно. В конце рабочего дня сотрудник должен привести в порядок письменный стол и убрать все офисные документы в запираемый

шкаф или сейф. Для утилизации конфиденциальных документов, должны использоваться уничтожители бумаги.

14.11 По окончании рабочего дня и в случае длительного отсутствия на рабочем месте необходимо запирать на замок все шкафы и сейфы.

15 ОБЩИЕ ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

15.1 При работе с ПО руководствоваться нормативной документацией (руководством пользователя);

15.2 Обращаться в службу поддержки пользователей или к специалистам, назначенными ответственными за системное администрирование и информационную безопасность, по всем техническим вопросам, связанным с работой в корпоративной ИС (подключение к корпоративной ИС/домену, инсталляция и настройка ПО, удаление вирусов, предоставление доступа в сеть Интернет и к внутренним сетевым ресурсам, ремонт и техническое обслуживание и т.п.), а также за необходимой методологической/консультационной помощью по вопросам применения технических и программных средств корпоративной ИС;

15.3 Знать признаки правильного функционирования установленных программных продуктов и средств защиты информации;

15.4 Минимизировать вывод на печать обрабатываемой информации.

15.5 Пользователю запрещено производить несанкционированное распространение справочной информации, которая становится доступна при подключении к корпоративной ИС АО «КазУТБ». Запрещено незаконное хранение на жестких дисках информации, являющейся объектом авторского права (ПО, фотографии, музыкальные файлы, игры, и т.д.). Решение о приобретении и установке программного обеспечения, необходимого для реализации образовательных, финансовых, административно-хозяйственных и других задач принимает руководитель ответственного отдела. Документы, подтверждающие покупку программного обеспечения, хранятся в бухгалтерии на протяжении всего времени использования лицензии, копии указанных документов вместе с лицензионными соглашениями на ПО, ключами защиты ПО и дистрибутивами хранятся в ЦИТ.

15.6 Самостоятельная установка программного обеспечения на АРМ запрещена. Установка и удаление любого программного обеспечения производится только сотрудниками отдела ИС СМТ.

15.7 В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться в отдел ЦИТ.

15.8 Сотрудники отдела ЦИТ имеют право осуществлять контроль над установленным на компьютере программным обеспечением, и принимать меры по ограничению возможностей несанкционированной установки программ.

15.9 Передача документов внутри АО «КазУТБ» производится только посредством общих папок, а также средствами электронной почты.

15.10 При работе в ИС АО «КазУТБ» сотрудник обязан:

- знать и выполнять требования внутренних организационно-распорядительных документов АО «КазУТБ»;
- использовать ИС и АРМ АО «КазУТБ» исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел ЦИТ о любых фактах нарушения требований ИБ;
- ставить в известность отдел ЦИТ о любых фактах сбоев ПО, некорректного завершения значимых операций, а также повреждения технических средств;

- незамедлительно выполнять предписания отдела ЦИТ АО «КазУТБ»;
- предоставлять АРМ сотрудникам отдела ЦИТ для контроля.
- при необходимости прекращения работы на некоторое время корректно закрывать все активные задачи, блокировать АРМ;
- в случае необходимости продолжения работы по окончании рабочего дня проинформировать об этом отдел ИС СМТ.

15.11 При использовании ИС АО «КазУТБ» запрещено:

- использовать АРМ и ИС в личных целях;
- отключать средства управления и средства защиты, установленные на рабочей станции;
- передавать:
- конфиденциальную информацию за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с отделом ИС СМТ;
- информацию, файлы или ПО, способные нарушить или ограничить функциональность любых программных и аппаратных средств, а также ссылки на вышеуказанные объекты;
- угрожающую, клеветническую, непристойную информацию;
- самовольно вносить изменения в конструкцию, конфигурацию, размещение АРМ и других узлов ИС АО «КазУТБ»;
- предоставлять сотрудникам Учреждения (за исключением администраторов ИС и ИБ) и третьим лицам доступ к своему АРМ;
- запускать на АРМ ПО, не входящее в Реестр разрешенного к использованию ПО;
- защищать информацию, способами, не согласованными с отделом ЦИТ заранее;
- самостоятельно подключать рабочую станцию и прочие технические средства к корпоративной ИС Учреждения;
- осуществлять поиск средств и путей повреждения, уничтожения технических средств и ресурсов ИС или осуществлять попытки несанкционированного доступа к ним;
- использовать для выполнения служебных обязанностей локальные (не доменные) учетные записи АРМ.

15.12 Информация о посещаемых ресурсах ИС протоколируется и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Руководству Учреждения. Все электронные сообщения и документы в электронном виде, передаваемые посредством ИС Учреждения подлежат обязательной проверке на отсутствие вредоносного ПО.

16 ИСПОЛЬЗОВАНИЕ РЕСУРСОВ ЛОКАЛЬНОЙ СЕТИ

16.1 Для выполнения своих служебных обязанностей каждый сотрудник обеспечивается доступом к соответствующим информационным ресурсам. Информационными ресурсами являются каталоги и файлы, хранящиеся на дисках серверов Учреждения, базы данных, электронная почта. Основными рабочими каталогами являются личные каталоги сотрудников и каталоги подразделений, созданные в соответствии с особенностями их работы. Доступ сотрудников к ресурсам сети осуществляется согласно матрицы доступа. Временное расширение прав доступа осуществляется отделом ЦИТ АО «КазУТБ» в соответствии с Порядком предоставления (изменения) полномочий пользователя.

17 ОБРАБОТКА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

17.1 При обработке конфиденциальной информации сотрудники обязаны:

- знать и выполнять требования Инструкции по работе с конфиденциальной информацией;
- при необходимости размещать конфиденциальную информацию на открытом ресурсе корпоративной сети Учреждения применять средства защиты от неавторизованного доступа;
- размещать экран монитора таким образом, чтобы исключить просмотр обрабатываемой информации посторонними лицами;
- не отправлять на печать конфиденциальные документы, если отсутствует возможность контроля вывода на печать и изъятия отпечатанных документов из принтера сразу по окончании печати;
- обязательно проверять адреса получателей электронной почты на предмет правильности их выбора;
- не запускать исполняемые файлы на съемных накопителях, полученные не из доверенного источника;
- не передавать конфиденциальную информацию по открытым каналам связи, кроме сетей корпоративной ИС;
- не оставлять без личного присмотра на рабочем месте или где бы то ни было электронные носители информации (CD/DVD – диски, Flash – устройства и пр.), а также распечатки из принтера или бумажные копии документов, содержащие конфиденциальную информацию.

17.2 Корпоративная электронная почта АО «КазУТБ» предназначена исключительно для использования в служебных целях. Функционирование электронной почты обеспечивается оборудованием, каналами связи и иными ресурсами, принадлежащими АО «КазУТБ». Все почтовые сообщения, переданные или принятые с использованием корпоративной электронной почты принадлежат АО «КазУТБ» и являются неотъемлемой частью его производственного процесса.

17.2 Любые сообщения корпоративной электронной почты могут быть прочитаны, использованы в интересах АО «КазУТБ» либо удалены уполномоченными сотрудниками Учреждения.

17.3 Пользователям корпоративной электронной почты Учреждения запрещено вести частную переписку с использованием средств корпоративной электронной почты АО «КазУТБ».

18 РАБОТА В СЕТИ

18.1 Доступ к сети Интернет предоставляется сотрудникам АО «КазУТБ» в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

18.2 Для доступа сотрудников АО «КазУТБ» к сети Интернет допускается применение ПО, входящего в Реестр разрешённого к использованию ПО.

18.3 При использовании сети Интернет необходимо:

- соблюдать требования настоящей Политики;
- использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел ТОиЦ любых фактах нарушения требований

настоящей Политики;

18.4 При использовании сети Интернет запрещено:

- использовать предоставленный АО «КазУТБ» доступ в сеть Интернет в личных целях;
- использовать несанкционированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет;
- Совершатьлюбыедействия, направленные на нарушение нормального функционирования элементов ИС АО «КазУТБ»;
- Публиковать, загружать и распространять материалы содержащие: конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, за исключением случаев, когда это входит в должностные обязанности и способ передачи является безопасным, согласованным с отделом ИС СМТ; угрожающую, клеветническую, непристойную информацию;
- вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также ссылки на него;
- фальсифицировать свой IP- адрес, а также прочую служебную информацию.

18.5 АО «КазУТБ» оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены законодательством.

18.6 Блокирование и ограничение доступа пользователей к Интернет-ресурсам осуществляется на основе Регламента применения категорий Интернет-ресурсов.
Информация о посещаемых сотрудниками АО «КазУТБ» Интернет-ресурсах протоколируется для последующего анализа и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Руководству Учреждения для контроля. Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

18.7 При использовании предоставленных АО «КазУТБ» мобильных устройств и носителей информации, сотрудник обязан:

- соблюдать требования настоящей Политики;
- использовать мобильные устройства и носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел ЦИТ о любых фактах нарушения требований настоящей Политики;
- эксплуатировать и транспортировать мобильные устройства и носители информации в соответствии с требованиями производителей;
- обеспечивать физическую безопасность мобильных устройств и носителей информации всеми разумными способами;
- извещать о фактах утраты (кражи) мобильных устройств и носителей информации.

19 ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО

19.1 Отдел ЦИТ регулярно проверяет сетевые ресурсы АО «КазУТБ» антивирусным программным обеспечением и обеспечивает защиту входящей электронной почты от проникновения вирусов и другого вредоносного ПО.

19.2 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных,

пропадание файлов, частое появление о системных ошибках, увеличение исходящего/входящего трафика и т.п.) сотрудник АО «КазУТБ» должен незамедлительно оповестить об этом отдел ТОиЦ. После чего администратор ИБ должен провести внеочередную полную проверку на вирусы рабочей станции пользователя, проверив, в первую очередь, работоспособность антивирусного ПО.

19.3 В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения заражения своего руководителя и отдел ИС СМТ, а также владельца файла и смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

19.4 Для предупреждения вирусного заражения рекомендуется:

- никогда не открывать файлы и не выполнять макросы, полученные в почтовых сообщениях от неизвестного или подозрительного отправителя. Удалять подозрительные вложения, не открывая их, и очищать корзину, где хранятся удаленные сообщения;
- удалять спам, рекламу и другие бесполезные сообщения;
- никогда не загружать файлы и программное обеспечение из подозрительных или неизвестных источников;
- периодически резервировать важные данные и системную конфигурацию, хранить резервные копии в безопасном месте.

20 СОБЛЮДЕНИЕ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА

20.1 Все значимые требования, установленные действующим законодательством, подзаконными актами и договорными отношениями, а также подход АО «КазУТБ» к обеспечению соответствия этим требованиям должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии. Необходимо соблюдение регламентированного процесса, предупреждающего нарушение целостности, достоверности и конфиденциальности ИР, содержащих персональные данные, начиная от стадии сбора и ввода данных до их хранения. Персональные данные конкретного сотрудника и процесс их обработки должен быть открытым для этого сотрудника. В АО «КазУТБ» должны быть внедрены соответствующие процедуры для обеспечения соблюдения законодательных ограничений, подзаконных актов и контрактных обязательств по использованию материалов, охраняемых авторским правом, а также по использованию лицензионного ПО. Важная документация АО «КазУТБ» должна быть защищена от утери, уничтожения и фальсификации в соответствии с требованиями законодательства, подзаконных актов, контрактных обязательств и бизнес-требований. Система хранения и обработки должна обеспечивать чёткую идентификацию записей и их периода хранения в соответствии с требованиями законов и нормативных актов. Эта система должна иметь возможность уничтожения записей по истечении периода хранения, если эти записи больше не требуются АО «КазУТБ». Криптографические средства должны использоваться в соответствии со всеми имеющимися соглашениями, законодательными и нормативными актами.

21 АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

21.1 АО «КазУТБ» должно проводить внутренние проверки СУИБ через

запланированные интервалы времени.

21.2 Основные цели проведения таких проверок:

- оценка текущего уровня защищённости ИС;
- выявление и локализация уязвимостей в системе защиты ИС;
- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ИР;
- оценка соответствия ИС требованиям настоящей Политики;
- выработка рекомендаций по совершенствованию СУИБ за счёт внедрения новых и повышения эффективности существующих мер защиты информации.

21.3 В число задач, решаемых при проведении проверок и аудитов СУИБ, входят:

- сбор и анализ исходных данных об организационной и функциональной структуре ИС, необходимых для оценки состояния ИБ;
- анализ существующей политики безопасности и других организационно-распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их разработке (или доработке);
- технико-экономическое обоснование механизмов безопасности;
- проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надёжности и безопасности ИС;
- разбор инцидентов ИБ и минимизация возможного ущерба от их проявления.

21.4 Руководство и сотрудники АО «КазУТБ» при проведении у них аудита СУИБ обязаны оказывать содействие аудиторам и предоставлять всю необходимую для проведения аудита информацию.

22 ОТВЕТСТВЕННОСТЬ

22.1 Руководитель отдела ТОиЦ АО «КазУТБ» определяет приоритетные направления деятельности в области обеспечения ИБ, меры по реализации настоящей Политики, утверждает списки объектов и сведений, подлежащих защите, а также осуществляет общее руководство обеспечением ИБ АО «КазУТБ». Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СУИБ АО «КазУТБ» лежит на руководстве отдела ТОиЦ. Все руководители несут прямую ответственность за реализацию Политики и её соблюдение персоналом в соответствующих подразделениях. Работники Учреждения несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности в отдел ТОиЦ.

22.2 В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность служебной информации, ставшей известной в силу выполнения своих обязанностей. Руководство АО «КазУТБ» регулярно проводит совещания, посвящённые проблемам обеспечения информационной безопасности с целью формирования чётких указаний по этому вопросу, осуществления контроля их выполнения, а также оказания административной поддержки инициативам по обеспечению ИБ. Нарушение требований нормативных актов АО «КазУТБ» по обеспечению ИБ является чрезвычайным происшествием и будет служить поводом и основанием для проведения служебного расследования.

23 КОНФИДЕНЦИАЛЬНОСТЬ

23.1 Настоящее Положение является внутренним нормативным документом АО «КазУТБ» и не подлежит представлению другим сторонам, кроме экспертов сертификационных органов при проведении сертификационного аудита, потребителей-партнеров с разрешения президент-ректора АО «КазУТБ».

24 СОГЛАСОВАНИЕ, ХРАНЕНИЕ И РАССЫЛКА

24.1 Ответственность за передачу утвержденного Положения (оригинал) на хранение несет ОТОиЦ.

24.2 Рассылка учтенных копий Положения осуществляется ООКиА.

24.3 Ответственность за хранение копий Положения несут руководители структурных подразделений.

25 ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ

25.1 Внесение изменений в Положение производится только по разрешению президент-ректора и обязательно оформляется документально за его подписью. Листы, изъятые из измененного варианта Положения, хранятся с документом о разрешении внесения изменений.

25.2 Выпускать извещения об изменении в переданное на хранение Положение имеет право только подразделение-разработчик.

Приложение А
(обязательно)

ЛИСТ СОГЛАСОВАНИЯ

Должность	Ф.И.О.	Дата	Подпись
Проректор по учебно-методической работе	Жамангарин Д.С.	22.02.2023г.	
Проректор по научной работе и внешним связям	Алтынбек С.А.	22.02.2023г.	
Проректор по воспитательной и социальной работе	Барлыков Е.К.	22.02.2023г.	
Главный бухгалтер	Шағырбай М.А.	22.02.2023г.	
Руководитель юридического отдела	Аяпов М.У.	22.02.2023г.	
Руководитель отдела обеспечения качества и аккредитации	Нурбаева М.З.	22.02.2023г.	
Руководитель учебно-методического отдела	Баядилова Б.М.	22.02.2023г.	
Руководитель отдела управления персоналом	Кабильдина З.З.	22.02.2023г.	

Приложение Б
(обязательно)

ЛИСТ ОЗНАКОМЛЕНИЯ

Должность	Ф.И.О.	Дата	Подпись

Приложение В
(обязательно)

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ изм.	№ извещ.	Номер листов (страниц)				Всего листов	Дата внесения изм-ий	Ф.И.О., осущ-го внесение изм-ий	Подпись вносившего изм-ия
		изм-ны	замен-ных	новых	аннул-ных				

Приложение Г
(обязательно)

ЛИСТ УЧЕТА ПЕРИОДИЧЕСКИХ ПРОВЕРОК

Дата проверки	**Ф.И.О. лица, выполнившего проверку**	**Подпись выполнившего проверку**	**Формулировка замечаний**