КЕНЖЕҒАЛИ САҒАДИЕВ АТЫНДАҒЫ ХАЛЫҚАРАЛЫҚ БИЗНЕС УНИВЕРСИТЕТІ

УНИВЕРСИТЕТ МЕЖДУНАРОДНОГО БИЗНЕСА ИМЕНИ КЕНЖЕГАЛИ САГАДИЕВА

УТВЕРЖДЕНО
Ученым Советом УМБ
имени Кенжегали Сагадиева
Протокол № 7 от 20.01.2023
Председатель Махметова А.М.

ПАРОЛЬНАЯ ПОЛИТИКА

ТОО «УНИВЕРСИТЕТ МЕЖДУНАРОДНОГО БИЗНЕСА ИМЕНИ КЕНЖЕГАЛИ САГАДИЕВА»

ИЗДАНИЕ 1

Введено в действие с даты утверждения

Алматы, 2023

Оглавление

Stu

Паспорт документа

Тип документа	Организационная документация
Наименование документа	Парольная политика УМБ им. Кенжегали Сагадиева
Цель документа	Политика определяет требования обеспечения информационной безопасности и регулирует процессы идентификации и аутентификации пользователя при работе с ИС Университета им. Кенжегали Сагадиева
Разработка	Директором ДИТ
Согласование	Проректора по направлениям Директор ДАВ Декан факультета базового высшего образования Директор Graduate School of Business Директор Департамента человеческим по ресурсам и документации Руководитель Центра Обеспечения Качества Юрисконсульт
Утверждение	Председателем УС
Исполнители документа	Работники ДИТ/ДЦТ, структурные подразделения УМБ, преподаватели и студенты УМБ
Контроль за исполнением	Первый руководитель УМБ
Приложения к документу	Нет
Нормативные ссылки	Политика разработан в соответствии с требованиями законодательства Республики Казахстан, Устава, а также внутренних нормативных и распорядительных документов ТОО «Университета международного бизнеса имени Кенжегали Сагадиева» 1. Закон Республики Казахстан «Об Образовании» *(с изменениями и дополнениями).* 2. Правила организации учебного процесса по кредитной технологии обучения, утвержденных приказом Министра образования и науки РК от 20.04.2011 № 152 *(с изменениями и дополнениями).*
Владелец оригинала	ДИТ

Лист согласования

Положение согласовано:

Проректор по науке
Нургалиева К. О. _____
«19» 01 2023 г.

Проректор по цифровизации
Мусабаев Н.Б. _____
«19» 01 2023 г.

Проректор по стратегии и социальному развитию:
Сабденалиев Б.А. _____
«19» 01 2023 г.

Директор ДАВ
Токина А.А. _____
«19» 01 2023 г.

Декан Факультета Базового Высшего Образования
Садыров Г.А. _____
«19» 01 2023 г.

Директор Graduate School of Business
Каликов М.А. _____
«19» 01 2023г.

Ио Директора Департамента человеческим по ресурсам и документации
Сихимбаева Г.М. _____
«19» 01 2023 г.

Руководитель Центра Обеспечения Качества
Кабдесов К.Т. _____
«19» 01 2023 г.

Юрисконсульт
Алибекова А.К. _____
«19» 01 2023 г.

Разработано:

Директор ДИТ
Фомичев С.В. _____
«19» 01 2023 г.

Редакция и оформление:

Project менеджер ЦОК
Дузбаева Р.М. _____
«19» 01 2023 г.

1. Общие положения

1.1 Настоящая Парольная политика ТОО «Университета международного бизнеса имени Кенжегали Сагадиева» (далее – Политика) разработана в соответствии с требованиями законодательства Республики Казахстан, Устава, внутренних нормативных и распорядительных документов ТОО «Университета международного бизнеса имени Кенжегали Сагадиева» (далее – Университета или УМБ).

1.2 Настоящая Политика является внутренним нормативным документом, определяющим требования обеспечения информационной безопасности Университета.

1.3 Настоящая Политика разработана в целях развития информационной безопасности Университета, в соответствии с международными стандартами и устанавливает единый порядок организационно-технического обеспечения процессов назначения, использования, смены и прекращения действия паролей для Информационных систем Университета.

1.4 Политика регулирует процессы идентификации и аутентификации пользователя при работе с информационными системами Университета.

1.5 Политика базируется на приоритетных направлениях по развитию Университета. Реализация требований и положений Политики направлена на обеспечение безопасности и непрерывности бизнес-процессов Университета.

1.6 Требования Политики распространяются на всех работников, преподавателей и студентов Университета.

1.7 Основные понятия, термины и сокращения, используемые в Политике:

1) **Лог-файлы сервера** — специальные файлы, в которых протоколируются определённые действия пользователя или программы на сервере;

2) **ИС** – информационные системы;

3) **Пользователь** – любой сотрудник, преподаватель и студент Университета

2. Требования безопасности и реализация парольной политики

2.1 В целях соблюдения требований информационной безопасности Университета, а также соблюдения принципа персональной ответственности за свои действия, каждому пользователю, присваивается персональное уникальное имя с паролем (далее по тексту - учетная запись).

2.2 Общие требования к содержимому паролей, их длине и остальным параметрам должны устанавливаться групповыми политиками домена (Active Directory), в частности:

1) пароль должен быть уникальным для каждого пользователя, тщательно продуманным и не быть простым словом или аббревиатурой, которое легко может быть подобрано;

2) пароль не должен быть коротким по количеству символов – длина пароля должна составлять не менее 8 (восьми) символов;

3) пароль должен содержать в себе буквы (заглавные и строчные - предпочтительно на латинице, цифры и специальные символы (%, $, @, &, *, #, ^ и т.п.);

4) пароль не должен повторяться – история паролей каждого пользователя должна сохраняться на сервере каждой ИС – не менее 5 (пять) паролей. При попытке ввода пароля, хранящегося в истории, должно всплывать информационное окно с предупреждающей надписью о повторяющемся пароле;

5) срок действия пароля должен быть ограничен - не более 90 (девяносто) календарных дней с предусмотренной функцией всплывающего ежедневно окна за 5 (пять) календарных дней до требуемой даты замены, которое содержит в себе сообщение предупреждающего/напоминающего характера о необходимости замены пароля;

6) рабочее место пользователя, не производящего никаких действий на компьютере, должно автоматически блокироваться операционной системой по истечении 15 (пятнадцать) минут;

7) количество неудачных попыток входа в операционную систему должно ограничиваться 5 (пять) попытками. В случае если количество неудачных попыток превысит указанный параметр, данная учетная запись должна блокироваться на 20 (двадцать) минут. Все случаи неверно введенных паролей, попытки несанкционированного подключения к системе и манипулирования учетными записями должны фиксироваться в системном журнале безопасности ИС с целью последующего анализа работником информационной безопасности ДИТ.

8) параметры сброса счетчика неудачных попыток аутентификации в домене должно быть установлено значение равным 20 (двадцать) минутам.

2.3 К ИС, администрируемым работниками ДИТ и ДЦТ, пароли к которым устанавливаются/изменяются вручную администраторами ИС, предъявляются следующие требования:

1) пароль должен быть уникальным для каждого администратора, тщательно продуманным и не быть простым словом или аббревиатурой, которое легко может быть подобрано;

2) пароль не должен быть коротким по количеству символов – длина пароля должна составлять не менее 10 (десять) символов;

3) пароль должен содержать в себе буквы (заглавные и строчные - предпочтительно на латинице, цифры и специальные символы (%, $, @, &, *, #, ^ и т.п.);

4) пароль не должен повторяться - история паролей должна сохраняться на сервере каждой ИС не менее 10 (десяти) паролей;

5) срок действия пароля должен быть ограничен – замена паролей должна проводиться не реже 1 раз в полгода, с передачей паролей в запечатанных конвертах на хранение директору ДИТ согласно пункту 16 настоящей Политики;

6) при увольнении или переводе на другую работу (не связанную с администрированием закрепленных ИС) администратором ИС должна быть произведена внеочередная смена паролей на ИС, администрируемых уволенным/переведенным работником, с передачей паролей в запечатанных конвертах на хранение Директору ДИТ согласно пункту 14 настоящей Политики;

7) рабочее место администратора ИС, не производящего никаких действий на компьютере, должно автоматически блокироваться операционной системой по истечении 7 (семь) минут

8) количество неудачных попыток входа в операционную систему должно ограничиваться 5 (пять) попытками. Все случаи неверно введенных паролей, попытки несанкционированного подключения к системе и манипулирования учетными записями должны фиксироваться в системном журнале безопасности ИС с целью последующего анализа.

2.4 Пароли для доступа к ресурсам ИС по умолчанию формируются пользователями и администраторами ИС самостоятельно, если иное не оговорено в

отдельных приказах, распоряжениях, требованиях сторонних программных продуктов.

2.5 При формировании паролей работникам запрещается:

1) использовать в качестве пароля легко вычисляемые сочетания (собственные имена, фамилии, имена детей, родственников, клички домашних животных, даты рождения, номер автомобиля, паспорта, телефона и т.д.) вне зависимости от регистра и раскладки клавиатуры (в т.ч. ввод на латинице и/или кириллице), которые возможно подобрать на основании имеющейся информации о пользователе;

2) использовать в качестве пароля набор символов, расположенных на клавиатуре рядом (подряд «qwerty@123», в обратном порядке «321@ytrewq» и т.д.);

3) вставлять пароли в тексты программ, записывать их в файлы, или подручные материалы (календари, стикеры и т.д.), доступные для общего доступа посторонних лиц, (например: обратной стороне клавиатуры, монитор и т.д.);

4) программно сохранять пароли, предлагаемые сервисами различного программного обеспечения с целью избегания его ввода каждый раз, когда он необходим (использовать «автозаполнение пароля»):

a. в программах, устанавливающих Интернет-соединения;
b. установка «флажка» «Сохранить пароль» (Save password) в соединениях удаленного доступа к сети и т.д.;

5) использовать «пустые» пароли (Enter).

2.6 Передача паролей третьим лицам (коллегам) запрещена.

2.7 Пароли администраторов ИС с именами учетных записей должны храниться в запечатанных конвертах в специальном сейфе ДИТ.

2.8 Работники Университета в обязательном порядке должны блокировать учетную запись, при условии даже одноминутного отлучения от рабочего места.

3. Общие положения по парольной защите

3.1 Ввод паролей осуществляется с учётом регистра (верхний-нижний) и с учётом текущей раскладки клавиатуры (EN-RU и др.). Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами и/или посторонними техническими средствами (например: мобильный телефон с функцией видеозаписи и т.д.).

3.2 С целью недопущения умышленных или запрещенных действий пользователями сети, их активность автоматически записывается в лог-файлах сервера ИС и отслеживается администратором ДИТ без предварительного уведомления пользователя. В случае определения нежелательных действий пользователя, данные пользователи немедленно отключаются от локальной сети, и администратором ДИТ инициируется служебное расследование по стандартным процедурам Университета. К нежелательным действиям относятся:

1) попытка или несанкционированный доступ к ресурсам, которые не входят в компетенцию пользователя сети;

2) совместное использование пользователями идентификационных имен и паролей
(в случае если на данные действия нет специального разрешения);

3) использование чужих идентификационных имен и паролей (в случае если на данные действия нет специального разрешения);

4) захват или использование чужих IP адресов;

5) попытки взлома компьютеров в локальной сети;

6) другие действия, связанные с деструктивными особенностями приложений или аппаратных средств.

3.4 В случае обнаружения пользователем каких-либо подозрительных признаков при работе систем (появление нестандартных подсказок ввода имени пользователя и пароля, изменение или удаление файлов, изменение конфигурации компьютера, произвольные действия клавиатуры/мышки) пользователи должны немедленно сообщить об этом, посредством телефонного звонка и/или продублировать запрос письменно по почте директору ДИТ. Затем, после исследования причин, по распоряжению директора ДИТ - изменить свой пароль, согласно требованиям настоящей Политики.

3.5 В случаях нарушения требований настоящей Политики работники Университета обязаны предоставить доступ к ресурсам своего персонального компьютера, файлам и документам системному администратору ДИТ и директору ДИТ по их требованию для проведения расследования нарушения.

3.6 Все случаи неверно введенных паролей, попытки несанкционированного подключения к системе и манипулирования учетными записями автоматически фиксируются в системных журналах безопасности ИС с целью последующего анализа для выявления предметов нарушений. Доступ к этим журналам имеют системные администраторы ДИТ (профильно: администраторы сетевой инфраструктуры, домена, базы данных). Директор ДИТ, совместно с системным администратором ДИТ, ежемесячно проводит процедуры по контролю информации в журналах безопасности на предмет выявления скрытых атак, подборов паролей, изменений настроек безопасности и учетных записей пользователей. Проверки производятся согласно требованиям внутренних нормативных документов.

4. Заключительные положения

4.1 Контроль над реализацией данной Политики, совершенствованием системы администрирования паролей и действиями администраторов ДИТ и директора ДИТ возлагается на Проректора по Цифровизации.

4.2 Организационное и техническое обеспечение процессов использования, смены и прекращения действия паролей возлагается на Директора ДИТ и системного администратора ДИТ.

4.3 Системные администраторы ДИТ обеспечивают реализацию групповых политик смены паролей, блокировку доступа к информационным ресурсам по истечении срока действия паролей, а также процедуру приема-передачи/уничтожения собственных.

4.4 Все пользователи Университета должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за несоблюдение правил данной политики, а также за разглашение парольной информации.

4.5 Ответственность за разглашение полученного пароля и действий, произведенных на персональном компьютере, возлагается на пользователя, получившего этот пароль и руководителя подразделения.

4.6 Данная Политика вступает в силу с момента ее утверждения и подписания Ученым советом УМБ.