«УТВЕРЖДЕНО»
Решением Правления
НАО «Университет Нархоз»
Протокол № 8 от
«15». 06 .2023 г.

Правила использования криптографических средств защиты информации IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»

Алматы, 2023

Оглавление

Паспорт документа

Наименование документа:	Правила использования криптографических средств защиты информации IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»
Краткое описание:	Правила использования криптографических средств защиты информации IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»
Тема:	Информационная безопасность
Статус:	Новый
Дата утверждения:	«___» _____2023г.
Дата завершения действия:	
Дата аудита:	Каждые 45 дней
Ответственный за аудит:	Эксперт по информационной безопасности

Лист согласования

Должность	Ф.И.О.	Подпись
Директор Административного департамента	Бисенғали Л.	
Советник по цифровизации	Тебаев Д. Б.	
и.о. Директора Департамента информационных технологий	Жумажанов Б.Ж.	

1 Общие положения

Настоящие Правила использования криптографических средств защиты информации IT инфраструктуры (далее – «Правила») определяют порядок учета, хранения и использования средств криптографической защиты информации и криптографических ключей, а также порядок смены, уничтожения криптографических ключей в целях обеспечения информационной безопасности при эксплуатации IT инфраструктуры НАО «Университет Нархоз» (далее – ITA «Нархоз»).

Требования настоящих Правил являются неотъемлемой частью комплекса мер безопасности и защиты информации в НАО «Университет Нархоз» (далее – «Нархоз»).

2 Глоссарий

Перечень использованных в настоящем документе определений:

– Эксперт по ИБ – должностное лицо, осуществляющее комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

– информационная безопасность (далее – ИБ) – состояние защищенности информационных ресурсов и систем, обеспечение конфиденциальности, целостности и доступности информации;

– конфиденциальность информации – обеспечение предоставления информации только авторизированным лицам;

– пароль – комбинация символов (буквы, цифры, специальные символы), устанавливаемые администратором ОС, СУБД, ППО при создании новой учетной записи;

– пользователь – сотрудники НАО и специалисты работающие с информационными система ITA «Нархоз»;

– целостность информации – состояние информации (ресурсов информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право;

– ЭЦП – электронно-цифровая подпись.

3 Ссылки

Настоящий документ разработан в соответствии со следующими нормативно-правовыми актами и документами:

• З Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V;

• Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;

• СТ РК ИСО/МЭК 27002 «Методы обеспечения защиты. Свод правил по управлению защитой информации»;

• СТ РК ИСО/МЭК 27001 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;

• СТ РК ГОСТ Р 50739 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».

• Стандарт по информационной безопасности ТОО «Verny Capital».

4 Контроль

Мероприятия по обеспечению безопасности доступа к ЭЦП применяются в соответствии со статьей 17, Закона Республики Казахстан от 7 января 2003 года №370 «Об электронном документе и электронной цифровой подписи». Дополнительно по обеспечению безопасности доступа к криптографии принимаются следующие мероприятия:

– ограничения импорта и/или экспорта аппаратных и программных средств для выполнения криптографических функций;

– ограничения импорта и/или экспорта аппаратных и программных средств, которые разработаны таким образом, что имеют, как дополнение, криптографические функции;

– ограничения на использование зашифровки;

– обязательные или дискреционные методы доступа со стороны государства к информации, зашифрованной с помощью аппаратных и программных средств для обеспечения конфиденциальности ее содержания.

5 Требования к системе управления ключами

Управление системой ключей осуществляется в соответствии с Приказом Министра по инвестициям и развитию Республики Казахстан от 23 декабря 2015 года № 1231 «Об утверждении Правил выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром, за исключением корневого удостоверяющего центра Республики Казахстан, удостоверяющего центра государственных органов, национального удостоверяющего центра Республики Казахстан и доверенной третьей стороны Республики Казахстан».

6 Требования по срокам активизации и дезактивации ключей

Активация и дезактивация ключей ЭЦП осуществляется в соответствии с Приказом Министра по инвестициям и развитию Республики Казахстан от 22 января 2016 года № 51 «О внесении изменения в приказ Министра по инвестициям и развитию Республики Казахстан от 24 апреля 2015 года № 491 "Об утверждении стандарта государственной услуги "Выдача и отзыв регистрационного свидетельства Национального удостоверяющего центра Республики Казахстан"», а так же Приказом Министра по инвестициям и развитию Республики Казахстан от 23 декабря 2015 года № 1231 «Об утверждении Правил выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром, за исключением корневого удостоверяющего центра Республики Казахстан, удостоверяющего центра государственных органов, национального удостоверяющего центра Республики Казахстан и доверенной третьей стороны Республики Казахстан».

7 Требования по сертификату открытых ключей

Каждый пользователь ITA «Университет Нархоз» должен иметь ЭЦП (открытый и закрытый ключ) выданную Национальным удостоверяющим центром Республики Казахстан. Открытый ключ должен быть действующим. В соответствии с Приказом Министра по инвестициям и развитию Республики Казахстан от 22 января 2016 года № 51 «О внесении изменения в приказ Министра по инвестициям и развитию Республики Казахстан от 24 апреля 2015 года № 491 «Об утверждении стандарта государственной услуги "Выдача и отзыв регистрационного свидетельства Национального удостоверяющего центра Республики Казахстан».

регистрационного свидетельства Национального удостоверяющего центра Республики Казахстан».

8 Требования к криптографическому шифрованию конфиденциальной информации при хранении, обработке и передаче по сетям телекоммуникаций

Криптографическое шифрование при обработке и передачи данных по сетям телекоммуникаций применяются в соответствии с Приказом Министра по инвестициям и развитию Республики Казахстан от 25 декабря 2015 года № 1241 «Об утверждении Правил применения сертификата безопасности».

9 Ответственность

Данные Правила обязательны для выполнения всеми работниками НАО «Университет Нархоз».

За неисполнение или ненадлежащее исполнение настоящих Правил работники несут дисциплинарную ответственность в соответствии с действующим законодательством Республики Казахстан.

10 Заключительные пожелания

10.1 Настоящие Правила утверждаются решением Правления Университета.

10.2 Изменения и дополнения в настоящие Правила вносятся на основании решения Правления Университета.

Лист ознакомления с правилами использования криптографических средств защиты информации

№	Фамилия, имя, отчество	Должность	Подпись	Дата
1	2	3	4	5