

Правила использования средств криптографической защиты информации

1. Общие положения

1. Правила использования средств криптографической защиты информации (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 безопасности эксплуатации информационных систем НАО «Евразийский национальный университет им Л.Н. Гумилева» (далее - Университет).

2. Настоящие Правила разработаны в соответствии с Государственным стандартом [СТ РК ИСО/МЭК 27002-2015](#) - Свод правил по управлению защитой информации и Политикой информационной безопасности, утвержденной настоящими правилами.

3. Перечень использованных в настоящем документе определений:

- Информационная безопасность (далее - ИБ) - состояние защищенности государственных информационных ресурсов и систем, обеспечение конфиденциальности, целостности и доступности информации;

- Администратор информационной системы - специалист, ответственный за администрирование, сопровождение и обеспечение бесперебойного функционирования всего комплекса информационных систем Университета;

- Пользователи информационной системы - сотрудники, работающие с информационными системами Университета;

- Конфиденциальность информации - обеспечение предоставления информации только авторизованным лицам;

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

- Аутентификация - подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа реализованными в системе;

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

- ЭЦП - электронно-цифровая подпись.

2. Политика использования криптографических средств защиты информации

4. 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».

5. Дополнительно по обеспечению безопасности доступа к криптографии принимаются следующие мероприятия:

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

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

3) ограничения на использование зашифровки;

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

6. 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».

7. 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».

8. Пользователи информационных систем с правом подписи электронных документов и иного предусмотренного законодательством Республики Казахстан должны иметь ЭЦП (открытый и закрытый ключ) выданную Национальным удостоверяющим центром Республики Казахстан. Открытый ключ должен быть действующим. В соответствие 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».

9. Требования к криптографическому шифрованию конфиденциальной информации при хранении, обработке и передаче по сетям телекоммуникаций в соответствии с заданием по безопасности

10. Применяются в соответствии с Приказом Министра по инвестициям и развитию Республики Казахстан от 25 декабря 2015 года № 1241 «Об утверждении Правил применения сертификата безопасности».