


**КГУ «Управление архитектуры, градостроительства и земельных  
отношений города Нур-Султан»**

**УТВЕРЖДЕНО**

**Директор ТОО  
«АстанаГорАрхитектура» города  
Нур-Султан**



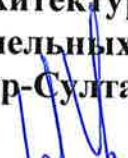
\_\_\_\_\_ Кенжебеков Н. К.



« 19 » сентября 20 20 г.

**УТВЕРЖДЕНО**

**Руководитель Управления  
архитектуры, градостроительства и  
земельных отношений города  
Нур-Султан**



\_\_\_\_\_ Уранхаев Н. Т.



« 19 » сентября 20 20 г.

**Правила использования средств криптографической защиты  
информации в  
Информационной системе «Геоинформационный портал  
города Нур-Султан»  
ГПГ.СМИБ.ПР.07.r02.20**

**г. Нур-Султан  
2020 г.**

## **1. Область применения**

Целью настоящего документа является описание правил использования криптографических средств защиты информации в ИС и определение порядка действий ответственных сотрудников Организации, а также определение ответственности при проведении этих мероприятий или нарушении требований настоящего Документа.

Настоящий документ обязателен для исполнения в рамках проекта обеспечения работы ИС.

Настоящий документ применим средствам вычислительной техники, телекоммуникационного оборудования и программного обеспечения ИС.

## **2. Нормативные ссылки**

Настоящий документ содержит указания к практическому исполнению требований, изложенных в нормативных документах согласно п. 3 Нормативные ссылки действующей Политики информационной безопасности.

## **3. Термины, определения и сокращения**

В настоящем документе используются термины и сокращения, принятые в действующей Политике информационной безопасности.

## **4. Общие положения**

Криптографические средства используются для того, чтобы защитить конфиденциальность, аутентичность или целостность информации проекта ИС.

Использование шифрования направлено на:

- a) сохранение конфиденциальности данных при помощи шифра;
- b) аутентификацию, в том числе контроля целостности данных ЭЦП;
- c) подписания документа;
- d) генерации, формирования, распределения и (или) управления ключами.

Любая конфиденциальная информация, хранимая или передаваемая в процессе сопровождения или эксплуатации ИС (при хранении, обработке и передаче по сетям телекоммуникаций) подлежит обязательному шифрованию. В настоящем документе в разделах 5, 6, 7 описаны требования к криптографическому шифрованию конфиденциальной информации при хранении, обработке и передаче по сетям телекоммуникаций в процессе сопровождения и эксплуатации ИС.

## **5. Шифровальные средства управления**

Настоящий документ гарантирует надлежащее и эффективное использование криптографии для защиты конфиденциальности, подлинности и/или целостности информации.

### **Политика в отношении использования шифровальных средств управления**

Руководство Организации и СОИБ должны обеспечить гармоничное развитие и внедрение процедуры использования шифровальных средств управления для защиты информации.

Настоящий документ предусматривает следующие аспекты:

- а) использование криптографических средств защиты в организации должно производиться строго в соответствии настоящего документа;
- б) выбираемый уровень и средства шифрования должны соответствовать степени риска;
- в) шифрование используется для подключения к ИС, для удаленной работы сотрудников проекта, в VPN;
- г) настоящий документ регламентирует подход к управлению ключами, включая методы, которые имеют дело с защитой ключей к шифру и восстановлением зашифрованной информации в случае потери, подверженности опасности или поврежденности ключей;
- д) распределение ответственности:
  - 1) за внедрение настоящего документа отвечает руководство Организации и СОИБ;
  - 2) за управление ключами отвечает СОИБ (см. 10.1.2);
- е) настоящий документ определяет используемые стандарты шифрования и выбор алгоритмов;
- ж) зашифрованная информация не должна подвергаться дополнительной проверки при передаче.

Шифровальные средства управления используются для обеспечения ИБ, в том числе для:

- а) конфиденциальности: использование шифрования информации, чтобы защитить чувствительную или важную информацию, или сохраненной или переданной;
- б) целостность/подлинность: использование цифровых подписей или кодов аутентификации сообщения, чтобы проверить подлинность или целостность сохраненной или переданной чувствительной или важной информации;
- в) не отказ от обязательств: использование шифровальных методов, чтобы представить свидетельства возникновения или не возникновения события или действия;
- г) идентификация: использование шифровальных методов, чтобы подтвердить подлинность пользователей и других системных предприятий,

запрашивающих доступ к системным пользователям, предприятиям и ресурсам или ведущих дела с указанными лицами и организациями.

### **Управление ключами**

Настоящий документ включает требования для управления ключами к шифру, требования к периоду эксплуатации ключей, создание, хранение, архивирование, восстановление, распределение, удаление и уничтожение ключей.

Шифровальные алгоритмы, длина ключа и методы использования выбраны согласно наиболее успешной практике. Соответствующее управление ключами требует безопасных процессов для создания, хранения, архивирования, восстановления, распределения, удаления и разрушения ключей к шифру.

Все ключи к шифру должны быть защищены от модификации и потери. Кроме того, секретные и частные ключи должны быть защищены от несанкционированного использования, а также раскрытия. Оборудование, используемое для производства, сохранения и архивирования ключей, должно быть физически защищено.

За сохранность частных/персональных ключей отвечают владельцы таких ключей. Ответственным за сохранность оборудования для производства ключей назначается СОИБ.

Период эксплуатации ключей не более одного года, если иное не предусмотрено действующим Законодательством РК.

В организации допускается использовать только следующие виды ключей:

1) ключи ЭЦП НУЦ РК, выданные на имя сотрудника Организации от юридического лица Организации для выполнения служебных обязанностей, ответственным за такие ключи назначается сам владелец ключей;

2) SSL-ключи для шифрования передачи данных ИС и аутентификации ИС, ответственным за такие ключи назначается СОИБ;

3) ключи локального удостоверяющего центра, которые применяются для генерации подписания ключей для VPN, ответственным за такие ключи назначается СОИБ;

4) ключи для аутентификации и шифрования трафика в VPN и SSH, которые генерируются локальным удостоверяющим центром, такие ключи генерируются администратором ИС для каждого сотрудника, допущенного к VPN и SSH индивидуально, ответственным за такие ключи назначается сам владелец ключей.

За исключением ключей для VPN и SSH, ключи генерируются внешними надежными источниками.

Система управления ключами VPN и SSH должна основана на согласованном наборе стандартов, процедур и безопасных методов для:

а) создания ключей для различных шифровальных систем и различных приложений;

- b) издания и получения сертификатов открытого ключа;
- c) передача ключей ответственному сотруднику лично в руки, установление пароля на контейнер с ключами;
- d) хранение ключей, включая то, как зарегистрированные пользователи получают доступ к ключам;

Для снижения вероятности неправильного использования, даты активации и даты деактивации ключей должны быть определены так, чтобы ключи могли только использоваться в течение промежутка времени, определенного в настоящем документе.

Содержание соглашений о сервисном обслуживании или контрактов с внешними поставщиками шифровальных услуг, например, с органом сертификации должны охватывать проблемы ответственности, надежности услуг и времени, затраченного для предоставления услуг.

## **6. Требования к криптографическому шифрованию конфиденциальной информации при хранении, обработке и передаче по сетям телекоммуникаций для работы пользователей ИС**

Средства криптографической защиты информации применяются при:

- a) аутентификации пользователей;
- b) шифровании трафика и обеспечения конфиденциальности и целостности информации в процессе обмена информацией между пользователями и серверами ИС;
- c) подписании документа электронной цифровой подписью пользователем;
- d) шифровании паролей пользователей;
- e) шифровании трафика при выполнении задач сопровождения серверов ИС;
- f) для шифрования трафика при репликации данных между компонентами ИС;
- g) при хранении, обработке и передаче по сетям телекоммуникаций в процессе сопровождения и эксплуатации ИС.

Программное обеспечение ИС, используемое в целях программно - криптографической защиты информации, использует следующие механизмы защиты:

- a) SSL (Secure Sockets Layer) – при аутентификации пользователей и обмене информации между пользователями и сервером;
- b) алгоритм RSA (Rivest-Shamir-Adleman) с длиной ключа 1024 бита – для шифрования трафика при выполнении задач сопровождения серверов ИС, репликации данных;
- c) ГОСТ 28147-89 с длиной ключа 1024 бита – для шифрования трафика при выполнении задач сопровождения серверов ИС, репликации данных;
- d) MD5 для шифрования паролей пользователей ИС;
- e) ЭЦП для аутентификации пользователей и серверов ИС.

ИС использует для защиты информации сертифицированные, в порядке, установленном законодательством Республики Казахстан, средства криптографической защиты информации (далее – СКЗИ), позволяющие идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации, в электронном виде.

В ИС используются, принимаются и признаются сертификаты ключей подписи, изданные удостоверяющими центрами, доверенными НУЦ.

Пользователи ИС – владельцы сертификатов ключей подписей при авторизации и подписании электронного документа используют для защиты информации, при передаче ее по открытым каналам связи, сертифицированные, в порядке, установленном законодательством РК, СКЗИ НУЦ, представленные в комплекте разработчика.

При работе с ИС, используются ключи, состоящие из открытой и закрытой частей, и вырабатываемые отдельно для каждого пользователя НУЦ.

ИС проверяет регистрационные свидетельства пользователя, выданные удостоверяющим центром, путем выполнения следующих проверок:

а) проверка построения корректной цепочки от проверяемого регистрационного свидетельства до доверенного корневого регистрационного свидетельства удостоверяющего центра, с учетом промежуточных регистрационных свидетельств удостоверяющих центров;

б) проверка срока действия регистрационного свидетельства от проверяемого регистрационного свидетельства до доверенного корневого регистрационного свидетельства удостоверяющего центра, с учетом промежуточных регистрационных свидетельств удостоверяющих центров;

с) проверка регистрационного свидетельства на отозванность (аннулирование);

д) проверка области использования ключа. Проверка заключается в проверке значения поля регистрационного свидетельства «использование ключа». Если поле содержит значения «Цифровая подпись» и «Неотрекаемость», то это регистрационное свидетельство используется для ЭЦП. А если поле содержит значение «Цифровая подпись» и «Шифрование ключей», то это регистрационное свидетельство используется для аутентификации;

е) проверка номера политики регистрационного свидетельства и разрешенных способах его использования. Если политика проверяемого регистрационного свидетельства предусматривает ограничение его использования (только в одной системе), то данное регистрационное свидетельство и соответствующий закрытый ключ не использовать в других системах;

ф) проверка метки времени. Доказательством подписания документа в указанный момент времени является квитанция метки времени, полученная в удостоверяющем центре и содержащая дату на которую

существовал документ. Данная проверка производится для электронных документов длительного хранения и формируется в момент подписания документа;

г) проверка полномочий лица, подписавшего документ.

Если выясняется, что ЭЦП или регистрационное свидетельство не соответствует требованиям хотя бы одного критерия, за исключением метки времени, то ЭЦП или регистрационное свидетельство считается недействительным.

Вход пользователя в ИС с использованием ЭЦП возможен только при наличии у данного пользователя действующего сертификата открытого ключа и пароля доступа в ИС.

При работе в ИС с использованием протокола HTTPS шифрование трафика производится ВС автоматически с помощью сеансовых ключей, генерируемых на время сеанса работы на основе ключевой информации НУЦ.

Все действия пользователя в ИС с использованием ЭЦП считаются правомерными, если аутентификация данного пользователя при входе в ИС произошла с использованием ЭЦП и производилось шифрование трафика между данным пользователем сервером с помощью сеансовых ключей.

## **7. Требования к криптографическому шифрованию конфиденциальной информации при хранении, обработке и передаче по сетям телекоммуникаций для сопровождения ИС**

Системные администраторы и ответственный за обеспечение информационной безопасности подключаются к серверам с помощью виртуальной частной сети (VPN) из помещения проекта ИС.

Для образования виртуальной частной сети и обеспечения защиты информации в процессе выполнения работ по сопровождению ИС используются только стойкие к взлому алгоритмы защиты аутентификации и шифрования передаваемой информации:

а) алгоритм RSA (Rivest-Shamir-Adleman) с длиной ключа 1024 бита – для шифрования трафика при выполнении задач сопровождения серверов ИС, репликации данных;

б) алгоритм AES (Advanced Encryption Standard) с длиной ключа 256 бит – для шифрования трафика при выполнении задач сопровождения серверов ИС, репликации данных;

с) ГОСТ 28147-89 с длиной ключа 1024 бита – для шифрования трафика при выполнении задач сопровождения серверов ИС, репликации данных;

д) MD5 (англ. Message Digest 5) — 128-битный алгоритм хеширования, предназначен для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности. Широко применялся для проверки целостности информации и хранения паролей в закрытом виде.

Генерация ключей для осуществления репликации данных между серверами ИС, для обеспечения шифрования трафика при сопровождении серверов и для осуществления аутентификации системного администратора и ответственного за обеспечение ИБ при доступе к консоли управления сервером ИС выполняется при помощи разрешенной системной утилиты.

Для защиты передаваемых при репликации данных между основным и резервным узлами ИС используется стойкое шифрование AES, RSA, ГОСТ 28147-89.

Ключи для шифрования трафика при репликации данных и шифровании паролей пользователей генерируются и устанавливаются системным администратором.

Для защиты паролей системных администраторов и ответственного за обеспечение ИБ используются методы безвозвратного шифрования основанные на MD5.

## **8. Защита ключей, сертификатов и ЭЦП**

Пользователи и сотрудники Организации должны защищать вверенные им ключи, ЭЦП и сертификаты от изменения и разрушения, а закрытые части ключей необходимо защищать от неавторизованного раскрытия.

Для уменьшения вероятности компрометации ключи имеют определенные даты активизации и деактивации, чтобы их можно было бы использовать в течение ограниченного периода времени, который устанавливается в соответствии с требованиями законодательства РК.

Для уменьшения вероятности компрометации ключей, сертификатов и ЭЦП определены даты их активизации и деактивации, чтобы их можно было бы использовать не более одного года. После истечения разрешенного срока использования ключей, сертификатов и ЭЦП они должны быть перевыпущены в порядке, установленном законодательством РК.

Закрытые ключи:

- a) запрещается выносить за пределы Организации;
- b) запрещается устанавливать на оборудование, не являющееся частью проекта ИС
- c) необходимо хранить в зашифрованном виде на служебной рабочей станции;
- d) запрещается передавать третьим лицам.

Защита открытого ключа обеспечивается с помощью сертификата открытых ключей доверенного удостоверяющего центра НУЦ РК. Пользователи должны хранить свои открытые ключи в тайне и передавать их только авторизованным лицам.

Существует угроза подделывания цифровой подписи и замены открытого ключа пользователя своим. Эта проблема решается с помощью сертификата открытых ключей. Этот процесс выполняется



уполномоченным органом по сертификации – НУЦ РК, который является признанной организацией, руководствующейся соответствующими правилами и процедурами информационной безопасности для обеспечения требуемой степени доверия к нему.

Открытые ключи:

- а) запрещается устанавливать на оборудование, не являющееся частью проекта ИС;
- б) запрещается передавать третьим лицам.

## **9. Ответственность**

СОИБ несет ответственность за:

- а) соблюдение требований законодательства в отношении ЭЦП;
- б) контроль исполнения требований настоящего документа,
- с) исполнение настоящей Инструкции.

Сотрудники проекта ИС:

- а) соблюдение требований законодательства в отношении ЭЦП;
- б) исполнение настоящей Инструкции.

Пользователи ИС:

- а) соблюдение требований законодательства в отношении ЭЦП;
- б) исполнение настоящей Инструкции.