КГУ «Управление архитектуры и градостроительства города Алматы»

УТВЕРЖДЕНО

Руководитель Управления архитектуры и градостроительства города Алматы

_____ Ахмеджанов А. Т.

«14» января 2019 г.

М. П.

Правила использования криптографических средств защиты информации в Информационной системы «3D автоматизированная геоинформационная система города Алматы» 3DГЕО.СМИБ.ПР.07.r01.19

г. Алматы
2019 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 обеспечении 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. 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 максимальной длиной ключа 512 бита – для шифрования трафика при выполнении задач сопровождения серверов ИС, репликации данных;

c) MD5 для шифрования паролей пользователей ИС;

d) 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:

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

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

c) проверка регистрационного свидетельства на отозванность (аннулирование);

d) 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;

e) 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;

f) 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 долговременного хранения и формируется в момент подписания документа;

g) 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 использование ЭЦП и производилось шифрование

трафика между данным пользователем сервером с помощью сеансовых ключей.

6. 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 передоваемой информации:

a) алгоритм RSA (Rivest-Shamir-Adleman) с максимальной длиной ключа 512 бита – для шифрования трафика при выполнении задач сопровождения серверов ИС, репликации данных;

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

c) 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.

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.

7. 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 дезактивации, 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 определенны даты их активизации и дезактивации, 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:

a) запрещается устанавливать на оборудование, не являющееся частью проекта ИС;

b) запрещается передавать третьим лицам.

8. Ответственность

СОИБ несет ответственность за:

a) соблюдение требований законодательства в отношении ЭЦП;
b) контроль исполнения требований настоящего документа,
c) исполнение настоящей Инструкции.

Сотрудники проекта ИС:

a) соблюдение требований законодательства в отношении ЭЦП;
b) исполнение настоящей Инструкции.

Пользователи ИС:

a) соблюдение требований законодательства в отношении ЭЦП;
b) исполнение настоящей Инструкции.