ПОЛИТИКА
применения квалифицированных сертификатов ключей проверки электронных подписей в системе электронного документооборота АО «Вертолеты России»

Содержание

1. Цель

1.1. Настоящая Политика применения квалифицированных сертификатов ключей проверки электронных подписей в системе электронного документооборота АО «Вертолеты России» (далее – Политика) разработана в связи с ведением в АО «Вертолеты России» (далее – Общество) электронного документооборота, позволяющего ускорить и оптимизировать процесс подписания работниками Общества документов, предусмотренных настоящей Политикой.

1.2. Настоящая Политика предусматривает порядок создания квалифицированных сертификатов ключей проверки электронных подписей (далее – сертификатов) для использования в системе электронного документооборота Общества (далее – СЭД) и условия их применения работниками Общества, включая обязанности работников Общества, строгое выполнение которых позволит обеспечить защиту информации при обмене электронными документами.

1.3. Настоящая Политика определяет правовые условия использования электронной подписи в электронных документах, при соблюдении которых электронная подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

2. Термины и определения

Владелец квалифицированного сертификата ключа проверки электронной подписи (Владелец) – лицо, которому выдан квалифицированный сертификат ключа проверки электронной подписи.

Ключ проверки электронной подписи (открытый ключ) – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее – проверка электронной подписи).

Ключ электронной подписи (закрытый ключ) – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключевой носитель – внешнее (съемное) устройство, используемое для хранения ключевой пары и сертификата ключа проверки электронной подписи.

Ключевая пара (электронные ключи) – открытый и закрытый ключи, связанные между собой особым математическим соотношением.

Компрометация закрытого ключа – результат действий физического лица, повлекший за собой разглашение закрытого ключа.

Менеджер Политики – физическое лицо, ответственное за исполнение настоящей Политики, утвержденное приказом генерального директора Общества.

Пользователь сертификата – физическое лицо, использующее полученные в Удостоверяющем центре сведения о сертификате для проверки принадлежности электронной подписи Владельцу сертификата.

Работник – физическое лицо, вступившее в трудовые отношения с Обществом.

Репозиторий (хранилище) — информационный ресурс, на котором хранятся и поддерживаются в актуальном состоянии какие-либо данные.

Квалифицированный сертификат ключа проверки электронной подписи (далее – Сертификат) – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу квалифицированного сертификата ключа проверки электронной подписи.

Список отозванных/приостановленных сертификатов (СОС) – электронный документ с электронной подписью Уполномоченного лица Удостоверяющего центра, содержащий список серийных номеров сертификатов, которые в определенный момент времени были отозваны либо действие которых было приостановлено. Сертификаты, чьи номера присутствуют в списке файла СОС, являются отозванными из обращения Удостоверяющим центром.

Средства электронной подписи – средства криптографической защиты информации, необходимые для создания и проверки электронных подписей, создания ключей электронных подписей (закрытого ключа) и ключей проверки электронных подписей (открытого ключа).

Средства криптографической защиты информации (СКЗИ) – средства вычислительной техники, осуществляющие криптографическое преобразование информации для обеспечения ее безопасности.

Удаленный оператор ЦР – работник Общества, уполномоченный приказом генерального директора формировать запросы на управление жизненным циклом сертификатов работников Общества.

Удостоверяющий центр – юридическое лицо или индивидуальный предприниматель, осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом Российской Федерации от 06 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Уполномоченное лицо Удостоверяющего центра – физическое лицо, являющееся работником Удостоверяющего центра и наделенное Удостоверяющим центром полномочиями по заверению сертификатов и Списков отозванных/приостановленных сертификатов.

Файл шаблона формы для автономной работы (MHT-файл) – используется для создания html-формы, обеспечивающей формирование ключевой пары и файла запроса на выпуск сертификата на рабочем месте пользователя.

Электронная подпись (ЭП) – информация в электронной форме, присоединенная к электронному документу или иным образом связанная с ним и позволяющая идентифицировать лицо, подписавшее электронный документ.

Электронный документ – документированная информация, представленная в электронной форме (т.е. в виде набора символов, звукозаписи или изображения и т.д., пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах), с реквизитами, позволяющими ее идентифицировать.

Электронный документооборот – движение документов в Обществе с использованием автоматизированной информационной системы (системы электронного документооборота) с момента их создания или получения до завершения исполнения или отправки,

3. Область действия

3.1. Требования настоящей Политики распространяются на всех работников Общества, использующих электронную подпись в системе электронного документооборота Общества.

4. Порядок создания и выпуска сертификата

4.1. Для работников Общества Сертификат выпускается аккредитованным удостоверяющим центром – ЗАО «Национальный удостоверяющий центр» (далее – УЦ).

4.2. Сертификат издается в соответствии с настоящей Политикой, Регламентом услуг УЦ и информацией, указанной в заявлении работника Общества на выпуск Сертификата.

4.3. Запрос на выпуск Сертификата

4.3.1. Для получения Сертификата работник Общества передает подписанное собственноручно заявление на выпуск сертификата (Приложение 1) Удаленному оператору ЦР.

4.3.2. При получении заявления на выпуск сертификата Удаленный оператор ЦР аутентифицирует работника Общества по фотографии в документе, удостоверяющем личность, представленном работником, и сверяет данные в заявлении на выпуск сертификата с данными в документе, удостоверяющем личность. В случае отсутствия ошибок в заявлении Удаленный оператор ЦР принимает заявление на выпуск сертификата к обработке и с помощью автоматизированного рабочего места Удаленного оператора ЦР, подключенного по защищенному каналу к УЦ, выполняет следующие действия:

– регистрирует работника в УЦ;

– форматирует ключевой носитель. При этом должны быть выполнены следующие настройки безопасности ключевого носителя:

- возможность смены пароля (PIN-кода) – только у пользователя (работника);
- для пользователя (работника) длина пароля (PIN-кода) – не менее 8 (восьми) символов;
- для пользователя (работника) количество неудачных попыток ввода пароля (PIN-кода) до блокировки ключевого носителя – 5 (пять);
- для администратора (Удаленного оператора ЦР) длина пароля (PIN-кода) – не менее 10 (десяти) символов;
- для администратора (Удаленного оператора ЦР) количество неудачных попыток ввода пароля (PIN-кода) до блокировки ключевого носителя – 3 (три);

– с помощью АРМ создает пароль (PIN-код) администратора ключевого носителя, который должен отвечать следующим требованиям:

- пароль (PIN-кода) администратора (Удаленного оператора ЦР) известен только Удаленному оператору ЦР;
- пароль (PIN-кода) администратора (Удаленного оператора ЦР) не должен содержать слов, словосочетаний, имен и т.п.;

– с помощью АРМ генерирует ключевые пары и формирует файл запроса на выпуск сертификата. Генерацию ключевых пар необходимо осуществлять на типы носителей, указанные в п. 14.2 настоящей Политики;

– проверяет соответствие данных в файле запроса на выпуск сертификата данным в заявлении на выпуск сертификата, подписанном рукописной подписью работника;

– в случае успешного результата проверки с помощью АРМ подписывает файл запроса на выпуск сертификата своей электронной подписью и направляет файл запроса на выпуск сертификата в УЦ.

4.4. Выпуск Удостоверяющим центром сертификата

4.4.1. После получения от Удаленного оператора ЦР файла запроса на выпуск сертификата УЦ выполняет следующие действия:

– проверяет действительность электронной подписи Удаленного оператора ЦР на файле запроса на выпуск сертификата работнику;

– в случае успешной проверки выпускает сертификат работнику.

4.4.2. УЦ передает сертификат Удаленному оператору ЦР.

4.4.3. После выпуска сертификата УЦ Удаленный оператор ЦР оповещает работника об издании сертификата лично либо по корпоративной электронной почте Общества.

4.4.4. Удаленный оператор ЦР передает ключевой носитель работнику подразделения информационной безопасности для его регистрации и учета в соответствии с Порядком учета, хранения и обращения ключевых носителей электронной подписи в Холдинге «Вертолеты России» от 10.08.2017 № 0019-

17-ЛНА/УК, утвержденным приказом АО «Вертолеты России» от 10.08.2017 № 0103-УК (далее – Порядок).

4.4.5. Передача ключевого носителя Владельцу или ответственному за использование электронной подписи осуществляется в соответствии с Порядком.

4.4.6. Для признания сертификата Владельцу необходимо заверить своей подписью сертификат на бумажном носителе. После признания сертификата работником Удаленный оператор ЦР уведомляет об этом УЦ с использованием АРМ.

4.4.7. В случае если УЦ не получает в течение трех рабочих дней от Удаленного оператора ЦР уведомления о признании либо непризнании сертификата работником, сертификат также считается признанным.

4.4.8. Удостоверяющий центр публикует выпущенные сертификаты в репозитории УЦ не позднее начала срока действия сертификата.

5. Обновление ключей

5.1. В случае необходимости обновления ключей выпускается новый сертификат.

5.2. Обновление ключей возможно в случае компрометации закрытого ключа, а также в случае истечения срока действия сертификата.

5.3. Заявление на выпуск сертификата при обновлении ключей может подать Владелец сертификата. Форма заявления на выпуск сертификата при обновлении ключей предусмотрена приложением к настоящей Политике.

5.4. Порядок подачи запроса на выпуск сертификата при обновлении ключей, его одобрение, издание сертификата, оповещение об издании сертификата и признание сертификата работником Общества осуществляется в порядке, предусмотренном в разделе 4 настоящей Политики.

5.5. В случае издания УЦ нового сертификата при обновлении ключей сертификат публикуется в репозитории УЦ.

6. Изменение сертификата

6.1. Изменением сертификата является выдача нового сертификата при необходимости изменения информации, включенной в существующий сертификат. При этом старый сертификат отзывается. Новый сертификат выпускается одновременно с генерацией новой ключевой пары.

6.2. Изменение сертификата производится в случае, если информация, содержащаяся в сертификате, становится не актуальной или при ее внесении в сертификат была допущена ошибка.

6.3. Заявление на изменение сертификата может подавать Владелец сертификата. Форма заявления на изменение сертификата предусмотрена приложением к настоящей Политике. Порядок подачи заявления на изменение сертификата, его одобрение, выпуск сертификата, оповещение о выпуске

сертификата и признание измененного сертификата работником Общества осуществляется в порядке, предусмотренном в разделе 4 настоящей Политики.

6.4. УЦ публикует измененный сертификат в репозитории УЦ.

7. Порядок использования сертификата

7.1. Владелец сертификата или ответственный за использование электронной подписи может использовать сертификат после его признания и в соответствии с требованиями настоящей Политики, Регламента услуг УЦ и Порядка.

7.2. Разрешено использование только действительного сертификата в соответствии с требованиями настоящей Политики.

7.3. Перед использованием Владельцам, ответственным за использование электронной подписи, и Пользователям сертификатов необходимо:

- ознакомиться с настоящей Политикой, Порядком и Регламентом услуг УЦ, в соответствии с которыми выпущен сертификат;
- проверить статус используемого сертификата.

8. Проверка статуса сертификата и подлинности ЭП в электронном документе

8.1. Для проверки статуса сертификата Владельцу, ответственному за использование электронной подписи, и/или Пользователю сертификата необходимо выполнить следующие действия:

8.1.1. проверить, что срок действия используемого сертификата не истек;

8.1.2. проверить статус (отозван/приостановлен) используемого сертификата, применяя список отозванных/приостановленных сертификатов (далее – СОС), публикуемых УЦ, или сервис online-проверки статуса сертификата;

8.1.3. проверить ЭП уполномоченного лица УЦ, которой подписан используемый сертификат (для проверки ЭП уполномоченного лица УЦ необходимо использовать сертификат уполномоченного лица УЦ, опубликованный на сайте Минкомсвязи России);

8.1.4. проверить статус сертификата уполномоченного лица УЦ, ЭП которого подписан используемый сертификат (для проверки информации о статусе сертификата уполномоченного лица УЦ необходимо использовать СОС головного удостоверяющего центра, опубликованный на сайте Минкомсвязи России).

8.2. Для подтверждения подлинности ЭП в электронном документе, то есть установления принадлежности ЭП, содержащейся в электронном документе, ее владельцу, и отсутствия искажения и подделки подписанного данной ЭП электронного документа используются средства ЭП и сертификат подписанта, содержащий в себе ключ проверки ЭП (открытый ключ).

8.3. Открытый ключ Владельца сертификата доступен любому Пользователю.

9. Допустимое использование сертификатов

9.1. В информационных системах Общества могут быть использованы квалифицированные сертификаты ключей проверки электронной подписи, выпущенные в рамках настоящей Политики, а также квалифицированные сертификаты ключей проверки электронной подписи, полученные работниками Общества самостоятельно в аккредитованных удостоверяющих центрах.

9.2. Квалифицированной электронной подписью допустимо подписывать электронные документы в случаях, предусмотренных:

- Федеральным законом Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- действующей редакцией Гражданского кодекса Российской Федерации от 30 ноября 1994 г. № 51-ФЗ;
- действующей редакцией Налогового кодекса Российской Федерации от 31 июля 1998 г. № 146-ФЗ;
- действующей редакцией Трудового кодекса Российской Федерации от 30 декабря 2001 г. № 197-ФЗ;
- другими нормативно-правовыми актами Российской Федерации.

9.3. Работник имеет право подписывать электронной подписью только те документы, полномочиями на подписание которых он обладает. Наличие электронной подписи не наделяет Работника какими-либо дополнительными полномочиями к ранее существующим. Работник наделяется дополнительными полномочиями только на основании выданной ему доверенности.

9.4. Ключ электронной подписи и сертификат применяются Владельцем сертификата или ответственным за использование электронной подписи для выполнения следующих операций:

- подписания электронных документов ЭП;
- проверки ЭП в электронном документе;
- шифрования/расшифрования содержания документов или сообщений;
- установки защищенных соединений;
- его аутентификации в информационных системах Общества.

9.5. Запрещается использовать сертификаты в иных целях или способами, не определенными в разделе 9 настоящей Политики.

10. Основные обязанности Владельцев сертификатов и ответственных за использование ЭП

10.1. Работник (Владелец сертификата) обязан:

10.1.1. Хранить в тайне закрытый ключ, обеспечить соблюдение мер, исключающих компрометацию закрытого ключа.

10.1.2. Не передавать третьим лицам ключевой носитель.

10.1.3. В случае компрометации закрытого ключа, а также в случае оснований полагать, что закрытый ключ мог быть скомпрометирован (см. п. 10.2 настоящей Политики), незамедлительно сообщить об этом работнику подразделения информационной безопасности, Удаленному оператору ЦР, либо Уполномоченному лицу УЦ.

10.1.4. Использовать ЭП только в целях, предусмотренных разделом 9 настоящей Политики.

10.1.5. В случае прекращения трудовых отношений с Обществом передать Обществу по акту приема-передачи все ключевые носители, выданные работнику в связи с использованием ЭП.

10.1.6. Использовать СКЗИ, указанные в п. 13.2 настоящей Политики.

10.1.7. Выполнять требования к Владельцам сертификатов, предусмотренные прочими пунктами настоящей Политики.

10.1.8. При работе с ЭП и сертификатами руководствоваться требованиями Порядка и положениями инструкции пользователя по работе с СКЗИ.

10.2. К фактам, которые могут рассматриваться как компрометация (или подозрение на компрометацию) ключей Владельцев ЭП, относятся следующие события:

10.2.1. утрата ключевых носителей;

10.2.2. выявление Владельцем сертификата событий, связанных с использованием его ключа ЭП без его участия;

10.2.3. в случае, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда носитель вышел из строя и имеется вероятность того, что это произошло в результате злоумышленных действий);

10.2.4. невозможность использования пароля (PIN-кода) пользователя для доступа к ключевому носителю Владельцем сертификата;

10.2.5. возникновение подозрений на несанкционированное копирование ключа ЭП или его искажение.

11. Порядок прекращения, приостановления и возобновления действия сертификата

11.1. Сертификат считается прекращенным или приостановленным с момента публикации в репозитории УЦ списка отозванных/приостановленных сертификатов, содержащего информацию об изменении статуса этого сертификата.

11.2. В случае возобновления действия сертификата УЦ исключает соответствующий сертификат из списка отозванных/приостановленных сертификатов.

11.3. Прекращение действия сертификата

11.3.1. Сертификат прекращает свое действие по истечении срока, на который он был выпущен, или в случае его отзыва лицами, указанными в п. 11.3.3. настоящей Политики.

11.3.2. Сертификат может быть отозван при следующих обстоятельствах:

– при прекращении действия трудового договора между Обществом и Владельцем сертификата;

– при компрометации закрытого ключа;

– при разрыве или несоблюдении соглашений между Обществом и УЦ, выпустившим данный сертификат;

– при несоблюдении Владельцем сертификата требований настоящей Политики;

– при прекращении деятельности УЦ, выпустившего данный сертификат;

– по запросу Владельца сертификата.

11.3.3. Запрос на отзыв сертификата может быть подан:

– Владельцем сертификата с обязательным уведомлением Удаленного оператора ЦР;

– директором по персоналу и организационному развитию;

– Удаленным оператором ЦР, если он располагает достоверной информацией, требующей отзыва сертификата;

– Уполномоченным лицом УЦ, если он располагает достоверной информацией, требующей отзыва сертификата.

11.3.4. Запрос на отзыв сертификата может быть подан в бумажной или электронной форме либо с использованием любых средств связи, но в любом случае с его аутентификацией Удаленным оператором ЦР по действительному сертификату или документально подтвержденному запросу на отзыв сертификата.

Запрос на отзыв сертификата должен содержать следующую информацию:

– серийный номер сертификата или иную информацию, позволяющую однозначно идентифицировать сертификат;

– причину отзыва сертификата;

– необходимые комментарии.

После получения запроса на отзыв сертификата УЦ производит верификацию запроса, и если таковая прошла успешно, то производит отзыв сертификата. После отзыва сертификата Владелец такового уведомляется об этом, а УЦ публикует СОС, содержащий информацию об отозванном сертификате.

11.3.5. Запрос на отзыв сертификата должен быть передан в УЦ так быстро, насколько это возможно. Запрос на отзыв сертификата, полученный от Владельца сертификата или от иных лиц, должен быть рассмотрен УЦ в течение 1 (одного) рабочего дня с момента его подачи. Временем подачи запроса на отзыв сертификата считается:

– при передаче по электронной почте – время передачи сообщения на почтовый сервер УЦ;

– при вручении лично или передачей иными способами – время получения.

Запрос на отзыв сертификата, полученный через АРМ Удаленного оператора Центра регистрации и подписанный квалифицированной электронной подписью Удаленного оператора ЦР, обрабатывается УЦ автоматически в режиме реального времени.

11.3.6. В случае отзыва, приостановления или возобновления действия какого-либо из сертификатов УЦ публикует измененный СОС в течение 30 (тридцати) минут с момент обработки соответствующего запроса. Если срок действия сертификата, включенного в СОС, истек, то он может быть удален из СОС.

11.4. Приостановление действия сертификата

11.4.1. Действие сертификата должно быть приостановлено при следующих обстоятельствах:

– по запросу Владельца сертификата с одновременным уведомлением Удаленного оператора ЦР;

– по запросу директора по персоналу и организационному развитию Общества;

– по запросу Удаленного оператора ЦР;

– при возникновении какого-либо разбирательства, не позволяющего на текущий момент принять решение о действительности сертификата.

11.4.2. Запрос на приостановление действия сертификата может быть подан:

– Владельцем сертификата;

– директором по персоналу и организационному развитию Общества;

– Удаленным оператором ЦР, если он располагает достоверной информацией, требующей приостановления сертификата;

– Уполномоченным лицом УЦ, если он располагает достоверной информацией, требующей приостановления сертификата.

11.4.3. Запрос на приостановление действия сертификата может быть подан в бумажной или электронной форме либо с использованием любых средств связи, но в любом случае с его аутентификацией Удаленным оператором ЦР по действительному сертификату или документально подтвержденному запросу на приостановление.

Запрос на приостановление действия сертификата должен содержать следующую информацию:

– серийный номер сертификата или иную информацию, позволяющую однозначно идентифицировать сертификат;

– причину приостановления;

– необходимые комментарии.

11.4.4. После получения запроса на приостановление действия сертификата УЦ производит верификацию запроса, и если таковая прошла

успешно, то производит приостановление сертификата. После приостановления сертификата владелец такового уведомляется об этом, а УЦ публикует СОС, содержащий информацию о приостановлении сертификата.

11.4.5. Запрос на приостановление действия сертификата, полученный от Владельца сертификата или от иных лиц, указанных в п. 11.4.2 настоящей Политики, должен быть рассмотрен в течение 1 (одного) рабочего дня с момента его подачи.

Временем подачи запроса на приостановление действия сертификата считается:

– при передаче по электронной почте – время передачи сообщения на почтовый сервер УЦ;

– при вручении лично или передачей иными способами – время получения.

Запрос на приостановление действия сертификата, полученный через АРМ и подписанный квалифицированной электронной подписью Удаленного оператора ЦР, обрабатывается УЦ автоматически в режиме реального времени.

11.5. Возобновление действия сертификата

11.5.1. Действие сертификата может быть возобновлено:

– по запросу Владельца сертификата;

– по запросу директора по персоналу и организационному развитию Общества;

– по запросу Удаленного оператора ЦР;

– по решению УЦ.

11.5.2. Запрос на возобновление действия сертификата может быть подан:

– Владельцем сертификата;

– директором по персоналу и организационному развитию Общества;

– Удаленным оператором ЦР;

– Уполномоченным лицом УЦ, если он располагает достоверной информацией, требующей возобновления действия сертификата, либо информацией об отсутствии причин для дальнейшего приостановления.

11.5.3. Запрос на возобновление действия сертификата может быть подан Владельцем сертификата и/или Удаленным оператором ЦР, действующим по заявке Владельца сертификата, в бумажной или электронной форме с аутентификацией по документу, удостоверяющему личность Владельца, или по сертификату Удаленного оператора ЦР при подаче запроса через АРМ. В любом случае запрос на возобновление действия сертификата должен содержать серийный номер сертификата или иную информацию, позволяющую однозначно идентифицировать сертификат.

11.5.4. После получения запроса на возобновление действия сертификата УЦ производит верификацию запроса, и если таковая прошла успешно, то производит возобновление действия сертификата. После возобновления действия сертификата владелец такового уведомляется, а СОС, не содержащий информацию о приостановлении сертификата, публикуется УЦ.

Запрос на возобновление действия сертификата, полученный от Владельца сертификата или от Руководителя дирекции по персоналу и организационному развития Общества, должен быть рассмотрен в течение 1 (одного) рабочего дня с момента его подачи.

Временем подачи запроса на возобновление действия сертификата считается:

– при передаче по электронной почте – время передачи сообщения на почтовый сервер УЦ;

– при вручении лично или передачей иными способами – время получения.

Запрос на возобновление действия сертификата, полученный через АРМ Удаленного оператора Центра регистрации и подписанный квалифицированной электронной подписью Удаленного оператора ЦР, обрабатывается УЦ автоматически в режиме реального времени.

12. Сервисы проверки статуса сертификата

12.1. Проверка статуса сертификатов осуществляется либо путем использования списков отозванных сертификатов, доступных в репозитории УЦ, либо с использованием сервисов online-проверки статуса сертификата, доступных круглосуточно.

13. Технические меры обеспечения безопасности

13.1. Работники Владельцы сертификатов, выпущенных непосредственно в аккредитованных удостоверяющих центрах, или ответственные за использование ЭП должны применять меры по обеспечению безопасности в соответствии с регламентами данных аккредитованных удостоверяющих центров и Порядком.

13.2. Управление эксплуатации информационных систем и связи обеспечивает работников в качестве средства электронной подписи сертифицированными ФСБ России средствами криптографической защиты (далее – СКЗИ) «КриптоПро CSP».

13.3. Ключи проверки ЭП должны быть доступны пользователям сертификатов.

13.4. Длина ключей электронной подписи должна быть следующей:

– закрытый ключ – 256 бит;

– открытый ключ – 512 бит (ГОСТ Р. 34.10-2001).

Длина ключей шифрования должна быть следующей:

– сессионный ключ для шифрования по ГОСТ 28147-89 – 256 бит;

– закрытый ключ – 256 бит;

– открытый ключ – 512 бит (на базе ГОСТ Р 34.10-2001).

Данные параметры ключей должны являться настройками СКЗИ по умолчанию.

14. Защита закрытого ключа и технический контроль ключевых носителей

14.1. Запрещается владельцам сертификатов или уполномоченным за эксплуатацию ЭП передавать ключ ЭП без согласования с подразделением информационной безопасности.

14.2. Формирование ключей ЭП производится на следующие типы носителей:

- Рутокен;
- eToken.

14.3. Копирование ключей ЭП на компьютер запрещено. Допускается резервное копирование и хранение резервных копий ключа ЭП с использованием методов и средств, обеспечивающих уровень защищенности не меньше уровня защищенности ключевого носителя.

14.4. Контроль ключа ЭП несколькими лицами недопустим.

14.5. Перенос ключа ЭП из ключевого носителя или в ключевой носитель должен осуществляться методами, гарантирующими его нераспространение.

14.6. При хранении ключа ЭП в ключевом носителе должны быть приняты меры, гарантирующие его нераспространение.

14.7. Активация ключа ЭП может осуществляться только Владельцем сертификата или ответственным за эксплуатацию электронной подписи. Для активации ключа ЭП должен использоваться пароль (PIN-код) пользователя, удовлетворяющий требованиям действующей политики парольной защиты. Активация ключа ЭП должна производиться на ограниченный период времени, необходимый для выполнения операции формирования электронной подписи, расшифрования данных или прохождения процедуры аутентификации в Системе электронного документооборота Общества. Пароль (PIN-код) пользователя должен защищаться от потери, кражи, разглашения, порчи, модификации или неавторизованного использования.

14.8. Деактивация ключа ЭП должна производиться либо автоматически, либо путем отключения работником ключевого носителя.

14.9. После окончания срока действия или архивного хранения, если таковое осуществляется, ключ ЭП уничтожается методами, гарантирующими невозможность его восстановления.

15. Конфиденциальность

15.1. Все работники должны не раскрывать и всячески препятствовать раскрытию Конфиденциальной информации третьим лицам за исключением случаев, требующих ее раскрытия в соответствии с действующим законодательством или при наличии судебного акта.

15.2. Конфиденциальной информацией считается:

- ключ ЭП;

– персональная и корпоративная информация владельцев сертификатов, содержащаяся в Удостоверяющем центре (далее – УЦ) и не подлежащая непосредственной рассылке в качестве части сертификата или списка отозванных сертификатов;

– информация, хранящаяся в журналах прикладных и операционных систем;

– информация о способах и порядке защиты аппаратного и программного обеспечения, способах администрирования и действий на случай непредвиденных ситуаций в Обществе;

– персональные данные, определенные Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных».

15.3. Информация, не являющейся конфиденциальной информацией, является открытой информацией. Открытая информация может публиковаться в соответствии с требованиями локальных нормативных актов Общества. Информация, включаемая в сертификаты и списки отозванных сертификатов, издаваемые УЦ, не считается конфиденциальной. При подписании Заявления на выпуск сертификата владелец сертификата знает, какая информация будет содержаться в сертификате, и согласен с ее публикацией. Вся информация, подлежащая публикации в соответствии с настоящей Политикой, также не считается конфиденциальной, если иное не предусмотрено действующим законодательством Российской Федерации.

15.4. Общество и УЦ должны осуществлять защиту персональных данных Владельцев сертификатов в соответствии с законодательством Российской Федерации.

Общество и УЦ должны защищать персональные данные Владельцев сертификатов и всячески препятствовать их раскрытию третьим лицам, действовать в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

Любое использование персональных данных возможно только с согласия их владельца. Заявление на выпуск сертификата считается согласием на использование указанных в заявлении персональных данных в сертификате.

Персональные данные, включаемые в сертификаты ключей подписей, издаваемые УЦ, относятся к общедоступным персональным данным.

Раскрытие персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации.

16. Возмещение ущерба

16.1. Работник обязан использовать выпущенный ему сертификат только в целях, для которых он ему был выпущен, и в пределах делегированных ему полномочий.

16.2. В случае самостоятельного получения работником сертификата (до момента возникновения трудовых отношений с Обществом) работник

обязуется использовать сертификат только в пределах делегированных ему полномочий.

16.3. За неисполнение или ненадлежащее исполнение положений настоящей Политики Общества Владельцы сертификатов несут ответственность в порядке, предусмотренном действующим законодательством Российской Федерации и положениями настоящей Политики.

16.4. Владелец сертификата несет ответственность за достоверность сведений, содержащихся в документах, представленных Обществу, а также сведений, публикуемых в сертификате работника и имеющих отношение к нему.

16.5. Общество не несет ответственности перед работниками и/или третьими лицами за ущерб, причиненный им в результате неправомерного использования сертификатов. Под неправомерным использованием сертификатов понимается следующее:

16.5.1. подписание работником документов с превышением своих полномочий;

16.5.2. подписание работником документов после отправки в УЦ запроса на приостановление действия его сертификата;

16.5.3. подписание работником документов после отправки в УЦ запроса на отзыв его сертификата;

16.5.4. подписание работником документов по истечении срока действия его сертификата;

16.5.5. подделка, подлог либо иное искажение информации третьими лицами в принадлежащих им сертификатах либо иных бумажных и электронных документах, с которыми Владелец сертификата ведет электронную переписку;

16.5.6. использование ключа электронной подписи лицом, не являющимся ответственным за использование ЭП или Владельцем сертификата, выпущенного на открытый ключ, соответствующий используемому ключу электронной подписи;

16.5.7. невыполнение Владельцем сертификата своих обязательств по настоящей Политике;

16.5.8. предоставление Владельцем сертификата заведомо ложной информации или непредоставление информации или материалов (документов) Общества в разумный срок по письменному или устному запросу Общества, а также утаивание информации Владельцем сертификата;

16.5.9. в иных случаях, при условии, что Общество выполнило все требования действующего законодательства Российской Федерации и положений настоящей Политики.

16.6. По обязательствам, принятым работником путем неправомерного использования им сертификата, Работник отвечает самостоятельно в полном объеме.

16.7. Владелец сертификата несет ответственность перед работодателем и третьими лицами за ущерб, причиненный им в результате неправомерного использования ЭП, в полном объеме.

17. Прочие положения

17.1. Настоящей Политике присвоен идентификатор (OID) 1.2.643.3.203.1.2.20, который указывается в сертификате Работника. В случае изменения настоящей Политики замена OID документа не осуществляется.

17.2. При возникновении споров Общество и УЦ предпринимают все необходимые шаги для урегулирования спорных вопросов, которые могут возникнуть в рамках настоящей Политики, путем переговоров. Споры между сторонами, связанные с действием настоящей Политики и не урегулированные в процессе переговоров, должны рассматриваться в Арбитражном суде в соответствии с действующим законодательством Российской Федерации.

17.3. Настоящая Политика вступает в силу с момента ее утверждения приказом генерального директора Общества.

17.4. Настоящая Политика может быть дополнена, изменена или отменена приказом генерального директора Общества.

17.5. В случае если по решению суда какие-либо положения настоящей Политики будут признаны не имеющими юридической силы, оставшиеся положения все равно остаются действительными.

17.6. Во всех случаях, не урегулированных настоящей Политикой, Общество руководствуется действующим законодательством Российской Федерации.

18. Вопросы и сомнения

18.1. Настоящая Политика находится в ведении Дирекции по информационным технологиям.

18.2. В случае возникновения вопросов или сомнений относительно применения тех или иных положений настоящей Политики работники должны обращаться к Удаленному оператору ЦР или в Управление по противодействию иностранным техническим разведкам и технической защите информации.