

ЗАО «Сигнал-КОМ»

УТВЕРЖДЁН

ШКНР.00054-01 90 03-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС
УДОСТОВЕРЯЮЩЕГО ЦЕНТРА
«NOTARY-PRO 2.8»

Руководство по безопасности

ШКНР.00054-01 90 03

Листов 33

2019

СОДЕРЖАНИЕ

Содержание	2
1. Введение.....	3
1.1. Список сокращений.....	3
2. Организация работ по защите информации в УЦ.....	5
3. Использование СКЗИ.....	7
4. Защита средств УЦ от НСД.....	8
5. Требования к идентификации и аутентификации	10
6. Защита УЦ от НСД при сетевом взаимодействии	12
6.1. Модель нарушителя	12
6.2. Типовые схемы размещения	13
6.3. Настройка межсетевого экрана и серверных компонентов ПАК УЦ	18
7. Разграничение доступа к функциям УЦ	20
7.1. Ролевое разграничение доступа к функциям УЦ.....	20
7.2. Объекты защиты (доступа) УЦ.....	21
8. Контроль целостности	24
8.1. Контроль целостности программного обеспечения.....	24
8.2. Контроль целостности технических средств	26
9. Требования к серверным и рабочим помещениям УЦ	28
9.1. Серверное помещение.....	28
9.2. Помещения обслуживающего персонала УЦ.....	28
9.3. Архивное хранение	28
10. Требования по установке программного обеспечения	29
11. Требования по условиям эксплуатации	32
Литература	33

1. ВВЕДЕНИЕ

Настоящий документ определяет требования и рекомендации для обеспечения защиты информации при установке и использовании программно-аппаратного комплекса удостоверяющего центра «Notary-PRO 2.8» (далее – ПАК УЦ «Notary-PRO»). Указанные в данном руководстве ограничения должны быть включены в должностные инструкции и функциональные обязанности сотрудников, ответственных за эксплуатацию удостоверяющего центра (далее – УЦ).

Для реализации функций защиты информации при установке и использовании ПАК УЦ «Notary-PRO» необходимо выполнение организационно-технических мероприятий по обеспечению правильности функционирования программных и технических средств УЦ в процессе обработки и передачи информации, а также выполнение соответствующих правил для обслуживающего персонала УЦ.

Компоненты ПАК УЦ «Notary-PRO» обеспечивают поддержку алгоритмов создания и проверки электронной подписи ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2001¹ и ГОСТ Р 34.11-94. Порядок функционирования ПАК УЦ в соответствии с положениями эксплуатационной документации в составе согласно Формуляра ШКНР.00054-01 30 01, не допускает использования других алгоритмов создания и проверки электронной подписи.

1.1. Список сокращений

АРМ	-	автоматизированное рабочее место
БД	-	база данных
ЛВС	-	локальная вычислительная сеть
МЭ	-	межсетевой экран
НСД	-	несанкционированный доступ
ОС	-	операционная система
ПАК	-	программно-аппаратный комплекс
ПО	-	программное обеспечение
РЦ	-	регистрационный центр
СКЗИ	-	средство криптографической защиты информации
СОП	-	сеть общего пользования

¹ Использование ГОСТ Р 34.10-2001 ограничено в соответствии с п. 3.6 Формуляра ШКНР.00054-01 30 01.

- УЦ - удостоверяющий центр
- ЭВМ - электронная вычислительная машина
- ЭП - электронная подпись

2. ОРГАНИЗАЦИЯ РАБОТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В УЦ

В организации, эксплуатирующей удостоверяющий центр, должен быть назначен Администратор безопасности УЦ, на которого возлагаются задачи по обеспечению работ в области информационной безопасности при использовании ПАК УЦ «Notary-PRO», выработки соответствующих инструкций для сотрудников УЦ, а также контроль за соблюдением требований, описанных в настоящем руководстве.

Правом доступа к рабочим местам с установленными компонентами ПАК УЦ «Notary-PRO» должны обладать только лица, прошедшие соответствующую подготовку. Администратор безопасности УЦ должен ознакомить под роспись каждого сотрудника УЦ, эксплуатирующего компоненты ПАК УЦ «Notary-PRO», с документацией на ПАК УЦ «Notary-PRO», а также с другими нормативными документами, созданными на её основе.

При организации работ по защите информации в УЦ должна быть обеспечена конфиденциальность и целостность информации.

Конфиденциальной считается следующая информация о пользователях УЦ:

- ключи электронной подписи (далее – ЭП), создаваемые по заявкам пользователей УЦ, обратившихся за получением сертификатов ключей проверки электронных подписей (далее – сертификаты);
- специальная парольная фраза для связи пользователя УЦ с Администратором УЦ по телефону;
- персональные данные владельцев сертификатов ключей проверки ЭП, не подлежащие включению в сертификат владельца;
- информация, конфиденциальность которой охраняется удостоверяющим центром в соответствии с договорами и локальными нормативными актами УЦ.

Набор данных, представляющий собой совокупность персональных сведений о пользователях УЦ, подлежит защите в соответствии с режимом, принятым для конфиденциальной информации.

Контроль целостности данных должен обеспечиваться в отношении следующей информации:

- сведения, включаемые в сертификаты ключей проверки ЭП;

- сведения, включаемые в списки аннулированных сертификатов ключей проверки ЭП, издаваемые удостоверяющим центром.

3. ИСПОЛЬЗОВАНИЕ СКЗИ

В ПАК УЦ «Notary-PRO» выполнение всех криптографических операций, необходимых для реализации функций удостоверяющего центра, а также контроль целостности программного обеспечения, с целью его защиты от несанкционированного изменения или нарушения правильности функционирования, обеспечивается с использованием СКЗИ «CADB 2.1» (вариант исполнения 2) [2], СКЗИ «Signal-COM JCP 3.1» (вариант исполнения 2) [3] и СКЗИ «Крипто-КОМ 3.3» (вариант исполнения 8) [4], реализующих следующие криптографические алгоритмы:

- создание ключей ЭП и ключей проверки ЭП в соответствии с ГОСТ Р 34.10-2012;
- создание ЭП в соответствии с ГОСТ Р 34.10-2012;
- проверка ЭП в соответствии с ГОСТ Р 34.10-2012 или ГОСТ Р 34.10-2001;
- выработка значения хэш-функции в соответствии с ГОСТ Р 34.11-2012 или ГОСТ Р 34.11-94;
- зашифрование/расшифрование данных и вычисление имитовставки в соответствии с ГОСТ 28147-89.

Средства ЭП, предоставляемые удостоверяющим центром конечным пользователям для создания ключа ЭП и ключа проверки ЭП, обеспечивают выполнение указанных функций с использованием СКЗИ «Крипто-КОМ 3.3» (варианты исполнения 7, 8) [4], СКЗИ «Signal-COM JCP 3.1» (варианты исполнения 1, 2) [3].

При эксплуатации СКЗИ в составе ПАК УЦ необходимо выполнять требования организационно-технических и административных мероприятий, описанных в Правилах пользования СКЗИ.

4. ЗАЩИТА СРЕДСТВ УЦ ОТ НСД

Защита от НСД средств УЦ и информации, циркулирующей в УЦ, должна обеспечиваться во всех режимах функционирования УЦ и на всех технологических этапах обработки информации, в том числе при проведении ремонтных и регламентных работ.

Защита средств УЦ от НСД обеспечивается установкой на компьютеры со средствами УЦ программно-аппаратных комплексов защиты от НСД, указанных в эксплуатационной документации на СКЗИ и сертифицированных ФСБ России по «Требованиям к аппаратно-программным модулям доверенной загрузки ЭВМ» по классу не ниже 2Б.

Защита средств УЦ от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости руководителем УЦ или Администратором безопасности УЦ.

Программные компоненты ПАК УЦ «Notary-PRO» должны использоваться совместно с антивирусными средствами защиты, сертифицированными по требованиям ФСБ России.

При организации работ по защите средств УЦ от НСД сотрудникам УЦ запрещается:

- оставлять без контроля вычислительные средства, на которых эксплуатируется ПО УЦ, после ввода ключевой информации либо иной конфиденциальной информации;
- использовать ПО УЦ в случае обнаружения отказа оборудования программно-аппаратных комплексов защиты от НСД, либо программного обеспечения защиты от НСД;
- вносить какие-либо изменения в программное обеспечение ПО УЦ;
- осуществлять несанкционированное Администратором безопасности УЦ копирование ключевых носителей; при создании резервных копий ключевых носителей необходимо руководствоваться требованиями к управлению ключевой информацией, определенными в эксплуатационной документации на СКЗИ, используемое в составе ПАК УЦ;

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;
- использовать ключи ЭП удостоверяющего центра, предназначенные для подписи сертификатов ключей проверки ЭП и списков аннулированных сертификатов, создаваемых удостоверяющим центром, для каких-либо иных целей;
- записывать на ключевые носители постороннюю информацию.

5. ТРЕБОВАНИЯ К ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

При осуществлении локального доступа к средствам ПАК УЦ еще до их перехода в рабочее состояние и до загрузки базовой ОС должна выполняться идентификация и аутентификация пользователей средств УЦ (сотрудников УЦ или членов групп администраторов средств УЦ) с помощью программно-аппаратных комплексов защиты от НСД, установленных на компьютеры со средствами УЦ в соответствии с требованиями эксплуатационной документации на используемое СКЗИ. При этом идентификация обеспечивается с помощью реализованного в системе контроля доступа средства защиты от НСД механизма персональных электронных идентификаторов, а аутентификация - с помощью паролевой защиты.

На этапе последующей загрузки программного обеспечения средства УЦ или в процессе его эксплуатации для распознавания пользователей средств УЦ используется дополнительная аутентификация по паролю.

Реализованный в ПАК УЦ механизм аутентификации по паролю блокирует доступ субъектов аутентификации к функциям УЦ не менее чем на 60 секунд, после трёх попыток ввода неверного пароля.

Требования к организации парольной защиты распространяются на следующие пароли, используемые в УЦ:

- пароль для доступа к главному ключу УЦ (см. [1], п.2.9.1);
- пароли для учетных записей ОС;
- пароли для учетных записей БД;
- пароли на ключевые носители.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в УЦ и контроль за действиями сотрудников УЦ при работе с паролями возлагается на Администратора безопасности УЦ.

Пароли, используемые в УЦ, должны генерироваться и распределяться централизованно, либо выбираться сотрудниками УЦ самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (USER, ADMIN и т.д.);
- плановая смена пароля должна проводиться не реже одного раза в 6 месяцев;
- личный пароль сотрудник УЦ не имеет права сообщать никому.

Сотрудники УЦ должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Вопрос необходимости централизованной генерации паролей решается Администратором безопасности УЦ.

Если формирование паролей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на Администратора безопасности УЦ.

Внеплановая смена пароля или удаление учетной записи сотрудника УЦ в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) должна производиться Администратором безопасности УЦ немедленно после окончания последнего сеанса работы данного сотрудника с УЦ.

Внеплановая, полная смена паролей всех сотрудников УЦ должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) Администратора безопасности УЦ.

В случае компрометации личного пароля сотрудника УЦ должны быть немедленно предприняты меры по внеплановой смене скомпрометированного личного пароля.

Хранение сотрудником УЦ значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.

Повседневный и периодический контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на Администратора безопасности УЦ.

Не допускается использование одного и того же пароля для защиты нескольких ключей электронной подписи.

6. ЗАЩИТА УЦ ОТ НСД ПРИ СЕТЕВОМ ВЗАИМОДЕЙСТВИИ

При необходимости взаимодействия средств ПАК УЦ «Notary-PRO» между собой, их подключение к информационно-телекоммуникационным сетям должно осуществляться в соответствии со схемами, приведенными на рисунках 1-3 в п.6.1. При этом использование сетей общего пользования, доступ к которым не ограничен определенным кругом лиц, допускается только в качестве транспортного канала, защищенного с помощью СКЗИ, имеющего сертификат или положительное заключение ФСБ России о соответствии «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по классу не ниже KB2.

При подключении средств УЦ к каналам связи, совместно с ПАК УЦ «Notary-PRO» необходимо использовать межсетевые экраны (МЭ), удовлетворяющие требованиям не ниже 4 класса защищенности в соответствии с требованиями ФСБ России к устройствам типа межсетевые экраны.

Средства ПАК УЦ «Notary-PRO 2.8» (за исключением компонентов OCSP Server и TSP Server) не предназначены для подключения к информационно-телекоммуникационной сети, доступ к которой не ограничен определенным кругом лиц (в том числе к информационно-телекоммуникационной сети «Интернет»).

Доставка в УЦ запросов на создание сертификатов ключей проверки ЭП с использованием информационно-телекоммуникационной сети, доступ к которой не ограничен определенным кругом лиц (в том числе с использованием информационно-телекоммуникационной сети «Интернет»), запрещена.

6.1. Модель нарушителя

ПАК УЦ «Notary-PRO» имеет сертификат ФСБ России о соответствии «Требованиям к средствам удостоверяющего центра» и «Требованиям к информационной безопасности удостоверяющих центров» ФСБ России, установленным для класса KC2, что обеспечивает защиту от воздействий нарушителей типа Н1 и Н2:

H_1 - нарушитель из числа лиц, не имеющих права доступа в контролируемую зону и не имеющих доступа к функциональным возможностям программно-аппаратных средств взаимодействия с УЦ, самостоятельно осуществляющий создание способов атак, подготовку и проведение атак;

H_2 - нарушитель из числа лиц, имеющих право постоянного или разового доступа в контролируемую зону, не имеющих права доступа к средствам вычислительной техники (СВТ), на которых реализован УЦ, самостоятельно осуществляющий создание способов атак, подготовку и проведение атак.

При подключении ПАК УЦ «Notary-PRO» к сетям общего пользования меры информационной безопасности, реализованные в ПАК УЦ «Notary-PRO», не обеспечивают защиту от нарушителя, возможности которого превосходят уровень защиты КС2.

6.2. Типовые схемы размещения

На рис.1 приводится типовая схема размещения компонентов ПАК УЦ «Notary-PRO» в пределах одной контролируемой зоны², без подключения каналов их взаимодействия к сетям общего пользования.

Данная схема размещения технических средств ПАК УЦ определяет модель нарушителя, возможности которого не превосходят уровень защиты КС2 и действия которого могут быть блокированы организационно-техническими мероприятиями, определенными в эксплуатационной документации ПАК УЦ «Notary-PRO» в составе согласно Формуляра ШКНР.00054-01 30 01.

² Контролируемая зона – пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и (или) транспортных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

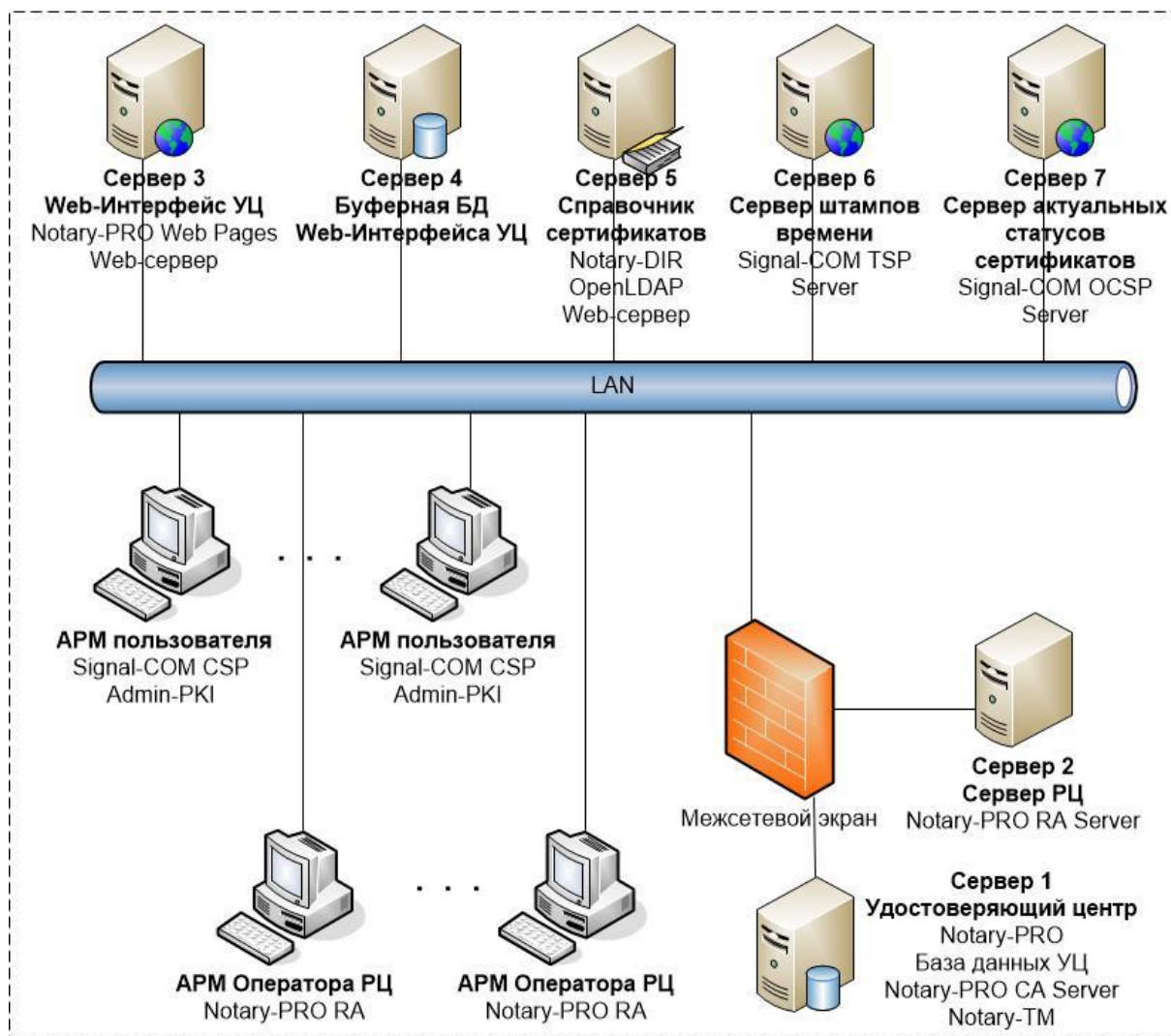


Рис.1. Схема размещения компонентов ПАК УЦ «Notary-PRO» в пределах одной контролируемой зоны

Схема размещения компонентов ПАК УЦ, приведенная на рис.1, позволяет автоматизировать следующие процессы в локальной сети ПАК УЦ, без нарушения требований информационной безопасности УЦ:

- публикацию сертификатов ключей проверки электронной подписи и списков аннулированных сертификатов ключей проверки электронной подписи (далее - САС) с помощью транспортного модуля «Notary-TM», обеспечивающего передачу сертификатов и САС из базы данных УЦ (Сервер 1) в справочник (реестр) сертификатов на сервере LDAP (Сервер 5); более подробно процедура публикации в реестре описана в [7];

- импорт в УЦ «Notary-PRO» запросов пользователей на создание сертификатов ключей проверки ЭП, поступающих через веб-интерфейс УЦ «Notary-PRO Web Pages» (Сервер 3) в буферную базу данных УЦ на Сервере 4, откуда приложение «Notary-PRO» или сервер УЦ «Notary-PRO CA Server» (на Сервере 1) с определенной периодичностью импортируют файлы запросов в базу данных УЦ (Сервер 1).

На рис.2 приводится типовая схема размещения компонентов ПАК УЦ «Notary-PRO» в различных контролируемых зонах, объединяемых каналами выделенной сети связи с ограниченным доступом, не имеющей подключения к сетям общего пользования (см. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи», гл.3, ст.14).

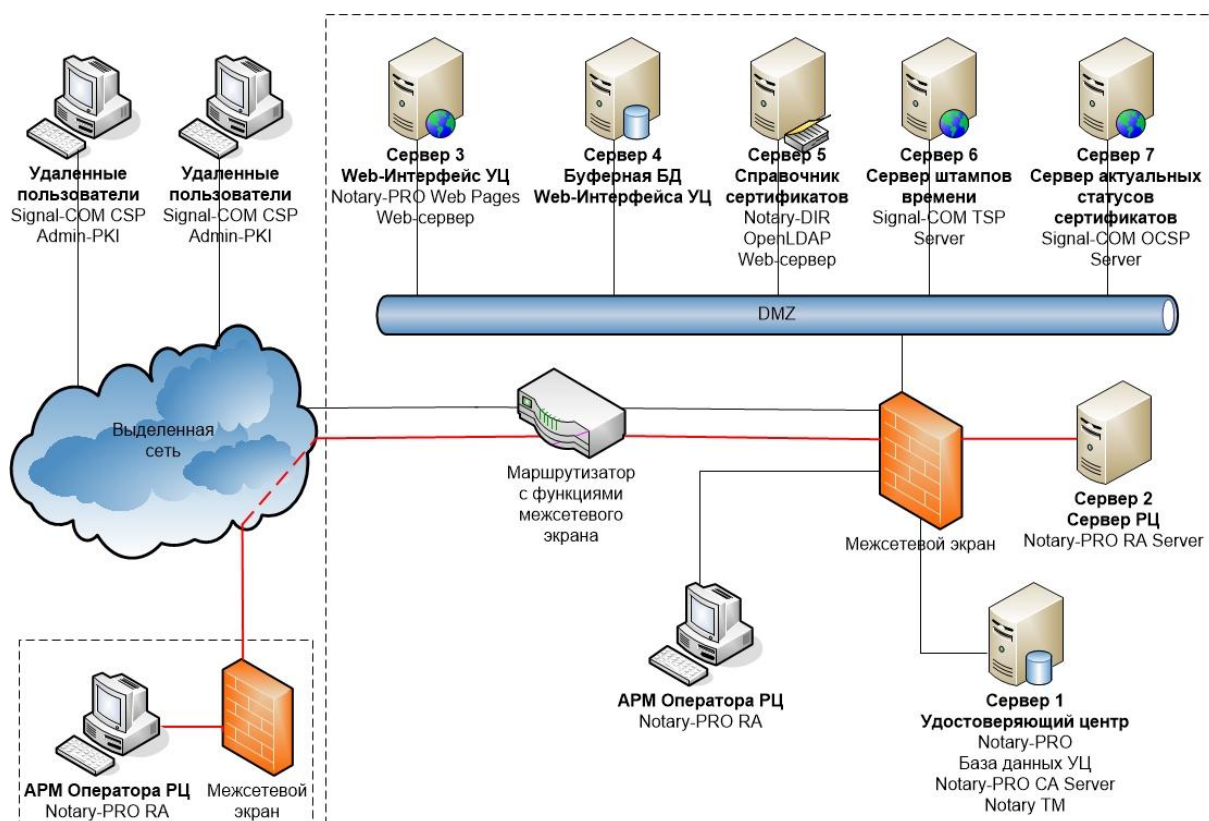


Рис.2. Схема размещения компонентов ПАК УЦ «Notary-PRO» при взаимодействии через выделенную сеть связи с ограниченным доступом

Отсутствие подключения к сетям общего пользования, а также настройки межсетевого экрана и сетевые настройки на серверах с установленными компонентами ПАК УЦ (см. описание в п.6.3), определяют в данной схеме размещения модель нарушителя, возможности которого не превосходят уровень защиты КС2, при условии

изоляции выделенной сети связи от сетей общего пользования, гарантируемой оператором связи.

Соответственно, так же, как и в случае размещения средств ПАК УЦ в пределах одной контролируемой зоны (рис.1), схема размещения на рис.2 допускает возможность организации автоматической публикации сертификатов и СОС в справочнике (реестре) сертификатов на сервере LDAP (Сервер 5) и автоматического импорта файлов запросов, поступивших от удаленных пользователей через выделенную сеть, из буферной базы данных веб-интерфейса УЦ (Сервер 4) в основную базу данных УЦ (Сервер 1).

На рис.3 приводится типовая схема размещения компонентов ПАК УЦ «Notary-PRO» в различных контролируемых зонах, объединяемых каналами связи сетей общего пользования (включая Интернет). В отличие от схем размещения, представленных на рис. 1 и 2, схема с подключением средств ПАК УЦ к сетям общего пользования определяет модель нарушителя, с возможностями, превосходящими уровень защиты КС2, которому соответствует ПАК УЦ «Notary-PRO».

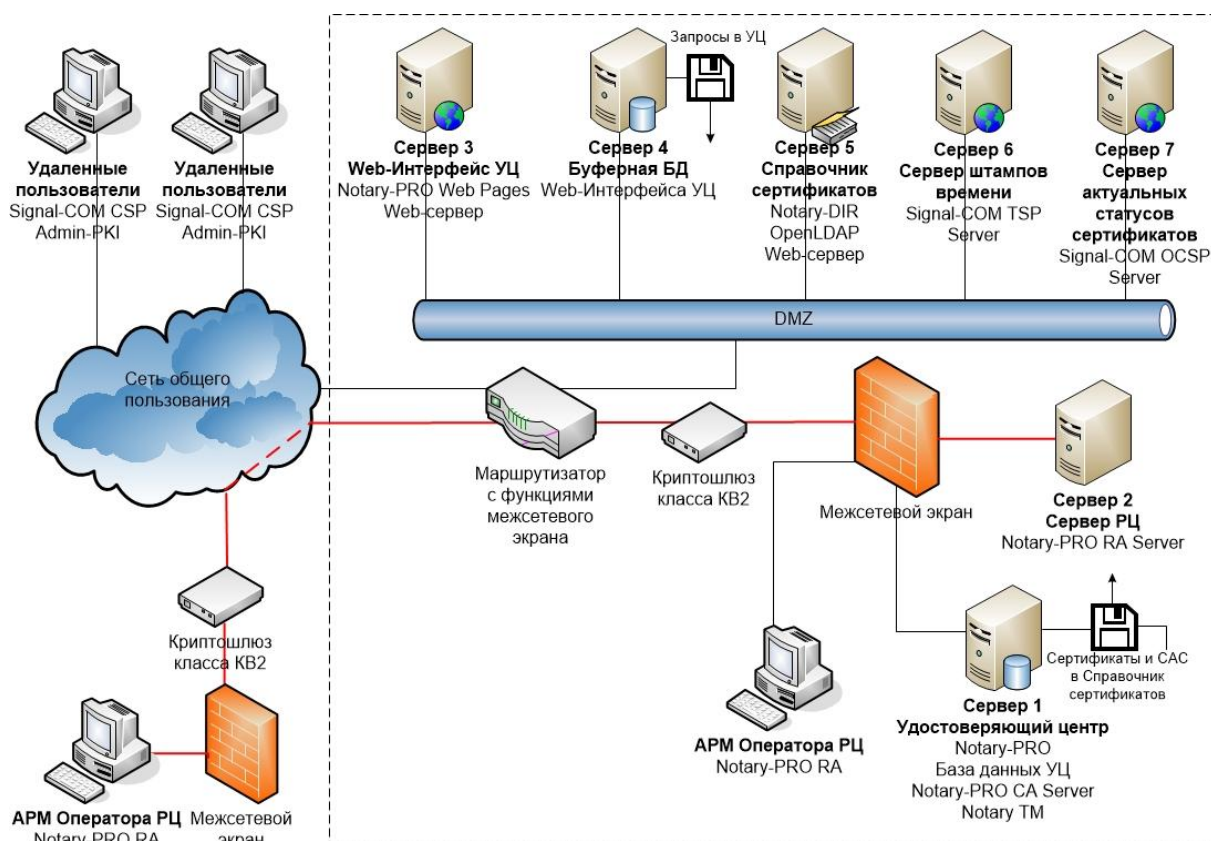


Рис. 3. Схема размещения компонентов ПАК УЦ «Notary-PRO» при взаимодействии через сети общего пользования

Защищенное взаимодействие средств ПАК УЦ, осуществляемое через сети общего пользования, доступ к которым не ограничен определенным кругом лиц, должно обеспечиваться установкой на входе в контролируемую зону УЦ средства VPN (криптошлюз) со встроенным СКЗИ, имеющим сертификат или положительное заключение ФСБ России о соответствии «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по классу не ниже KB2.

В схеме с подключением сервера LDAP к сетям общего пользования (см. рис.3) автоматическая публикация сертификатов ключей проверки ЭП и списков аннулированных сертификатов ключей проверки ЭП в справочнике сертификатов «Notary-DIR» возможна только в случае гарантированной изоляции сервера LDAP от доступа нарушителя из сети общего пользования. В противном случае, публикация сертификатов и САС в справочнике сертификатов должна выполняться вручную Администратором УЦ, путем экспорта необходимых файлов сертификатов и САС из удостоверяющего центра на отчуждаемый носитель и их последующего импорта в справочник сертификатов через консоль сервера LDAP (более подробно см. [7]).

Точно так же автоматический импорт запросов пользователей из буферной базы данных «Notary-PRO Web Pages» в базу данных УЦ возможен только в случае гарантированной изоляции буферной базы данных УЦ от доступа нарушителя из сети общего пользования. В противном случае, импорт запросов в базу данных УЦ должен выполняться вручную Администратором УЦ, путем переноса файлов на отчуждаемом носителе с Сервера 4 на Сервер 1.

В схемах размещения компонентов ПАК УЦ, допускающих подключение удаленных пользователей к УЦ через веб-интерфейс «Notary-PRO Web Pages», для защиты канала сетевого взаимодействия между браузерами пользователей и Web-сервером УЦ (Сервер 3) от навязывания ложной информации и модифицированного программного обеспечения рекомендуется использовать внешние средства VPN со встроенными СКЗИ, имеющим сертификат или положительное заключение ФСБ России, обеспечивающие надежную аутентификацию веб-сервера УЦ и защиту трафика в канале от НСД (например, средства защиты веб-приложений, реализующие протокол TLS с использованием СКЗИ).

Через незащищенный веб-интерфейс «Notary-PRO Web Pages» допускается передача только файлов запросов на создание сертификатов ключей проверки ЭП, заранее сформированных в режиме off-line средством ЭП со встроенным СКЗИ (имеющим сертификат или положительное заключение ФСБ России), установленным на рабочем месте пользователя из дистрибутива, полученного по доверенному каналу. Защита от навязывания ложной информации в полях запросов на сертификат формата PKCS #10, поступающих в УЦ через веб-интерфейс, обеспечивается их обязательной проверкой перед сертификацией Администратором УЦ в соответствии с регламентом удостоверяющего центра [8]. Запросы на сертификат формата СМС, защищенные действующей электронной подписью пользователя, перед сертификацией подлежат обязательной проверке ЭП средствами УЦ [1].

6.3. Настройка межсетевого экрана и серверных компонентов ПАК УЦ

Согласно приведенным схемам, совместно с ПАК УЦ «Notary-PRO» должен использоваться межсетевой экран, сертифицированный ФСБ России по требованиям к межсетевым экранам не ниже 4-го класса защиты, подключенный внешним интерфейсом к внешним каналам связи, а внутренними – к ресурсам УЦ, настроенным следующим образом:

- **Сервер 1 – УЦ «Notary-PRO», «Notary-PRO CA Server», «Notary-TM»;** на Сервере 1 должны быть закрыты все UDP и TCP порты, кроме портов 1433 (при использовании СУБД MS SQL) и 1525 (при использовании СУБД Oracle), через которые обеспечивается локальный доступ «Notary-PRO RA Server», расположенного на Сервере 2, к БД УЦ на Сервере 1;
- **Сервер 2 – «Notary-PRO RA Server»;** на Сервере 2 должны быть закрыты все TCP и UDP порты, кроме TCP порта 443 https-протокола, поверх которого обеспечивается взаимодействие АРМ Операторов Регистрационных центров (РЦ) «Notary-PRO RA» с сервером РЦ «Notary-PRO RA Server», защищаемое встроенными средствами ПАК УЦ «Notary-PRO», реализованными на базе СКЗИ «CADB 2.1» (вариант исполнения 2) (аутентификация сторон по сертификатам и электронная подпись транзакций);
- **Сервер 3 – веб-интерфейс УЦ «Notary-PRO Web Pages»;** на Сервере 3 должен быть открыт порт 80 и рекомендуется организовать парольную аутентификацию пользователей, от которых поступают запросы на

сертификацию, импортируемые далее в буферную БД Web-интерфейса УЦ на Сервере 4;

- **Сервер 4 – буферная БД веб-интерфейса УЦ;** на Сервере 4 должны быть закрыты все UDP и TCP порты, кроме портов 1433 (при использовании СУБД MS SQL) и 1525 (при использовании СУБД Oracle), через которые обеспечивается локальный доступ к буферной БД УЦ с Сервера 1 и с Сервера 3;
- **Сервер 5 – справочник сертификатов «Notary-DIR»;** на Сервере 5 должен быть открыт порт 389 – для доступа по протоколу LDAP.
- **Сервер 6 – сервер штампов времени «Signal-COM TSP Server»;** на Сервере 6 должен быть открыт порт 80 – для доступа по протоколу HTTP.
- **Сервер 7 – сервер актуальных статусов сертификатов «Signal-COM OCSP Server»;** на Сервере 7 должен быть открыт порт 80 – для доступа по протоколу HTTP.

Настройка МЭ должна осуществляться по принципу: «всё, что не разрешено, то запрещено», а также на основе следующих правил фильтрации:

- для компьютера Сервера 1 должен быть разрешен доступ только с IP-адреса Сервера 2 к портам БД УЦ 1433 (при использовании СУБД MS SQL) и 1525 (при использовании СУБД Oracle);
- для компьютера Сервера 2 должен быть разрешен доступ только с фиксированных IP-адресов АРМ Операторов РЦ «Notary-PRO RA» к TCP порту 443;
- для компьютера Сервера 4 должен быть разрешен доступ только с IP-адресов Сервера 1 и Сервера 3 к портам буферной БД УЦ 1433 (при использовании СУБД MS SQL) и 1525 (при использовании СУБД Oracle);
- для компьютера Сервера 5 должен быть разрешен доступ к портам 389.

7. РАЗГРАНИЧЕНИЕ ДОСТУПА К ФУНКЦИЯМ УЦ

7.1. Ролевое разграничение доступа к функциям УЦ

Для обеспечения функционирования программно-аппаратного комплекса удостоверяющего центра используется ролевое разграничение членов группы администраторов и сотрудников, обслуживающих ПАК УЦ:

- Руководитель УЦ – выполняет организационно-административные функции, осуществляя контроль за деятельностью удостоверяющего центра, в том числе за обслуживающим персоналом, в целях соблюдения установленных правил работы в удостоверяющем центре;
- Системный администратор – сотрудник УЦ, выполняющий функции администрирования общесистемного программного обеспечения и сетевых компонентов, необходимых для функционирования элементов инфраструктуры ПАК УЦ «Notary-PRO» (УЦ, РЦ, справочника сертификатов); отвечает за установку, настройку, бесперебойную эксплуатацию и проведение профилактических работ общесистемного ПО и сетевых компонентов;
- Администратор безопасности УЦ – обеспечивает контроль за состоянием информационной безопасности удостоверяющего центра, а также проводит работы в области информационной безопасности в соответствии с требованиями разделов 0 - 0 настоящего документа; обеспечивает установку и администрирование программно-аппаратных средств, реализующих меры защиты от НСД и контроль целостности программных средств ПАК УЦ;
- Администратор УЦ – уполномоченное лицо удостоверяющего центра, отвечающее за создание ключа электронной подписи и сертификата ключа проверки электронной подписи УЦ, их эксплуатацию, обновление и уничтожение; отвечает за функционирование УЦ, обеспечивая выполнение интегрированного набора услуг по формированию (при необходимости), сертификации и обслуживанию ключей проверки электронной подписи Пользователей УЦ; выполняет регистрацию, создание сертификатов ключей проверки ЭП и назначение полномочий для удаленных РЦ; обеспечивает установку, конфигурацию, бесперебойную эксплуатацию и проведение профилактических работ программных и технических средств УЦ, серверного

компонента РЦ и справочника сертификатов; обеспечивает формирование отчетной документации и выдачу Пользователям УЦ необходимого программного обеспечения;

- Дежурные Администраторы УЦ – сотрудники УЦ, ответственные за хранение ключевых носителей с частями ключевого контейнера, обеспечивающего защиту ключей электронной подписи УЦ (при использовании схемы «разделения секрета» активация ключа электронной подписи УЦ осуществляется только при предъявлении количества ключевых контейнеров не меньше порогового значения);
- Администратор РЦ - обеспечивает установку, настройку и бесперебойное функционирование ПО РЦ; выполняет контроль за состоянием информационной безопасности РЦ;
- Оператор РЦ – отвечает за функционирование регистрационного центра, обеспечивая выполнение процедур по регистрации и обслуживанию ключей проверки электронной подписи Пользователей УЦ; отвечает за формирование отчетной документации и выдачу Пользователям УЦ необходимого программного обеспечения; обеспечивает формирование ключей электронной подписи и запроса для получения сертификата Оператора РЦ, необходимого для аутентифицируемого защищенного взаимодействия с удаленным сервером РЦ.

При необходимости, в удостоверяющем центре в одном лице могут совмещаться функции Администратора УЦ и Администратора безопасности, а в регистрационном центре – функции Администратора РЦ и Оператора РЦ.

7.2. Объекты защиты (доступа) УЦ

В Таблице 2 приводится перечень объектов удостоверяющего центра, в отношении которых необходимо обеспечивать разграничение и контроль доступа, дается список сотрудников УЦ (субъектов доступа), которым разрешен доступ к защищаемым объектам УЦ в соответствии с назначенными им полномочиями (ролями), и указывается используемый механизм разграничения доступа.

Руководитель УЦ выполняет организационно-административные функции и не имеет непосредственного доступа к объектам ПАК УЦ «Notary-PRO».

№ п/п	Объект доступа	Субъект доступа	Механизм
1. Технические средства			
1.1.	Технические средства и сетевые компоненты	Системный администратор Администратор безопасности УЦ Администратор УЦ Администратор РЦ Оператор РЦ	организационные меры по ограничению доступа в помещения
1.2.	Системное программное обеспечение	Системный администратор Администратор безопасности УЦ Администратор УЦ Администратор РЦ Оператор РЦ	учетные записи членов группы Администраторов операционной системы, функционирующей на компьютерах с установленным программным обеспечением из состава ПАК УЦ учетные записи членов группы Пользователей (Users) операционной системы, функционирующей на компьютерах с установленным программным обеспечением из состава ПАК УЦ
2. Функции УЦ			
2.1.	Удостоверяющий центр с функциями регистрации запросов и сертификации («Notary-PRO», «Notary-PRO CA Server»)	Администратор УЦ	1) электронный ключ HardLock 2) пароль к главному ключу УЦ 3) ПАК защиты от НСД

№ п/п	Объект доступа	Субъект доступа	Механизм
2.2	Ключ электронной подписи УЦ	Администратор УЦ (Уполномоченное лицо УЦ) Дежурные Администраторы УЦ	1) съемный ключевой контейнер для защиты ключей электронной подписи УЦ в соответствии с требованиями СКЗИ «Крипто-КОМ 3.3» или несколько ключевых контейнеров в случае использования схемы с разделением секрета; 2) главный ключ УЦ, на котором дополнительно зашифрованы ключи электронной подписи УЦ
2.3	БД УЦ «Notary-PRO»	Администратор УЦ	имя пользователя и пароль к базе данных УЦ
3. Функции РЦ			
3.1.	Сервер регистрационного центра («Notary-PRO RA Server»)	Администратор УЦ Оператор РЦ	1) электронный ключ HardLock 2) аутентификация по сертификату Оператора РЦ 3) ПАК защиты от НСД
3.2.	Регистрационный центр («Notary-PRO RA»)	Администратор РЦ сервер РЦ	1) электронный ключ HardLock; 2) аутентификация по сертификату сервера РЦ 3) ПАК защиты от НСД
4.	Справочник сертификатов («Notary-DIR»)	Администратор УЦ	учетная запись члена группы Администраторов операционной системы
5.	Сервер штампов времени («TSP Server»)	Администратор УЦ	учетная запись члена группы Администраторов операционной системы
6.	Сервер онлайн-проверки статуса сертификатов («OCSP Server»)	Администратор УЦ	учетная запись члена группы Администраторов операционной системы
7. Удаленная регистрация запросов			
7.1	Веб-интерфейс УЦ («Notary-PRO Web Pages»)	Администратор УЦ	учетная запись члена группы Администраторов операционной системы
7.2	Веб-служба УЦ («Notary-PRO Web Service»)	Администратор УЦ	учетная запись члена группы Администраторов операционной системы
7.3	Буферная БД «Notary-PRO Web Pages»	Администратор УЦ	имя пользователя и пароль к буферной базе данных УЦ

8. КОНТРОЛЬ ЦЕЛОСТНОСТИ

8.1. Контроль целостности программного обеспечения

Контролю целостности подлежат следующие программные компоненты из состава программного обеспечения, эксплуатируемого удостоверяющим центром:

- Notary-PRO;
- Notary-PRO CA Server;
- Notary-PRO RA;
- Notary-PRO RA Server;
- Notary-PRO Web Pages;
- Notary-PRO Web Service;
- Notary-DIR;
- Notary-TM;
- TSP Server;
- OCSP Server;
- Arbiter-PKI.

В качестве средства контроля целостности программных компонентов ПАК УЦ необходимо использовать программно-аппаратные комплексы защиты от НСД, определенные в эксплуатационной документации на СКЗИ и сертифицированные ФСБ России по «Требованиям к аппаратно-программным модулям доверенной загрузки ЭВМ» по классу не ниже 2Б.

Контролю целостности подлежат все файлы, входящие в дистрибутив компонентов ПАК УЦ, включая конфигурационные файлы, файлы с программным кодом и с кодом интерпретируемых языков. Дистрибутив каждого компонента ПАК УЦ содержит файл с соответствующими вычисленными контрольными суммами.

Контроль целостности и контроль лицензионной чистоты установленного ПО выполняется перед вводом удостоверяющего центра в эксплуатацию, а также в ходе выполнения регламентных работ и проведения проверки на отсутствие программных закладок.

Перечень наиболее важных файлов, подлежащих контролю целостности для каждого компонента, приведен в следующей таблице:

Компонент	Файлы, подлежащие контролю целостности
СКЗИ «CADB 2.1» в составе компонентов ПАК УЦ	cadb.dll, libcadb.so
СКЗИ «Signal-COM JCP 3.1» в составе компонентов ПАК УЦ	sccsp.jar
СКЗИ «Крипто-КОМ 3.3» в составе компонентов ПАК УЦ	mespro.dll, libmespro.so
Notary-PRO	Notary3m.exe PropertyGridCOM.dll stack.dll Notary3m.ini
Notary-PRO CA Server	NotaryCASvr.exe NotaryCASetup.exe CASvrMsg.dll stack.dll
Notary-PRO RA Server	NotaryRASvSetup.exe NotaryRASvr.exe RASvrMsg.dll DataRequest.dll
Notary-PRO RA	Notary3mRa.exe NotaryRASvrProxy.dll DataRequest.dll PropertyGridCOM.dll Notary3mRA.ini
Notary-PRO Web Pages	mespro.dll
Notary-PRO Web Service	libmespro.so
TSP Server	tsp-server.war sccsp.jar sccms.jar sctsp.jar

Компонент	Файлы, подлежащие контролю целостности
OCSP Server	ocsp-server.war sccsp.jar sccms.jar
Notary-DIR	cert2ldif certinfo cert2ldap cert2ldap.conf xps.schema upload.php
Notary-TM	NotaryTM.exe NotaryTMSvr.exe
Arbiter-PKI	Arbiter-PKI.exe

Контроль целостности программных средств ПАК УЦ «Notary-PRO 2.8» должен выполняться при каждой перезагрузке операционной системы.

Администратор безопасности УЦ должен не реже 1 раза в месяц проводить контроль целостности и легальности установленных копий ПО на всех технических средствах удостоверяющего центра.

При нарушении целостности средств УЦ необходимо выполнить действия по повторной установке и настройке параметров согласно инструкциям, указанным в руководстве системного программиста соответствующего компонента УЦ.

8.2. Контроль целостности технических средств

Контроль целостности технических средств удостоверяющего центра обеспечивается опечатыванием корпусов устройств, препятствующим их неконтролируемому вскрытию.

Опечатывание устройств выполняется перед вводом технических средств в эксплуатацию и после выполнения регламентных работ и проведения проверки на отсутствие аппаратных закладок.

Контроль целостности печатей осуществляется в начале каждого рабочего дня и при каждой перезагрузке операционной системы, в окружении которой функционируют средства УЦ.

Ответственность за выполнение мероприятий по контролю целостности технических средств возлагается на Администратора безопасности УЦ.

9. ТРЕБОВАНИЯ К СЕРВЕРНЫМ И РАБОЧИМ ПОМЕЩЕНИЯМ УЦ

9.1. Серверное помещение

Серверное и телекоммуникационное оборудование УЦ рекомендуется размещать в отдельном помещении (далее – выделенное серверное помещение УЦ).

Организация доступа в выделенное серверное помещение осуществляется Администратором безопасности УЦ по приказу руководителя УЦ.

При невозможности размещения серверного и телекоммуникационного оборудования УЦ в отдельном помещении, необходимо обеспечить невозможность несанкционированного доступа в место размещения серверного и телекоммуникационного оборудования УЦ сотрудников организации, по роду своей деятельности не являющихся персоналом, допущенным к работе в этом помещении.

Помещение, в котором расположено серверное и телекоммуникационное оборудование УЦ, должно быть оборудовано металлической дверью с механическим замком, системой контроля доступа электромеханического типа с идентификацией по карте или персональному цифровому коду.

9.2. Помещения обслуживающего персонала УЦ

Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях обслуживающего персонала УЦ должны обеспечивать сохранность конфиденциальных документов и сведений, включая ключевую информацию.

Помещения обслуживающего персонала УЦ должны оборудоваться механическими замками.

Ключи механических замков рабочих помещений удостоверяющего центра выдаются сотрудникам удостоверяющего центра по распоряжению руководителя удостоверяющего центра на основании схемы организации рабочих мест персонала.

Во внерабочее время все помещения обслуживающего персонала УЦ должны быть опечатаны.

9.3. Архивное хранение

Архивному хранению в УЦ подлежат все издаваемые сертификаты ключей проверки электронной подписи в электронной форме и в виде бумажных копий.

Архивные документы должны храниться в специально оборудованном помещении, обеспечивающем режим хранения архивных документов, устанавливаемый законодательством Российской Федерации.

10. ТРЕБОВАНИЯ ПО УСТАНОВКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

К установке общесистемного и специального программного обеспечения, а также программного обеспечения удостоверяющего центра (далее – ПО УЦ), допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО.

Установка общесистемного и специального программного обеспечения, а также ПО УЦ, должна осуществляться под контролем Администратора безопасности УЦ.

Администратор безопасности УЦ должен самостоятельно сконфигурировать операционную систему, в среде которой планируется использовать ПО УЦ, и осуществлять периодический контроль сделанных настроек.

При установке и конфигурировании ПО Администратор безопасности УЦ должен обеспечить выполнение следующих требований:

- запрещается использование нестандартных, измененных или отладочных версий ОС;
- только Администратор безопасности УЦ имеет право управления учетными записями;
- только Администратор безопасности УЦ имеет право установки, модификации и удаления ПО;
- ОС должна быть настроена только для работы с ПО УЦ, все неиспользуемые ресурсы системы должны быть отключены (протоколы, сервисы и т.п.);
- режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;
- все пользователи и группы, зарегистрированные в ОС, должны иметь минимально возможные для нормальной работы права;
- запрещается удаленное управление, администрирование и модификация ОС и её настроек;
- доступ к следующим ресурсам системы должен быть максимально ограниченным (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):
 - системный реестр;
 - файлы и каталоги;
 - временные файлы;

- журналы системы;
 - файлы подкачки;
 - кэшируемая информация (пароли и т.п.);
 - отладочная информация.
- временные файлы и файлы подкачки, формируемые или модифицируемые в процессе работы ПО УЦ, должны затираться по окончании сеанса работы; если это невыполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям;
 - должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии;
 - необходимо организовать и использовать комплекс мероприятий антивирусной защиты с применением антивирусного ПО, сертифицированного по требованиям ФСБ России к антивирусным средствам по классу не ниже А2.

Администратор безопасности УЦ должен:

- ежедневно проверять выход новых пакетов обновлений безопасности ОС (Service Pack, Hot fix и т.п.) и устанавливать их;
- ежедневно обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС;
- организовать и использовать систему аудита;
- осуществлять ежедневный анализ результатов аудита.

На ЭВМ не должны устанавливаться средства разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано Администратором безопасности УЦ. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования и просмотра кода и памяти ПО УЦ и приложений, использующих ПО УЦ, в процессе обработки ПО УЦ защищаемой информации и/или при загруженной ключевой информации.

Программное обеспечение, устанавливаемое на технические средства УЦ, не должно содержать возможностей, позволяющих:

- просматривать и редактировать содержимое произвольных областей памяти;
- просматривать и редактировать собственный код и код других подпрограмм;
- просматривать и редактировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать функции ОС, недокументированные фирмой-разработчиком.

11. ТРЕБОВАНИЯ ПО УСЛОВИЯМ ЭКСПЛУАТАЦИИ

Технические средства удостоверяющего центра должны быть подключены к общегородской сети электроснабжения.

Серверное и телекоммуникационное оборудование должно размещаться в помещении, оборудованном системами бесперебойного питания, кондиционирования и пожаротушения.

Если в информационных системах, подлежащих защите, технические средства должны проходить проверку на соответствие «Специальным требованиям и рекомендациям по технической защите конфиденциальной информации» (СТР-К), то технические средства, на которых разворачивается удостоверяющий центр, обслуживающий данные системы, также должны проходить проверку на СТР-К, а при монтаже каналов связи УЦ с внешними сетями должны использоваться оптоволоконные развязки.

ЛИТЕРАТУРА

1. ПАК УЦ «Notary-PRO 2.8». Notary-PRO. Автоматизированное рабочее место администратора удостоверяющего центра. Руководство администратора. ШКНР.00054-01 34 01. ЗАО «Сигнал-КОМ», 2019.
2. СКЗИ «CADB 2.1». Формуляр. ШКНР.00053-01 30 01, ЗАО «Сигнал-КОМ», 2019.
3. СКЗИ «Signal-COM JCP 3.1». Формуляр. ШКНР.00049-01 30 01, ЗАО «Сигнал-КОМ», 2019.
4. СКЗИ «Крипто-КОМ 3.3». Формуляр. ШКНР.00035-07 30 08, ЗАО «Сигнал-КОМ», 2018.
5. ПАК УЦ «Notary-PRO 2.8». Notary-PRO RA Server. Сервер регистрационного центра. Руководство системного программиста. ШКНР.00054-01 32 03. ЗАО «Сигнал-КОМ», 2019.
6. ПАК УЦ «Notary-PRO 2.8». Notary-PRO Web Pages. Веб-приложение удостоверяющего центра. Руководство системного программиста. ШКНР.00054-01 32 07. ЗАО «Сигнал-КОМ», 2019.
7. ПАК УЦ «Notary-PRO 2.8». Notary-DIR. Справочник сертификатов. Руководство системного программиста. ШКНР.00054-01 32 04. ЗАО «Сигнал-КОМ», 2019.
8. ПАК УЦ «Notary-PRO 2.8». Типовой регламент. ШКНР.00054-01 90 02. ЗАО «Сигнал-КОМ», 2019.