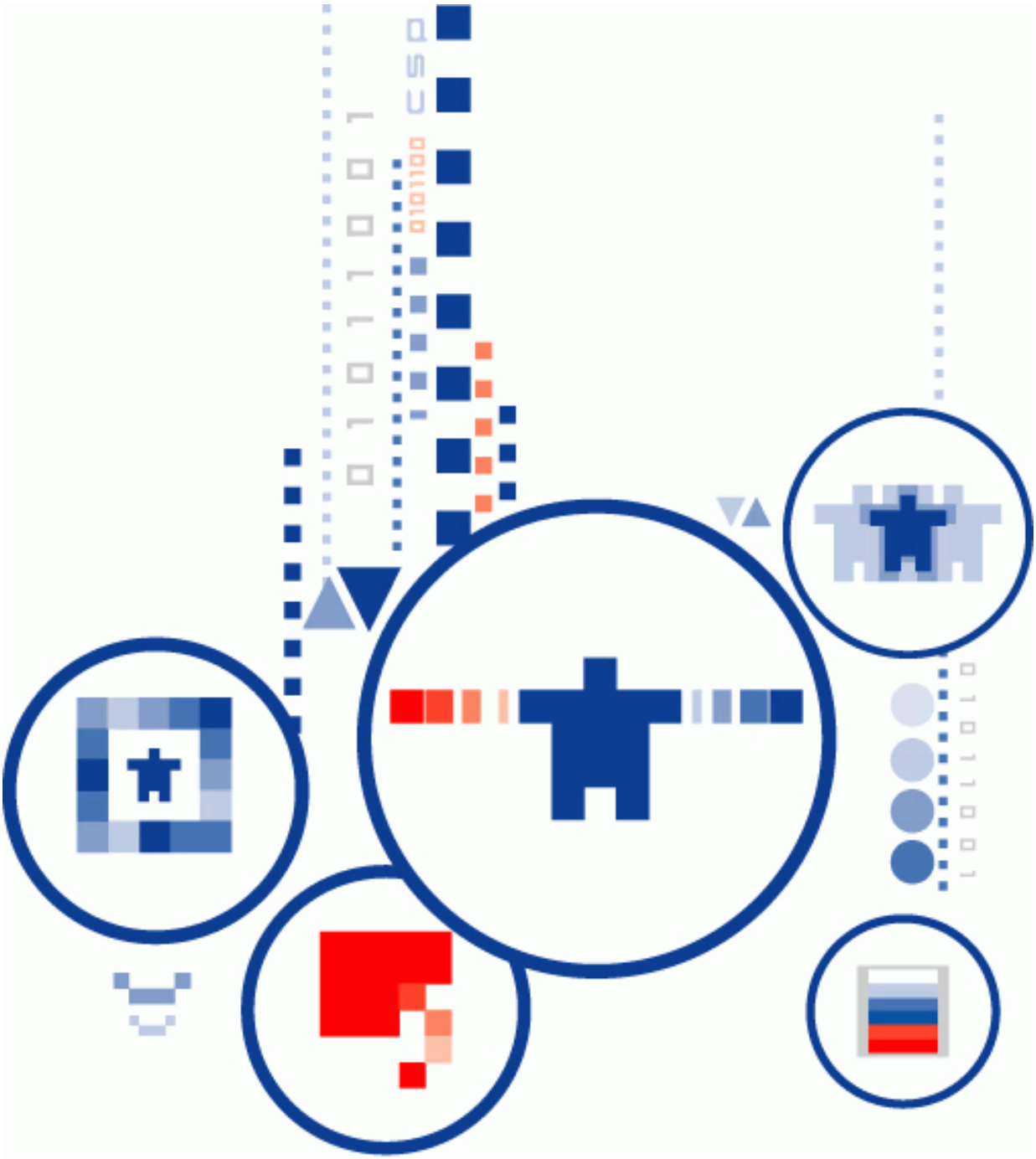

Служба проверки сертификатов и электронной подписи

КриптоПро SVS

Руководство по безопасности

АННОТАЦИЯ

Настоящий документ содержит описание регламентных работ по обеспечению информационной безопасности при эксплуатации Службы проверки сертификатов и электронной подписи «КриптоПро SVS».

Данное руководство предназначено для администраторов безопасности Службы проверки сертификатов и электронной подписи «КриптоПро SVS» или для системных администраторов подразделения, ответственного за эксплуатацию службы.

Информация о разработчике «КриптоПро SVS»:

ООО «КРИПТО-ПРО»
127018, Москва, ул. Сущёвский вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Введение 4
2. Настройка стека протоколов TCP/IP операционной системы 5
3. Использование СКЗИ КриптоПро CSP 6
4. Использование и настройка межсетевого экрана и СОА 7
5. Организационно-технические меры обеспечения безопасности 10
5.1. Требования по выбору и периодичности смены пароля 10
5.2. Требования к аутентификации 10
5.3. Устранение выявленных уязвимостей программного обеспечения 10
5.4. Объекты контроля целостности 10
5.5. Требования при подключении к сетям общего доступа 12
6. Возможности нарушителя 14
7. Аудит КриптоПро SVS 15
7.1. Настройка аудита 15
7.2. Структуры записей аудита 19
8. Рекомендации по серверному помещению 22
9. Перечень сокращений 23

1. Введение

Угроза, реализованная с использованием уязвимостей информационной системы, называется атакой.

Существует три основные категории атак:

- отказ в обслуживании;
- раскрытие информации;
- нарушение целостности.

Отказ в обслуживании (Denial of Service, DoS) — наиболее часто встречающийся на сегодняшний день вид нападения, т.к. его можно выполнить удаленно и с высокой степенью анонимности.

Наиболее известные формы DoS-атак:

- захват всех ресурсов системы, так что на долю авторизованных пользователей их не остается;
- аварийный останов системы – например, использование дефекта операционной системы (ОС), который приводит к нарушению прав доступа и в результате – к аварийному завершению работы ОС.

Раскрытие информации — следствие несанкционированного доступа к данным.

Нарушение целостности — умышленное искажение информации.

Для обнаружения атак можно пользоваться содержимым журналов событий (регистрационных файлов) ОС, системного и прикладного программного обеспечения. Такие журналы называются журналами аудита.

Целью аудита является сбор информации об удачных и неудачных попытках доступа к объектам, применении привилегий и других важных, с точки зрения безопасности, действиях и протоколирование этих событий для дальнейшего анализа.

Далее в документе описываются обязательные меры и рекомендации для предупреждения нарушения информационной безопасности при эксплуатации Службы проверки сертификатов и электронной подписи «КриптоПро SVS» (далее — КриптоПро SVS).

2. Настройка стека протоколов TCP/IP операционной системы

С помощью программы REGEDIT установите параметры TCP/IP-стека в реестре Windows в соответствии с приведенными ниже значениями.

```
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableSecurityFilters=1
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=1
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery=0
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=300000
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=1
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetra
nsmissions=2
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions=
3
MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\NoNameReleaseOnDemand=1
```

Установка данных параметров увеличит сопротивляемость TCP/IP-стека распределенным атакам типа «отказ от обслуживания» (DDoS).

Подробнее об установке данных параметров см. на сайте https://technet.microsoft.com

Воспользуйтесь поиском по фразе “Security Considerations for Network Attacks”.

3. Использование СКЗИ КриптоПро CSP

Средство криптографической защиты информации (СКЗИ) КриптоПро CSP в Службе проверки сертификатов и электронной подписи предназначено для:

- Использования в качестве средства электронной подписи при формировании, проверке электронной подписи (ЭП) и генерации ключей ЭП (ключей электронной подписи и ключей проверки электронной подписи) в соответствии с отечественными стандартами ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012;
- обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с ГОСТ 28147-89;
- контроля целостности программного обеспечения СКЗИ для его защиты от несанкционированного изменения или от нарушения правильности функционирования.
- управления ключами операторов TLS-сервера.

В процессе установки и эксплуатации СКЗИ «КриптоПро CSP» в составе КриптоПро SVS необходимо руководствоваться положениями эксплуатационной документации на СКЗИ «КриптоПро CSP», в том числе и в части обращения с ключевыми документами.

В частности, при эксплуатации СКЗИ «КриптоПро CSP» в составе КриптоПро SVS ЗАПРЕЩАЕТСЯ:

- создавать контейнеры закрытых ключей без установленного пароля;
- использовать пароли длиной менее 8 символов;
- использовать алфавит пароля менее 36 символов.

Указанные выше ограничения на использование СКЗИ КриптоПро CSP в составе КриптоПро SVS должны быть включены в организационно-распорядительные и организационно-штатные документы подразделения, ответственного за эксплуатацию Службы проверки сертификатов и электронной подписи.

4. Использование и настройка межсетевого экрана и СОА

Служба проверки сертификатов и электронной подписи «КриптоПро SVS», подключаемая к корпоративной информационной системе, для защиты от негативного сетевого воздействия должен использовать средства межсетевого экранирования, сертифицированные ФСБ России по 4 классу. В качестве такого межсетевого экрана может использоваться изделие ЦУС Континент, а также иные аналогичные продукты, сертифицированные ФСБ России.

Рисунок 1 иллюстрирует типовую схему подключения КриптоПро SVS при подключении к корпоративной информационной системе:

Рисунок 1. Типовая схема подключения КриптоПро SVS к корпоративной информационной системе

Ниже описаны рекомендации по настройке межсетевого экрана, в которых подразумевается, что на ЭВМ со Службой проверки сертификатов и электронной подписи для входящих соединений по протоколу HTTP используется порт 80, а по протоколу HTTPS – порт 443. Эти номера портов используются по умолчанию. Если они были изменены, настройку правил необходимо осуществлять для новых номеров.

На межсетевом экране необходимо создать следующие правила фильтрации:

- Разрешить прохождение пакетов с внешних IP-адресов на IP-адрес Службы на порты 80 и/или 443. Номера портов определяются используемыми протоколами доступа к Службе.
- Если используется протокол HTTP, разрешить команды протокола HTTP GET и POST и запретить все остальные.
- Для большей защищённости можно также скрыть реальный IP-адрес Службы при помощи трансляции сетевых адресов (NAT).

Помимо описанных правил рекомендуется включить автоматическое протоколирование соединений по этим правилам.

Технические средства, на которых размещается «КриптоПро SVS», должны осуществлять подключение к сетям общего доступа через сертифицированное ФСБ России средство обнаружения атак (СОА).

При настройке СОА необходимо обеспечить:

- настройку адреса внутренней сети (IP-адрес Службы штампов времени);
- наличие в базе решающих правил СОА правил, обеспечивающих обработку атак в соответствии с таблицей 1;
- периодическое обновление базы решающих правил.

Таблица 1. Правила обработки атак СОА

Классы атак	**Пример атаки**	**Рекомендуемая реакция СОА**	**Комментарий**
DoS атаки на уровне приложений	Различные попытки реализации атак «отказ в обслуживании» (Large Chunk Size, Slow HTTP DoS)	Обнаружение, аудит и предотвращение атаки (например, методом блокировки IP-адресов атакующих), блокировка запроса, имеющего признаки атаки	Признак атаки — открытие множества соединений без передачи данных
Проведение подозрительных запросов	Проведение запросов, не характерных для защищаемой автоматизированный системы	Блокировка запроса, имеющего признаки атаки	Параметры характерного запроса определяются с учетом профиля системы на этапе внедрения
Попытки запуска исполняемого кода	Наличие в запросе данных, имеющих признаки исполняемого кода или вызова исполняемого кода	Блокировка запроса, имеющего признаки атаки	—
Ошибки в сетевых протоколах	Некорректное использование параметров и возможностей протокола TCP.	Обнаружение, аудит и предотвращение атаки (может использоваться блокировка IP-адресов атакующих), блокировка запроса, имеющего признаки атаки	Штатные значения параметров протокола TCP предполагаются зашитыми в СОА
Явные нарушения спецификации протокола HTTP	Использование Path-Traversal-уязвимостей, связанных с различными видами атак (исполнение кода, кража критичной информации)	Блокировка запроса, имеющего признаки атаки	—
Использование запрещенных методов запроса	HTTP-Verb-Tampering-атаки	Блокировка запроса, имеющего признаки атаки	Может потребоваться модель, сопоставляющая различным группам или шаблонам URL-адресов разрешенные методы запроса
Различные нарушения политики безопасности	Использование двойного кодирования, нулевых символов и т. п.	Блокировка запроса, имеющего признаки атаки	Само по себе не запрещено спецификацией HTTP и не является атакой, но может быть признаком атаки

			(особенно в случае использования техник защиты от обнаружения)
Отсутствие или дублирование параметров запроса (HTTP)	Атаки класса HPP (HTTP Parameter Pollution)	Блокировка запроса, имеющего признаки атаки	Требуется построение моделей/профилей параметров для установление необходимых/уникальных параметров запроса в каждой группе шаблонов URL-адресов
Нарушение синтаксиса параметров (HTTP)	Различные виды инъекций через параметры и заголовки запроса: SQLi-инъекции всех видов, инъекции PHP-кода, команд операционной системы, XML/XPath, LDAP- и SSI-инъекции	Блокировка запроса, имеющего признаки атаки	Поиск характерных конструкций, нарушение синтаксиса параметра или заголовка
Передача небезопасных данных в теле запроса (HTTP)	Различные атаки класса «отказ в обслуживании» на интерпретаторы (например, XML bomb)	Блокировка запроса, имеющего признаки атаки	—
Переборные атаки	Подборы паролей или идентификатора пользовательской сессии,	Обнаружение, аудит и предотвращение атаки (например, методом блокировки IP-адресов атакующих)	Обнаружение с помощью оценки числа неудачных запросов за единицу времени
Отклонение наблюдаемого поведения пользователя от составленного профиля	Атаки класса CSRF, Эксплуатация веб-приложения от имени пользователя после того, как учетные данные были получены злоумышленником с помощью произвольных методов и средств	Блокировка запроса, имеющего признаки атаки	Обнаруживаются по отклонению поведения от составленного ранее профиля

5. Организационно-технические меры обеспечения безопасности

5.1. Требования по выбору и периодичности смены пароля

Для локального доступа администраторов выбираются надежные пароли входа в систему, удовлетворяющие следующим требованиям:

- длина пароля не менее 8 символов;
- мощность алфавита пароля должна быть не менее 36 символов (среди символов пароля встречаются заглавные символы, прописные символы, цифры и специальные символы);
- срок смены пароля не реже одного раза в месяц;
- доступ к паролю должен быть обеспечен только его владельцу.

5.2. Требования к аутентификации

При доступе в систему администраторов при их аутентификации необходимо установить ограничение по количеству подряд идущих неудачных попыток аутентификации в следующем объёме — не более 3-х попыток.

После превышения указанного числа неудачных попыток аутентификации доступ указанного субъекта должен быть заблокирован на срок не менее одних суток.

5.3. Устранение выявленных уязвимостей программного обеспечения

В процессе эксплуатации сервера, на котором развёрнут КриптоПро SVS, должны своевременно устраняться новые выявленные уязвимости установленного на данный сервер программного обеспечения (ОС, драйверы, общесистемное ПО, антивирусы).

Для этого необходимо осуществлять своевременную установку обновлений ОС Windows и антивирусного ПО, а также отслеживать информацию об уязвимостях, публикуемую в открытых источниках, в том числе в бюллетенях по безопасности Microsoft (http://technet.microsoft.com/ru-ru/security/bulletin), бюллетенях по безопасности производителя антивирусного ПО и базах уязвимостей (http://www.securitylab.ru/vulnerability/, http://www.osvdb.org/).

Выявленные уязвимости следует устранять в соответствии с инструкциями производителя ПО, в котором обнаружена уязвимость.

5.4. Объекты контроля целостности

В следующих двух таблицах приведены объекты (библиотеки), подлежащие контролю целостности.

Таблица 2 содержит перечень библиотеки, входящих в состав КриптоПро SVS и разрабатываемых ООО «КРИПТО-ПРО».

Таблица 3 содержит перечень сторонних библиотек, не разрабатываемых ООО «КРИПТО-ПРО», но которые также входят в состав КриптоПро SVS и устанавливаются установщиком КриптоПро SVS.

Под <Каталог установки> понимается путь, по которому был установлен продукт. Данный путь может быть указан пользователем во время установки. По умолчанию используется <%Program Files%>\Crypto Pro\DSS\.

Часть библиотек устанавливается в <%WinDir%>\Microsoft.NET\assembly\GAC_MSIL\ - так называемый GAC (глобальный кэш сборок, Global Assembly Cache). Часть библиотек ставится в подкаталоги <%WinDir%>\WinSxS.

В данный перечень не включены библиотеки, входящие в состав КриптоПро CSP и КриптоПро .NET. Данные компоненты хотя и необходимы для работы КриптоПро SVS, но устанавливаются отдельно, в качестве независимых продуктов.

Таблица 2. Объекты контроля целостности.

Имя библиотеки	Местоположение
CryptoPro.DSS.PowerShell.VS.dll	<Каталог установки>\VerificationService\bin\
CryptoPro.DSS.VerificationService.Diagnostics.CryptoPro-SVS-VerificationService.etwManifest.dll	<Каталог установки>\VerificationService\bin\
CryptoPro.DSS.VerificationService.Diagnostics.dll	<Каталог установки>\VerificationService\bin\
CryptoPro.DSS.VerificationService.Service.dll	<Каталог установки>\VerificationService\bin\
CryptoPro.DSS.VerificationService.Web.dll	<Каталог установки>\VerificationService\bin\
DSS.DocumentConverter.Dtbs.dll	<Каталог установки>\Plugins\Converters\
DSS.DocumentConverter.PdfStub.dll	<Каталог установки>\Plugins\Converters\
DSS.DocumentConverter.Word.dll	<Каталог установки>\Plugins\Converters\
CryptoPro.DSS.Common.dll	Подкаталоги <%WinDir%>\Microsoft.NET\assembly\GAC_MSIL\
CryptoPro.DSS.Common.Cryptography.dll	Подкаталоги <%WinDir%>\Microsoft.NET\assembly\GAC_MSIL\
CryptoPro.DSS.Common.Notification.dll	Подкаталоги <%WinDir%>\Microsoft.NET\assembly\GAC_MSIL\
CryptoPro.DSS.Common.Utils.dll	Подкаталоги <%WinDir%>\Microsoft.NET\assembly\GAC_MSIL\
CryptoPro.DSS.Common.Web.dll	Подкаталоги <%WinDir%>\Microsoft.NET\assembly\GAC_MSIL\
CryptoPro.DSS.PowerShell.Common.dll	Подкаталоги <%WinDir%>\Microsoft.NET\assembly\GAC_MSIL\
CryptoPro.Asn1.dll	Подкаталоги <%WinDir%>\Microsoft.NET\assembly\GAC_MSIL\
cades.dll	Подкаталоги <%WinDir%>\WinSxS\
ocsp.dll	Подкаталоги <%WinDir%>\WinSxS\
ocspcli.dll	Подкаталоги <%WinDir%>\WinSxS\
tsp.dll	Подкаталоги <%WinDir%>\WinSxS\
tspcli.dll	Подкаталоги <%WinDir%>\WinSxS\
asn1.dll	Подкаталоги <%WinDir%>\WinSxS\
cplib.dll	Подкаталоги <%WinDir%>\WinSxS\
asn1bercpp.dll	Подкаталоги <%WinDir%>\WinSxS\
asn1rtcpp.dll	Подкаталоги <%WinDir%>\WinSxS\
asn1xercpp.dll	Подкаталоги <%WinDir%>\WinSxS\
cpasn1.dll	Подкаталоги <%WinDir%>\WinSxS\

Таблица 3. Сторонние библиотеки, устанавливаемые вместе с SVS.

Имя библиотеки	Местоположение
LibSassHost.Native-32.dll	<Каталог установки>\VerificationService\bin\ LibSassHost.Native\
LibSassHost.Native-64.dll	<Каталог установки>\VerificationService\bin\ LibSassHost.Native\
AjaxMin.dll	<Каталог установки>\VerificationService\bin\
Antlr3.Runtime.dll	<Каталог установки>\VerificationService\bin\
BundleTransformer.Core.dll	<Каталог установки>\VerificationService\bin\
BundleTransformer.MicrosoftAjax.dll	<Каталог установки>\VerificationService\bin\
BundleTransformer.SassAndScss.dll	<Каталог установки>\VerificationService\bin\
itextsharp.dll	<Каталог установки>\VerificationService\bin\
LibSassHost.dll	<Каталог установки>\VerificationService\bin\
Microsoft.Diagnostics.Tracing.EventSource.dll	<Каталог установки>\VerificationService\bin\
Microsoft.Web.Infrastructure.dll	<Каталог установки>\VerificationService\bin\
Newtonsoft.Json.dll	<Каталог установки>\VerificationService\bin\
System.Web.Helpers.dll	<Каталог установки>\VerificationService\bin\
System.Web.Mvc.dll	<Каталог установки>\VerificationService\bin\
System.Web.Optimization.dll	<Каталог установки>\VerificationService\bin\
System.Web.Razor.dll	<Каталог установки>\VerificationService\bin\
System.Web.WebPages.Deployment.dll	<Каталог установки>\VerificationService\bin\
System.Web.WebPages.dll	<Каталог установки>\VerificationService\bin\
System.Web.WebPages.Razor.dll	<Каталог установки>\VerificationService\bin\
WebGrease.dll	<Каталог установки>\VerificationService\bin\
Aspose.Words.dll	<Каталог установки>\Plugins\Converters\

Целостность всех перечисленных библиотек необходимо контролировать перед каждым запуском КриптоПро SVS.

При эксплуатации КриптоПро SVS из состава ПАК «Службы УЦ» версии 2.0 варианта исполнения 2 контроль целостности должен производиться не реже 1 (одного) раза в сутки.

5.5. Требования при подключении к сетям общего доступа

В случае необходимости подключения вычислительных средств ПАК «Службы УЦ 2.0» (см. п. 2.11, «ЖТЯИ.00094-01 30 01. Службы УЦ 2.0. Формуляр») к информационно-телекоммуникационным сетям, доступ к которым не ограничен определенным кругом лиц, необходимо выполнение следующих требований:

- хранение всех ключей ЭП, используемых серверными компонентами ПАК «Службы УЦ 2.0», а также выполнение всех операций с ключами ЭП, используемых серверными компонентами ПАК «Службы УЦ 2.0», производится ПАКМ «КриптоПро HSM» версии 2.0 (Комплектация 1 исполнение 1); при этом хранение ключей ЭП производится в ПАКМ в неизвлекаемом виде;
- подключение осуществляется через межсетевой экран, сертифицированный ФСБ России (соответствующий 3 классу защищенности или выше по требованиям ФСБ России к устройствам типа межсетевые экраны), и средство обнаружения атак, сертифицированное ФСБ России (соответствующее классу Б или выше по требованиям ФСБ России к программным, программно-аппаратным или аппаратным

средствам обнаружения компьютерных атак или классу АП по требованиям к средствам обнаружения компьютерных атак);

- на указанных технических средствах установлено программное обеспечение Secure Pack Rus 3.0 (SPR 3.0), формуляр ЖТЯИ.00106-01 30 01.

Кроме того, необходимо выполнить настройку межсетевого экрана и настройку средства обнаружения атак в соответствии с требованиями, изложенными в разделе 4 настоящего документа.

6. Возможности нарушителя

КриптоПро SVS, входящий в состав ПАК «Службы УЦ» версии 2.0 варианта исполнения 5, соответствует «Требованиям к средствам удостоверяющего центра» и «Требованиям к информационной безопасности удостоверяющих центров» ФСБ России по классу КС2, что обеспечивает защиту от воздействий нарушителей типа Н2.

КриптоПро SVS, входящий в составе ПАК «Службы УЦ» версии 2.0 варианта исполнения 6, соответствует «Требованиям к средствам удостоверяющего центра» и «Требованиям к информационной безопасности удостоверяющих центров» ФСБ России по классу КС3, что обеспечивает защиту от воздействий нарушителей типа Н3.

Н2 — нарушитель, имеющий право постоянного или разового доступа в контролируемую зону, не имеющий права доступа к средствам вычислительной техники, на которых реализован КриптоПро SVS, самостоятельно осуществляющий создание способов атак, подготовку и проведение атак.

Н3 — нарушитель, не имеющий права доступа в контролируемую зону, а за пределами контролируемой зоны являющийся пользователем, имеющим доступ к функциональным возможностям программно-аппаратных средств взаимодействия с КриптоПро SVS на основе легального обладания аутентифицирующей информацией, или нарушитель, имеющий право постоянного или разового доступа в контролируемую зону, являющийся пользователем средств вычислительной техники, на которых реализован КриптоПро SVS, но не являющийся членом группы администраторов КриптоПро SVS, самостоятельно осуществляющий создание способов атак, подготовку и проведение атак.

При подключении КриптоПро SVS к техническим средствам сетей общего пользования (внешних информационных систем) на КриптоПро SVS может воздействовать потенциальный нарушитель с возможностями, превышающими возможности нарушителей типа Н1, Н2 и Н3.

7. Аудит КриптоПро SVS

События на ЭВМ Службы проверки сертификатов и электронной подписи регистрируются в нескольких журналах:

- журналы событий операционной системы (журнал приложений, журнал безопасности и журнал системы);
- журнал событий веб-сервера Microsoft IIS.

7.1. Настройка аудита

7.1.1. Настройка аудита безопасности Windows

В Microsoft Windows можно настроить правила (политику) аудита на локальном компьютере, не входящем в домен. Если компьютер работает в домене, эти правила можно сделать глобальными.

1. В списке утилит «Администрирование» откройте «Локальную политику безопасности», в узле «Локальные политики», выберите «Политика аудита» (Рисунок 2).

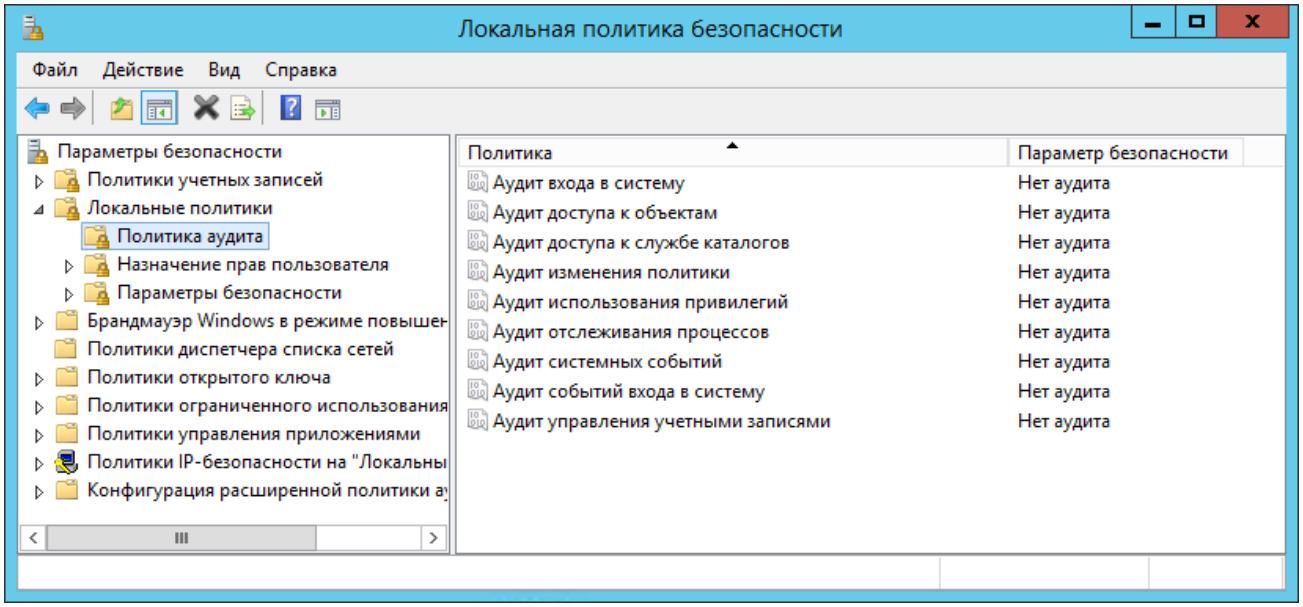

Рисунок 2. Параметры локальной политики аудита безопасности

2. Создайте политику в соответствии с приведенной ниже таблице:

Правило	Параметры
Audit account logon events (аудит событий входа в систему)	Success, Failure (удача, неудача)
Audit account management (аудит управления учетными записями)	Success, Failure (удача, неудача)
Audit directory services access (аудит доступа к службе каталогов)	Failure (неудача)
Audit logon events (аудит входа в систему)	Success, Failure (удача, неудача)

Правило	Параметры
Audit object access (аудит доступа к объектам)	Failure (неудача)
Audit policy change (аудит изменения политики)	Success, Failure (удача, неудача)
Audit privilege use (аудит использования привилегий)	Failure (неудача)
Audit process tracking (аудит отслеживания процессов)	No auditing (аудит отключен)
Audit system events (аудит системных событий)	No auditing (аудит отключен)

После определения параметров аудита необходимо настроить параметры журнала безопасности. Для этого выполните следующие действия:

1. Откройте окно «Просмотр событий» (Event Log) из списка утилит «Администрирование».
2. В дереве консоли выберите «Журналы Windows», «Безопасность» (Security).
3. В меню **Действие (Action)** выберите команду **Свойства (Properties)**.

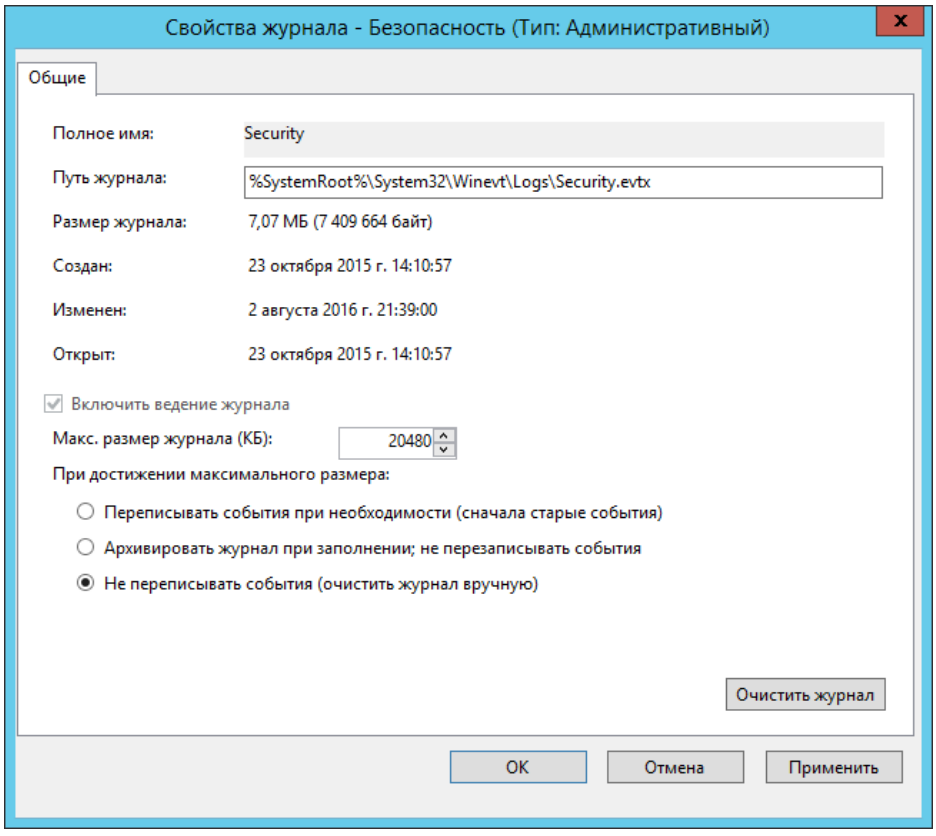

Рисунок 3. Настройки свойств журнала событий

4. На вкладке **Общие (All)** установите требуемые параметры:

   - Максимальный размер журнала – рекомендуется не менее 2Мб (2048 Кб).

- По достижении максимального размера журнала – не переписывать события (очистить журнал вручную).

Для выполнения настройки аудита и параметров журнала безопасности необходимо войти в систему с учетной записью «Администратор» или члена группы «Администраторы».

7.1.2. Настройка аудита Microsoft IIS

Для настройки аудита в MS IIS выполните следующие действия:

1. Из списка утилит «Администрирование» откройте «Диспетчер служб IIS».
2. В «Диспетчере служб IIS» выберите веб-узел и начальной странице настроек сайта в блоке настроек IIS откройте «Ведение журнала».
3. В настройках ведения журнала запросов к веб-серверу укажите:

- периодичность создания нового файла журнала – рекомендуемое значение Ежедневно;
- если не хотите пользоваться принятым по умолчанию стандартом времени UTC (или GMT), включите параметр **Использовать местное время в имени файла** (Use Local Time For Naming And Rollover);
- формат файла журнала – W3C.

Затем нажмите кнопку Выбрать поля.

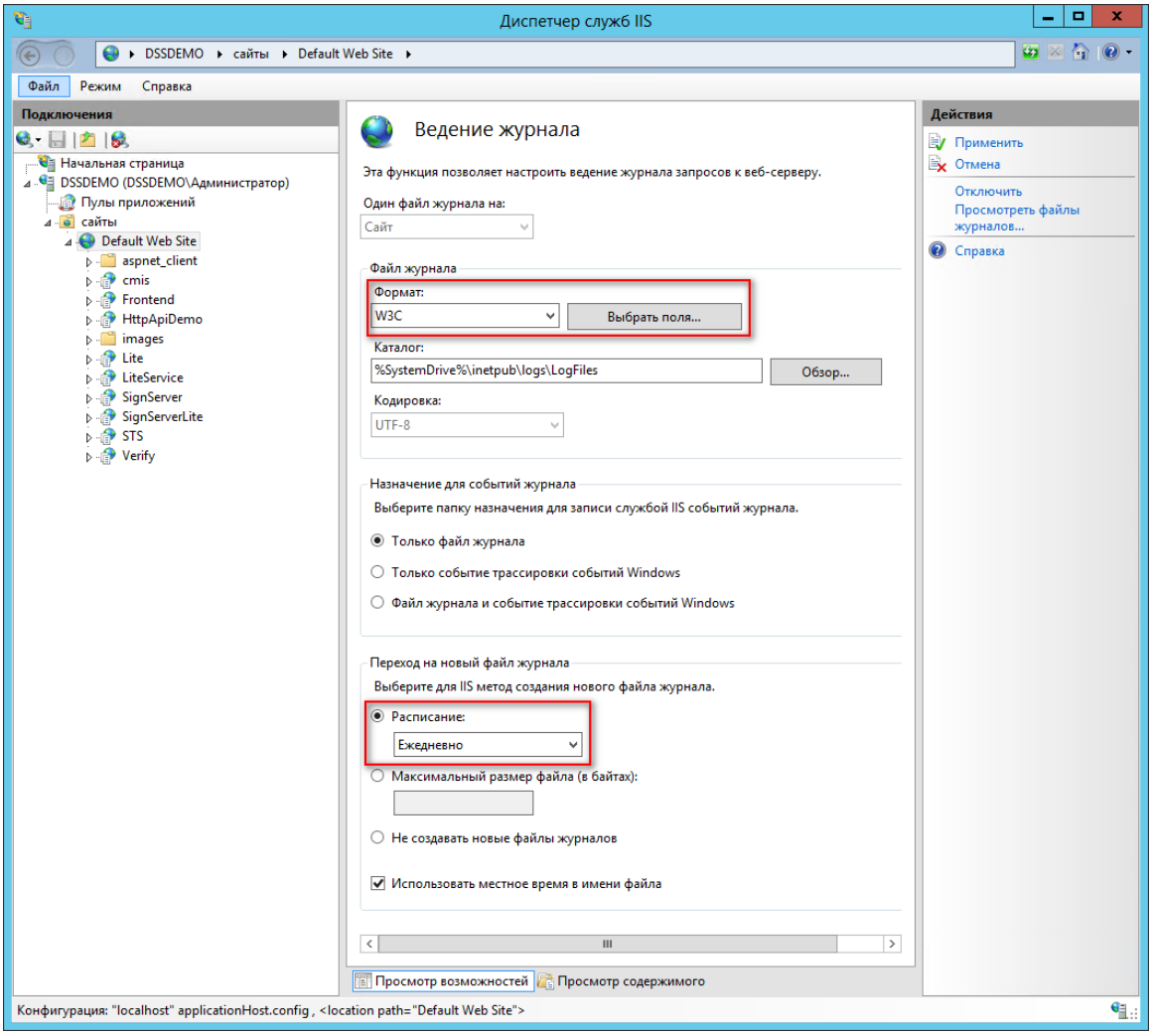

Рисунок 4. Настройки свойств журнала IIS

4. Укажите поля регистрации значений в журнале.

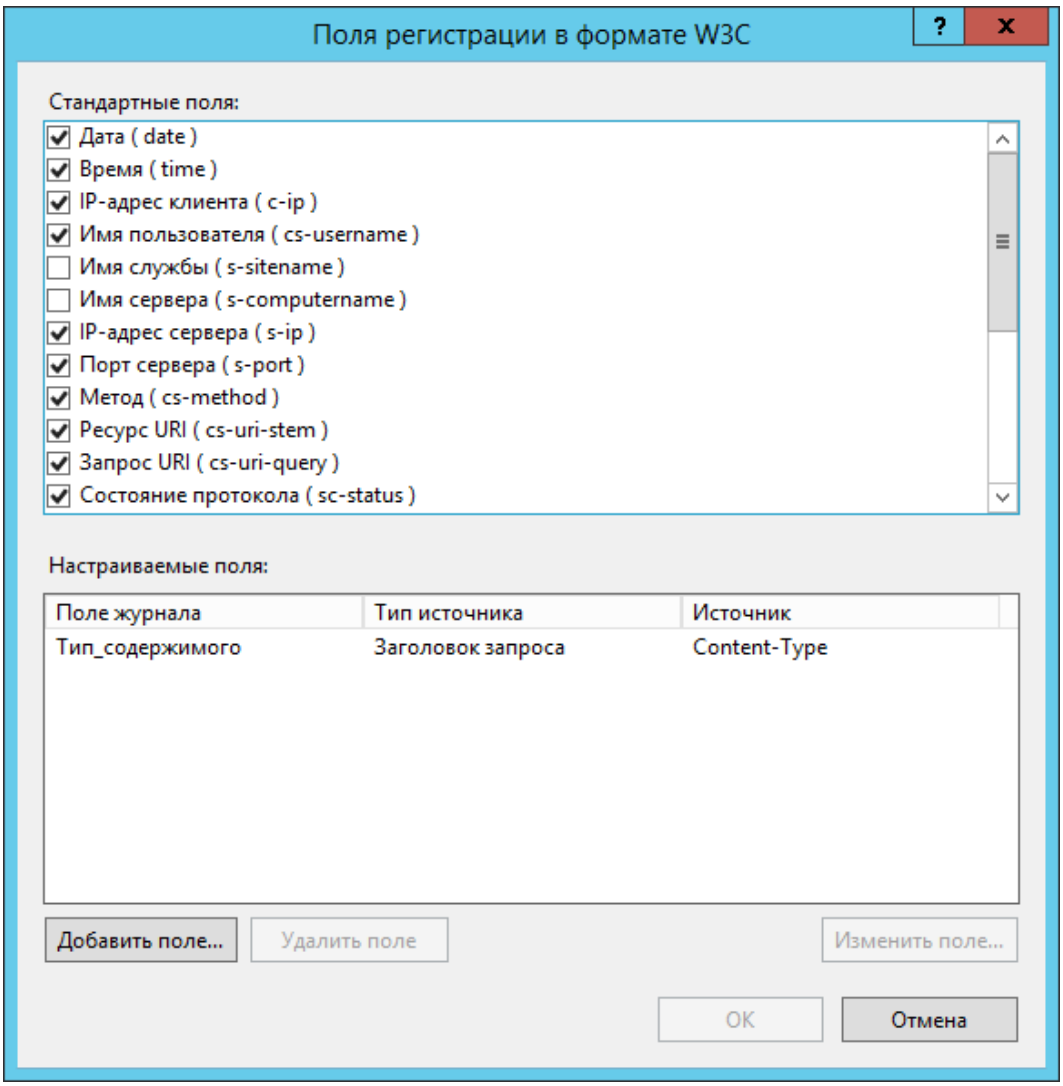

Рисунок 5. Выбор событий для регистрации в журнале IIS

Убедитесь, что в отчет включены следующие элементы:

- Client IP Address (IP-адрес клиента);
- User Name (имя пользователя, получившего доступ к серверу);
- Method (метод, действие которое пытался выполнить клиент (например, POST));
- URI Stem (ресурс URI, т.е. ресурс к которому было выполнено обращение);
- URI Query (запрос URI, т.е. запрос который пытался выполнить клиент);
- Protocol Status (состояние протокола в терминах HTTP);
- Win32 Status (состояние Win32);
- Bytes Sent (отправлено байт сервером);
- Bytes Received (получено байт сервером);
- Time Token (время, которое заняло действие);

User Agent (агент пользователя, т.е. обозреватель пользователя).

7.2. Структуры записей аудита

7.2.1. Структура записи аудита Windows

Структуру записи аудита Windows описывает Таблица 4.

Таблица 4. Структура записи аудита в Windows

Поле	Описание
Дата	Дата, когда произошло данное событие.
Время	Локальное время, когда произошло данное событие.
Пользователь	Имя пользователя, действия которого привели к данному событию. Это имя соответствует коду процесса клиента, если событие было вызвано процессом-сервером, и коду основного процесса в случае, если пользователь не причастен к событию. В некоторых случаях запись журнала безопасности содержит оба кода. (Олицетворение происходит в тех случаях, когда в Windows один процесс присваивает атрибуты безопасности другого процесса.)
Компьютер	Имя компьютера, на котором произошло событие. Обычно это имя локального компьютера, если только просмотр событий не выполняется с другого компьютера Windows.
Код события	Число, определяющее конкретный тип события. В первой строке описания обычно содержится название типа события. Например, 6005 — это идентификатор события, которое происходит при запуске службы ведения журналов событий. Соответственно, в начале описания этого события находится строка «Запущена служба журнала событий». Код события и имя источника записи могут использоваться представителями группы поддержки программного продукта для устранения неполадок.
Источник	Программа, занесшая событие. Это может быть как имя программы (например, «SQL Server»), так и название компонента системы или большого приложения (например, название драйвера). Например, «Elnkii» означает драйвер EtherLink II.
Тип	Уровень важности события: «Ошибка», «Уведомление» или «Предупреждение» в журналах системы и приложений; «Аудит успехов» или «Аудит отказов» в журнале безопасности. В окне просмотра событий тип события представлен соответствующим значком.
Категория	Категория события в зависимости от источника события. Это сведения используются преимущественно в журнале безопасности. Например, для аудита событий безопасности категория соответствует одному из типов событий, для которых в групповой политике может быть включен аудит успехов или отказов.

7.2.2. Структура записи аудита Microsoft IIS

Структуру записи аудита Microsoft IIS описывает Таблица 5.

Таблица 5. Структура записи аудита Microsoft IIS

Поле	Обозначение в журнале аудита	Описание
Дата	`date`	Дата возникновения события.

Поле	Обозначение в журнале аудита	Описание
Время	time	Время возникновения события.
IP-адрес клиента	c-ip	IP-адрес клиента, получившего доступ к серверу.
Имя пользователя	cs-username	Имя пользователя, получившего доступ к серверу. Это не относится к анонимным пользователям, которые обозначаются черточками.
Имя службы	s-sitename	Служба IIS, выполнявшаяся на компьютере клиента, и номер экземпляра.
Имя сервера	s-computername	Имя сервера, на котором была создана запись журнала.
IP-адрес сервера	s-ip	IP-адрес сервера, на котором была создана запись журнала.
Метод	cs-method	Действие, которое пытался выполнить клиент (например, метод GET).
Ресурс URI	cs-uri-stem	Ресурс, к которому было выполнено обращение, например Default.htm.
Запрос URI	cs-uri-query	Запрос, который пытался выполнить клиент.
Состояние протокола	sc-status	Состояние действия (в терминах HTTP, FTP).
Подсостояние протокола	sc-substatus	Подсостояние действия (в терминах HTTP, FTP).
Состояние Win32	sc-win32-status	Состояние действия (в терминах Windows).
Отправлено байтов	sc-bytes	Число байт, отправленных сервером.
Получено байтов	cs-bytes	Число байт, полученных сервером.
Порт сервера	s-port	Номер порта, к которому подключен клиент.
Заняло времени	time-taken	Время, которое заняло выполнение действия.

Поле	Обозначение в журнале аудита	Описание
Версия протокола	`cs-version`	Версия протокола (HTTP, FTP), используемого клиентом. Для протокола HTTP это либо HTTP 1.0, либо HTTP 1.1.
Узел	`cs-host`	Имя узла (если имеется).
Агент пользователя	`cs(User-Agent)`	Обозреватель, используемый клиентом.
Файлы «cookie»	`cs(Cookie)`	Содержимое отправленного или полученного модуля настройки клиента (cookie) (если имеется).
Источник ссылки	`cs(Referer)`	Предыдущий просмотренный пользователем узел. На этом узле содержалась ссылка на данный узел.

Все поля в записи журнала аудита разделяются пробелами.

8. Рекомендации по серверному помещению

Сервер Службы служба проверки сертификатов и электронной подписи и телекоммуникационное оборудование должны быть размещены в выделенном помещении (далее по тексту — серверное помещение).

Серверное помещение должно быть оборудовано системой контроля доступа с идентификацией по карте.

Идентификационные карты для доступа в серверное помещение выдаются сотрудникам из состава Службы Безопасности и Технической Службы по приказу руководителя подразделения, ответственного за эксплуатацию службы.

Серверное помещение должно быть оборудовано исполнительным устройством системы контроля доступа электромеханического типа.

Электрические сети и электрооборудование должны отвечать требованиям действующих «Правил устройства электроустановок», «Правил технической эксплуатации электроустановок потребителей», «Правил техники безопасности при эксплуатации электроустановок потребителей».

Серверное помещение должно быть оборудовано средствами вентиляции и кондиционирования воздуха, обеспечивающих соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха в соответствии с санитарно-гигиеническими нормами СНиП, устанавливаемыми законодательством Российской Федерации.

Серверное помещение должно быть оборудовано системой автоматического пожаротушения, пожарной сигнализации и дымоудаления.

Пожарная безопасность помещений обеспечивается в соответствии с нормами и требованиями СНиП по классу Ф3.5, устанавливаемыми законодательством Российской Федерации.

9. Перечень сокращений

CSP	Криптопровайдер (Cryptographic Service Provider)
IIS	Internet Information Services
IP	Центр идентификации (Identity Provider)
URL	Единый указатель ресурсов (Uniform Resource Locator)
WCF	Windows Communication Foundation
БД	База данных
ОС	Операционная система
ПК	Программный комплекс
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СЭП	Сервер электронной подписи
ЭП	Электронная цифровая подпись
ЦИ	Центр Идентификации
OTP	One-time password (одноразовый пароль)
МФА	Многофакторная аутентификация
УЦ	Удостоверяющий Центр
HOTP	Алгоритм аутентификации с использованием одноразовых паролей на основе HMAC (HMAC-Based One-Time Password Algorithm)