Содержание

[1. Центр сертификации 3](#_Toc98044497)

[1.1. Общие сведения 3](#_Toc98044498)

[1.2. Аккредитация центров сертификации 4](#_Toc98044499)

[1.3. Инфраструктура центров сертификации 4](#_Toc98044500)

[2. SSL сертификаты. 6](#_Toc98044501)

[2.1. История и термин 6](#_Toc98044502)

[2.2. Принцип работы 7](#_Toc98044503)

[2.3. Типы SSL-сертификатов 8](#_Toc98044504)

[2.3.1. Сертификаты с расширенной проверкой (EV SSL) 8](#_Toc98044505)

[2.3.2. Сертификаты, подтверждающие организацию (OV SSL) 8](#_Toc98044506)

[2.3.3. Сертификаты, подтверждающие домен (DV SSL) 9](#_Toc98044507)

[2.3.4. Wildcard-сертификаты 9](#_Toc98044508)

[2.3.5. Мультидоменные сертификаты (MDC) 10](#_Toc98044509)

[2.3.6. Сертификаты унифицированных коммуникаций (UCC) 10](#_Toc98044510)

[3. Центр сертификации на базе Windows Server 2022 11](#_Toc98044511)

[3.1. Инфраструктура открытых ключей PKI 11](#_Toc98044512)

[3.2. Изменение срока действия кэшированного маркера TLS 12](#_Toc98044513)

[4. Практическая часть 15](#_Toc98044514)

[4.1. Установка и настройка центра сертификации Windows Server 2022 на практическом примере. 15](#_Toc98044515)

[Этапы установки и настройки Служб сертификации: 15](#_Toc98044516)

[1) Установка Служб сертификации. 15](#_Toc98044517)

[2) Добавление шаблонов сертификатов в Центр Сертификации. 15](#_Toc98044518)

[3) Создание сертификата домена и привязка его к сайту. 15](#_Toc98044519)

[4.2. Базовая настройка и запуск. 15](#_Toc98044520)

[4.2.1. Запускаем сервер на базе windows 2022. 15](#_Toc98044521)

[4.2.2. Производим базовую настройку сети и служб. 15](#_Toc98044522)

[4.2.3. В диспетчере серверов добавляем новую роль. 15](#_Toc98044523)

[4.2.4. В окне мастер добавления ролей и компонентов ознакамливаемся с информацией. 15](#_Toc98044524)

[4.2.5. Подтверждаем выбор. 15](#_Toc98044525)

[Заключение 25](#_Toc98044526)

# Введение:

Актуальность – Центры сертификации необходимы в современном мире никакая информация не может существовать без защиты. В интернете все больше служб, корпораций, хостингов обязуют к использованию шифрования и цифровых подписей. Еще 15 лет назад все эти методы были неизвестны большинству IT специалистам, но сегодня они стали необходимостью. Сейчас мы находимся в фазе стремительного роста клиент-серверных веб-сервисов, огромная часть информационной деятельности людей приходится на интернет. Каждый человек хранит в интернете десятки и сотни гигабайт нужных ему данных, использует различное ПО в интернете, пишет тысячи писем и десятки тысяч сообщений. Все это задает новые требования к защите информации. Крупные IT компании активно продвигают идеологию «безопасного интернета», требуя поддержки цифровых сертификатов, начиная от серверов с конфиденциальными данными, облачных служб, вплоть до кухонного чайника.

Объект исследования – Интернет безопасность

Предмет исследования – Установка и настройка центра сертификации Windows Server 2022

Метод исследования - Изучение литературы и других источников информации. А также практический опыт

Цель работы – рассказать о центре сертификации Windows Server 2022, показать установку и настройку центра сертификации Windows Server 2022

# Задачи:

1. Рассказать, что такое центр сертификации.
2. Изучить что такое SSL сертификат и как он работает.
3. Ознакомить со структурой центра сертификации на базе Windows Server 2022.
4. Произвести установку и настройку центра сертификации Windows Server 2022 на практическом примере.
5. Сделать вывод.
6. Центр сертификации
   1. Общие сведения

Центр сертификации (Удостоверяющий центр) (англ. Certification authority, CA) выдает цифровые сертификаты. Это компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей. Цифровые сертификаты — это верифицируемые файлы данных, которые содержат сведения, чтобы помочь веб-сайтам, людям и устройствам подтвердить свою идентификацию в сети (ее подлинность проверяется центром сертификации). Центры сертификации играют важнейшую роль в работе интернета и в выполнении прозрачных и надежных онлайн-транзакций. Центры сертификации выдают миллионы цифровых сертификатов каждый год, и эти сертификаты используются для защиты информации, шифрования миллиардов транзакций и обеспечения безопасного обмена данными. Так же обеспечивается целостность документов подписанных с сертификатом, они не могут быть изменены третьей стороной в пути.

Открытые ключи и другая информация о пользователях хранится центрами сертификации в виде цифровых сертификатов, имеющих следующую структуру:

1. серийный номер сертификата;
2. объектный идентификатор алгоритма электронной подписи;
3. имя удостоверяющего центра;
4. срок годности;
5. имя владельца сертификата (имя пользователя, которому принадлежит сертификат);
6. открытые ключи владельца сертификата (ключей может быть несколько);
7. объектные идентификаторы алгоритмов, ассоциированных с открытыми ключами владельца сертификата;

Объектные идентификаторы алгоритмов, ассоциированных с открытыми ключами владельца сертификата; электронная подпись, сгенерированная с использованием секретного ключа удостоверяющего центра (подписывается результат хэширования всей информации, хранящейся в сертификате).

Асимметричный шифр позволяет шифровать одним ключом, а расшифровывать другим. Таким образом, один ключ (ключ расшифровки, «секретный») хранится у принимающей стороны, а второй (ключ шифрования, «открытый») можно получить при сеансе прямой связи, по почте, найти на «электронной доске объявлений», и т. д.

Когда сеть очень велика, нагрузка на центр сертификации получается большая. Поэтому сертификаты могут образовывать цепочки: корневой центр сертификации подписывает ключ службы безопасности компании, а та — ключи сотрудников.

* 1. Аккредитация центров сертификации

Отличием аккредитованного центра является то, что он находится в договорных отношениях с вышестоящим удостоверяющим центром и не является первым владельцем само-подписанного сертификата в списке удостоверенных корневых сертификатов. Корневой сертификат аккредитованного центра удостоверен вышестоящим удостоверяющим центром в иерархии системы удостоверения. Таким образом, аккредитованный центр получает «техническое право» работы и наследует «доверие» от организации, выполнившей аккредитацию.

Аккредитованный центр сертификации ключей обязан выполнять все обязательства и требования, установленные законодательством страны нахождения или организацией, проводящей аккредитацию в своих интересах и в соответствии со своими правилами.

Порядок аккредитации и требования, которым должен отвечать аккредитованный центр сертификации ключей, устанавливаются соответствующим уполномоченным органом государства или организации, выполняющей аккредитацию.

* 1. Инфраструктура центров сертификации

Открытые ключи и другая информация о пользователях сохраняется центрами сертификации, в виде цифровых сертификатов, которые имеют следующую структуру: серийный номер сертификата; объектный идентификатор алгоритма электронной подписи; имя центра, который удостоверяет; срок действия; имя владельца сертификата (имя пользователя, которому принадлежит сертификат; открытый ключ владельца сертификата; объектные идентификаторы алгоритмов, ассоциированных с открытыми ключами владельца сертификата;

Центр сертификации ключей имеет право:

1. предоставлять услуги по удостоверению сертификатов электронной цифровой подписи
2. обслуживать сертификаты открытых ключей
3. получать и проверять информацию, необходимую для создания соответствия информации, указанной в сертификате ключа и предъявленными документами.

Центры сертификации служат оплотом доверия в интернете и поэтому несут особую ответственность. Работа центра сертификации с соблюдением всех требований к аудиту является сложной задачей. Инфраструктура центров сертификации включает в себя значительное количество операционных элементов, аппаратного и программного обеспечения, политик отправителей и положений о правилах, проверок, элементов инфраструктуры безопасности и персонала. В совокупности эти элементы называются доверенной инфраструктурой открытого ключа (PKI).

Популярные Российские удостоверяющие центры:

1. ЗАО «АНК»
2. ООО ПНК
3. ЗАО Удостоверяющий Центр (Нижний Новгород)
4. ЗАО Удостоверяющий Центр (Санкт-Петербург)
5. ООО «Компания „Тензор“
6. ОАО „Электронная Москва“
7. SSL сертификаты.
   1. История и термин

Сертификаты бывают разных форматов и поддерживают не только SSL, а еще и аутентификацию людей и устройств, а также заверяют подлинность кода и документов. Однако SSL сертификаты самый распространенный на данный момент тип сертификатов в Интернет. Они используются, например в интернет-магазинах, то есть на сайтах, где есть функция заказа и где клиент вводит свои персональные данные. Для того, чтобы эти данные в момент передачи из браузера на сервер невозможно было перехватить используется специальный протокол HTTPS, который шифрует все передаваемые данные.

Сертификат SSL — Аббревиатура SSL означает Secure Sockets Layer – протокол безопасности, создающий зашифрованное соединение между веб-сервером и веб-браузером. Это популярный тип цифрового сертификата, который привязывает информацию о владельце веб-сервера (и веб-сайта) к ключу шифрования. Эти ключи используются в протоколе SSL/TLS для создания безопасной сессии между браузером и веб-сервером, на котором расположен SSL-сертификат. Чтобы браузер мог доверять SSL-сертификату и выполнял сессию SSL/TLS без предупреждений безопасности, SSL-сертификат должен содержать доменное имя веб-сайта, использующего этот сертификат, должен быть выдан надежным центром сертификации и быть действующим.

Компаниям и организациям необходимо добавлять SSL-сертификаты на веб-сайты для защиты онлайн-транзакций и обеспечения конфиденциальности и безопасности клиентских данных.

SSL обеспечивает безопасность интернет-соединений и не позволяет злоумышленникам считывать или изменять информацию, передаваемую между двумя системами. Если в адресной строке рядом с веб-адресом отображается значок замка, значит этот веб-сайт защищен с помощью SSL.

С момента создания протокола SSL около 25 лет назад, он был доступен в нескольких версиях. При использовании каждой из этих версий в определенный момент возникали проблемы безопасности. Затем появилась обновленная переименованная версия протокола – TLS (Transport Layer Security), которая используется до сих пор. Однако аббревиатура SSL прижилась, поэтому новая версия протокола по-прежнему часто называется старым именем.

* 1. Принцип работы

Использование SSL гарантирует, что данные, передаваемые между пользователями и веб-сайтами или между двумя системами, невозможно прочитать сторонним лицам или системам. SSL использует алгоритмы для шифрования передаваемых данных, что не позволяет злоумышленникам считать их при передаче через зашифрованное соединение. Эти данные включают потенциально конфиденциальную информацию, такую как имена, адреса, номера кредитных карт и другие финансовые данные.

Процесс работает следующим образом:

1. Браузер или сервер пытается подключиться к веб-сайту (веб-серверу), защищенному с помощью SSL.
2. Браузер или сервер запрашивает идентификацию у веб-сервера.
3. В ответ веб-сервер отправляет браузеру или серверу копию своего SSL-сертификата.
4. Браузер или сервер проверяет, является ли этот SSL-сертификат доверенным. Если это так, он сообщает об этом веб-серверу.
5. Затем веб-сервер возвращает подтверждение с цифровой подписью и начинает сеанс, зашифрованный с использованием SSL.
6. Зашифрованные данные используются совместно браузером или сервером и веб-сервером.
7. Этот процесс иногда называют подтверждением SSL-соединения. Хотя по описанию этот процесс выглядит длительным, в реальности он занимает миллисекунды.

Если веб-сайт защищен SSL-сертификатом, в веб-адресе появляется аббревиатура HTTPS (безопасный протокол передачи гипертекста). Для сайтов без SSL-сертификата отображается аббревиатура HTTP, без буквы S, соответствующей Secure (безопасный). Также в адресной строке веб-адреса будет отображаться значок замка. Это свидетельствует о безопасности и обеспечивает уверенность посетителям веб-сайта.

* 1. Типы SSL-сертификатов

Существуют разные типы SSL-сертификатов с разными уровнями проверки. Шесть основных типов:

1. Сертификаты с расширенной проверкой (EV SSL)
2. Сертификаты, подтверждающие организацию (OV SSL)
3. Сертификаты, подтверждающие домен (DV SSL)
4. Wildcard-сертификаты
5. Мультидоменные сертификаты (MDC)
6. Сертификаты унифицированных коммуникаций (UCC)
   * 1. Сертификаты с расширенной проверкой (EV SSL)

Это самый высокорейтинговый и наиболее дорогой тип SSL-сертификатов. Как правило, он используется для популярных веб-сайтов, которые собирают данные и используют онлайн-платежи. После установки этого SSL-сертификата в адресной строке браузера отображается замок, HTTPS, название и страна компании. Отображение информации о владельце веб-сайта в адресной строке помогает отличить сайт от вредоносных. Чтобы настроить сертификат с расширенной проверкой, владелец веб-сайта должен пройти стандартизированный процесс проверки подлинности и подтвердить, что он на законных основаниях имеет исключительные права на домен. Также сертификат позволяет шифровать данные пользователей. Тем самым, не позволяя злоумышленникам получать данные аутентификации.

* + 1. Сертификаты, подтверждающие организацию (OV SSL)

Этот тип SSL-сертификатов имеет такой же уровень доверия, что и сертификаты с расширенной проверкой, поскольку для его получения владелец веб-сайта должен пройти основательную проверку. Для этого типа сертификатов информация о владельце веб-сайта также отображается в адресной строке, что позволяет отличить его от вредоносных сайтов. SSL-сертификаты, подтверждающие организацию, обычно являются вторыми по стоимости (после SSL-сертификатов с расширенной проверкой). Их основная цель – зашифровать конфиденциальные данные пользователей при транзакциях. Коммерческие или общедоступные веб-сайты должны устанавливать сертификаты, подтверждающие организацию, чтобы гарантировать конфиденциальность информации о клиентах.

* + 1. Сертификаты, подтверждающие домен (DV SSL)

Процесс проверки для получения SSL-сертификата этого типа минимален. В результате SSL-сертификаты, подтверждающие домен, обеспечивают меньшую надежность и минимальный уровень шифрования. Такие сертификаты, как правило, используются для блогов или информационных веб-сайтов, т. е. для сайтов, не связанных со сбором данных или онлайн-платежами. Этот тип SSL-сертификатов является одним из самых дешевых и самых быстрых для получения. Многие хвостовые центры бесплатно раздают сертификаты данного типа. Процесс проверки требует только, чтобы владелец веб-сайта подтвердил право собственности на домен, ответив на электронное письмо или телефонный звонок. В адресной строке браузера отображается только HTTPS и замок без названия компании.

* + 1. Wildcard-сертификаты

Wildcard-сертификаты (сертификаты с подстановочными символами) позволяют защитить базовый домен и неограниченное количество поддоменов с помощью одного сертификата. Если имеется несколько поддоменов, которые нужно защитить, приобретение Wildcard-сертификата будет намного дешевле, чем приобретение отдельных SSL-сертификатов для каждого поддомена. Wildcard-сертификаты содержат звездочку (\*) как часть общего имени. Звездочка указывается вместо любого допустимого поддомена в составе одного базового домена.

* + 1. Мультидоменные сертификаты (MDC)

Мультидоменные сертификаты можно использовать для защиты нескольких доменных и поддоменных имен, включая сочетания полностью уникальных доменов и поддоменов с разными доменами верхнего уровня (TLD), за исключением локальных / внутренних доменов.

По умолчанию мультидоменные сертификаты не поддерживают поддомены. Если требуется защитить сайты www.example.com и example.com с помощью одного мультидоменного сертификата, то при получении сертификата следует указать оба имени хоста.

* + 1. Сертификаты унифицированных коммуникаций (UCC)

Сертификаты унифицированных коммуникаций (UCC) также считаются мультидоменными SSL-сертификатами. Сертификаты унифицированных коммуникаций изначально были разработаны для защиты серверов Microsoft Exchange и Live Communications. Сегодня любой владелец веб-сайта может использовать эти сертификаты, чтобы обеспечить защиту нескольких доменных имен с помощью одного сертификата. Сертификаты унифицированных коммуникаций проверяются на уровне организации. Для них в браузере отображается значок замка. Сертификаты унифицированных коммуникаций можно использовать в качестве сертификатов с расширенной проверкой, чтобы обеспечить посетителям веб-сайта максимальную безопасность.

Важно различать типы SSL-сертификатов, чтобы получить правильный тип сертификата для веб-сайта.

1. Центр сертификации на базе Windows Server 2022
   1. Инфраструктура открытых ключей PKI

Ключевым элементом PKI (Public Key Infrastructure — инфраструктура открытого ключа) является центр сертификации (CA). Служба сертификации Active Directory является одной из возможных ролей сервера под управлением операционной системы Windows Server.

Инфраструктура открытых ключей PKI основана на строгой иерархической модели, в которой выделяют:

- Корневой центр сертификации (англ. Root CA). Корневой центр сертификации всегда имеет само-подписанный сертификат.

- Промежуточные центры сертификации (англ. Subordinate CA), которые доверяют соответствующему корневому центру сертификации. Промежуточные центры сертификации могут образовывать многоуровневую иерархию.

Для создания центра сертификации нам понадобится сервер, работающий под управлением Windows Server, который может быть как выделенным, так и совмещать роль центра сертификации с другими ролями. Однако следует помнить, что после развертывания центра сертификации вы не сможете поменять имя компьютера и его принадлежность к домену (рабочей группе).

На базе Microsoft Windows Server можно организовать центр сертификации одного из двух типов:

Таблица 1- Заполненная таблица преимуществ центра сертификации

|  |  |  |
| --- | --- | --- |
|  | Автономный центр сертификации (Stand-Alone CA) | Центр сертификации предприятия (Enterprise CA) |
| Интеграция с Active Directory | - | + |
| Запрос сертификатов | Через web-интерфейс или через утилиту командной строки certreq.exe | Через web-интерфейс, консоль mmc или через утилиту командной строки certreq.exe |
| Автоматическое получение и обновление сертификатов | - | + |
| Использование шаблонов | - | + |
| Данные сертификата | Должны вводиться вручную | Могут браться из Active Directory |
| Публикация сертификатов и списка отозванных сертификатов в AD | - | + |

При развертывании метода проверки подлинности на основе сертификата, такого как расширенная проверка подлинности Protocol-Transport уровень безопасности (EAP-TLS), защищенная Расширенная проверка подлинности Protocol-Transport уровня безопасности (PEAP-TLS) и PEAP-Microsoft протокол проверки подлинности подтверждения связи версии 2 (MS-CHAP v2), необходимо зарегистрировать сертификат сервера для всех НПСС. Сертификат сервера должен:

- Выполнять минимальные требования к сертификату сервера.

- Выдается центром сертификации (ЦС), который является доверенным для клиентских компьютеров. ЦС является доверенным, если его сертификат существует в хранилище сертификатов доверенных корневых центров сертификации для текущего пользователя и локального компьютера.

- Следующие инструкции помогают управлять сертификатами NPS в развертываниях, где доверенный корневой ЦС является сторонним центром сертификации, например VeriSign, или центром сертификации, развернутым для инфраструктуры открытых ключей (PKI) с помощью служб сертификатов Active Directory (AD CS).

* 1. Изменение срока действия кэшированного маркера TLS

В процессе первоначальной проверки подлинности для EAP-TLS, PEAP-TLS и PEAP-MS-CHAP v2 сервер политики сети кэширует часть свойств подключения TLS подключающегося клиента. Клиент также кэширует часть свойств подключения TLS NPS.

Каждая отдельная коллекция этих свойств подключения TLS называется маркером TLS.

Клиентские компьютеры могут кэшировать дескрипторы TLS для нескольких сторон проверки подлинности, в то время как НПСС может кэшировать дескрипторы TLS многих клиентских компьютеров.

Кэшированные обработчики TLS на клиенте и сервере позволяют более быстро выполнять процесс повторной проверки подлинности. Например, при повторной проверке подлинности беспроводного компьютера с NPS сервер политики сети может проверить обработчик TLS для беспроводного клиента и быстро определить, что клиентское подключение является переподключением. NPS разрешает подключение, не выполняя полную проверку подлинности.

Соответственно, клиент проверяет обработчик TLS для сервера политики сети, определяет, что он является повторно подключенным и не требует проверки подлинности сервера. На компьютерах с Windows 10 и Windows Server 2022 срок действия маркера TLS по умолчанию составляет 10 часов.

В некоторых случаях может потребоваться увеличить или уменьшить время окончания срока действия маркера TLS. Например, может потребоваться уменьшить срок действия маркера TLS в случаях, когда сертификат пользователя отзывается администратором, а срок действия сертификата истек. В этом случае пользователь по-прежнему может подключиться к сети, если NPS имеет кэшированный обработчик TLS, срок действия которого не истек. Уменьшение срока действия маркера TLS может помочь предотвратить повторное подключение таких пользователей с отозванными сертификатами.

Эту процедуру можно использовать для изменения времени, в течение которого клиентские компьютеры кэшируют обработчик TLS сервера политики сети. После успешной проверки подлинности сервера политики сети клиентские компьютеры кэшируют свойства TLS-подключения NPS в качестве обработчика TLS. Значение по умолчанию для маркера TLS составляет 10 часов (36 000 000 миллисекунд). Вы можете увеличить или уменьшить время окончания срока действия маркера TLS, выполнив следующую процедуру.

|  |
| --- |
| 1. Практическая часть    1. Установка и настройка центра сертификации Windows Server 2022 на практическом примере.   Этапы установки и настройки Служб сертификации:   1. Настройка сети 2. Установка Служб сертификации. 3. Развертывание центра сертификации 4. Добавление шаблонов сертификатов в Центр Сертификации. 5. Создание сертификата домена и привязка его к сайту. |

|  |
| --- |
| * 1. Запускаем сервер на базе windows 2022. |
|  |

Рисунок 1 – Запуск сервера.

|  |
| --- |
| * 1. Производим базовую настройку сети и служб. |
|  |

Рисунок 2 – Настойка сети.

|  |
| --- |
| * 1. В диспетчере серверов добавляем новую роль. |
|  |

Рисунок 3 – Добавление ролей и компонентов.

|  |
| --- |
| * 1. В окне мастер добавления ролей и компонентов ознакамливаемся с информацией и нажимаем далее. |
|  |

Рисунок 4 – Тип инициализации.

|  |
| --- |
| * 1. Дальше выбираем сервер и подтверждаем выбор. |
|  |

Рисунок 5 – Выбор сервера.

|  |
| --- |
| * 1. Выбираем роль Active Directory Certificate Services, после выбираем далее и устанавливаем. |
|  |

Рисунок 6 – Добавление ролей.

|  |
| --- |
| * 1. После установки Active Directory Certificate Services, начинаем его развертывание. Ознакамливаемся с информацией и нажимаем далее. |
|  |

Рисунок 7 – Начало развертывания CA.

|  |
| --- |
| * 1. В окне службы ролей выбираем центр сертификации, нажимаем далее. Вариант установки Enterprise CA. |
|  |

Рисунок 8 – Базовый Тип центра сертификации.

|  |
| --- |
| * 1. В нашем случае тип центра сертификации root CA. Выбираем и нажимаем далее. |
|  |

Рисунок 9 – Ролевой тип CA.

|  |
| --- |
| * 1. Выбираем создание нового ключа, а не использование существующего. |
|  |

Рисунок 10 – Создание ключа.

|  |
| --- |
| * 1. В следующем окне для указания параметров шифрования в раскрывающемся списке, выбираем – поставщик служб шифрования, Длину ключа, хеш-алгоритм. Нажимаем далее. |
|  |

Рисунок 11 – настройка шифрования.

|  |
| --- |
| * 1. Указываем имя и суффикс центра сертификации. |
|  |

Рисунок 12 – Создания имени и суффикса.

|  |
| --- |
| * 1. Далее указываем период действие сертификата и расположение базы данных. Подтверждаем и ждем завершение настройки. |
|  |

Рисунок 13 – Установка CA.

|  |
| --- |
| * 1. Теперь создадим само-подписанный сертификат. Открываем server manager, сервера и создаем новый сертификат. |
|  |

Рисунок 14 – Создание сертификата в менеджере серверов.

|  |
| --- |
| * 1. Указываем данные о сертификате. |
|  |

Рисунок 15 – Настройка имени сертификата.

|  |
| --- |
| * 1. Устанавливаем сетевую директорию, и триггер имя. |
|  |

Рисунок 16 – Указание директории сертификата.

|  |
| --- |
| * 1. Выбираем сайт, к которому мы хотим привязать данный сертификат. |
|  |

Рисунок 17 – Привязка сайта к сертификату.

|  |
| --- |
| * 1. Запускам сайт. Как видно сертификат был подключен к сайту. Однако выдает ошибку поскольку центр сертификации не имеет подписи от центра сертификации первого уровня, или не установлен как центр сертификации первого уровня. |
|  |

Рисунок 18 – Проверка в браузере.

# Заключение

Центры сертификации стали обязательной нормой в мире. Сегодня все электронные продукты, временные или постоянные обязуются быть сертифицированными. По определению, данном в руководстве ИСО/МЭК 2 «Сертификация соответствия - действие третьей стороны, доказывающее, что обеспечивается необходимая уверенность в том, что должным образом идентифицированная продукция, процесс или услуга соответствуют конкретному стандарту или другому нормативному документу». Закон РФ о сертификации продукции и услуг следующим образом определяет это понятие: «Сертификация - это деятельность по подтверждению соответствия продукции установленным требованиям». Такое подтверждение оформляется в виде документа (сертификата), который выдается изготовителю органом по сертификации и удостоверяет, что продукция или услуга соответствует определенным стандартам или техническим условиям. Международный опыт свидетельствует, что необходимым инструментом, гарантирующим соответствие качества продукции требованиям НД, является сертификация.

Из всего этого выходит, что актуальность центров сертификации и специалистов в данной области далеко не на своем пике. Умения и навыки в данной деятельности необходимы, а примерно 70 % центров сертификации установлены на базе Windows Server.

Список использованных источников

Список использованной литературы:

* 1. US-CERT. TA14-290A: SSL 3.0 Protocol Vulnerability and POODLE Attack (англ.) (октябрь 2014).
  2. Overview of SSL/TLS Encryption Microsoft TechNet. Updated July 31, 2003.
  3. SSL/TLS in Detail Microsoft TechNet. Updated July 31, 2003.
  4. Microsoft. Secure Channel (англ.) (5 сентября 2012).
  5. Microsoft. MS-TLSP Appendix A (англ.) (27 февраля 2009).
  6. Apple. Features (англ.) (10 июня 2009).
  7. Apple. Technical Note TN2287 - iOS 5 and TLS 1.2 Interoperability Issues (англ.) (14 октября 2011).
  8. Игорь Савчук. Это СОРМ, детка. Часть 1. Возможности современных средств шифрования // «БИТ. Бизнес&Информационные технологии» : Журнал. — М.: ООО «Издателький дом «Положевец и партнеры», 2014. — Вып. 1, № 34. — ISSN 2313-8718.
  9. Dan Goodin. Hackers break SSL encryption used by millions of sites (англ.) (19 сентября 2011).
  10. Y Combinator comments on the issue (англ.) (20 сентября 2011).
  11. Security of CBC Ciphersuites in SSL/TLS: Problems and Countermeasures (англ.) (20 мая 2004).
  12. Christopher Allen, Tim Dierks. Протокол SSL – Перевод – версия 1.0. Certicom. Семенов Ю. А.
  13. David Wagner. Analysis of the SSL 3.0 Protocol (англ.). University of California.

Интернет-ресурсы:

* 1. Сообщество IT-специалистов «Habr»: компьютерный портал [Электронный ресурс] – Режим доступа: https://habr.com.
  2. Официальный сайт-энциклопедия компании Microsoft [Электронный ресурс] - Режим доступа https://docs.microsoft.com.
  3. Прортал документации "Рутокен" [Электронный ресурс] - Режим доступа https://dev.rutoken.ru.
  4. Электронный документ от компании "Esmart" [Электронный ресурс] - Режим доступа https://esmart.ru.
  5. ФЕДЕРАЛЬНЫЙ ЗАКОН Об электронной подписи (с изменениями на 24 февраля 2021 года). https://docs.cntd.ru/. docs.cntd.ru.
  6. Аккредитация удостоверяющих центров. digital.gov.ru. digital.gov.ru.