Федеральное агентство по рыболовству
БГАРФ ФГБОУ ВО «КГТУ»
Калининградский морской рыбопромышленный колледж

Утверждаю
Заместитель начальника колледжа
по учебно-методической работе
А.И.Колесниченко

Подписано цифровой подписью: Колесниченко Андрей Игоревич
Причина: Я утвердил этот документ
Дата: 19 Март 2025 г. 15:01:32
DN: E=uc_fk@roskazna.ru, S=77 Москва, ИНН ЮЛ=7710568760, ОГРН=1047797019830, STREET="Большой Златоустинский переулок, д. 6, строение 1", L=г. Москва, C=RU, O=Казначейство России, CN=Федеральное казначейство

МДК.07.02 СЕРТИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Методические указания для выполнения практических занятий
по специальности
09.02.07 Информационные системы и программирование

МО-09 02 07-МДК.07.02.ПЗ

РАЗРАБОТЧИКИ	Богатырева Т.Н.
ЗАВЕДУЮЩИЙ ОТДЕЛЕНИЕМ	Кругленя В.Ю.
ГОД РАЗРАБОТКИ	2024
ГОД ОБНОВЛЕНИЯ	2025

Содержание

Практическая работа №1. Разработка политики безопасности корпоративной сети

Цель занятия: Познакомить обучающихся с основными приемами работы с политиками безопасности корпоративной сети;

Содержание и порядок выполнения задания:

Теоретический материал

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАЗ ДАННЫХ

Информационная безопасность - защищенность информации и поддерживающейинфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести *неприемлемый ущерб субъектам информационных отношений*, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

ГОСТ "*Защита информации*. Основные термины и определения" вводит понятие **информационной безопасности** как состояние защищенности информации, при котором обеспечены ее *конфиденциальность*, доступность и *целостность*.

- ***Конфиденциальность*** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
- ***Целостность*** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- ***Доступность*** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Угрозы информационной безопасности – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. ***Атакой*** называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, - ***злоумышленником***. Потенциальные злоумышленники называются *источниками угрозы*.

Угрозы можно классифицировать по нескольким критериям:

- по *свойствам информации* (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные,программы, аппаратура, *поддерживающая инфраструктура*);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Угроза является следствием наличия **уязвимых мест илиуязвимостей** винформационной системе.

Причинами возникновения уязвимостей в общем случае являются:

1. ошибки при разработке программного обеспечения;
2. преднамеренные изменения программного обеспечения с целью внесенияуязвимостей;
3. неправильные настройки программного обеспечения;
4. несанкционированное внедрение вредоносных программ;
5. неумышленные действия пользователей;
6. сбои в работе программного и аппаратного обеспечения.

Уязвимости можно классифицировать по различным признакам:

1. по типу ПО – системное или прикладное.
2. По этапу жизненного цикла ПО, на котором возникла уязвимость – проектирование, эксплуатация и пр.
3. По причине возникновения уязвимости, например, недостатки механизмов аутентификации сетевых протоколов.
4. по характеру последствий от реализации атак – изменение прав доступа, подборпароля, вывод из строя системы в целом и пр.

Прежде чем приступать к построению системы защиты информации необходимо провести *анализ уязвимостей* ИС и попытаться сократить их количество, то есть использовать метод превентивности.

Важнейшие угрозы безопасности баз данных:

1. Чрезмерные и неиспользуемые пользовательские привилегии

Когда кто-либо получает привилегии, объемы которых превышают необходимые для выполнения должностных обязанностей, возникает вероятность злоупотребления этими привилегиями. Более того, когда какого-либо работника переводят на другую должность или он увольняется, уровень его доступа к конфиденциальной информации часто остается неизменным.

2. Злоупотребление привилегиями

Существует вероятность использования пользователями своих легитимных прав доступав противоправных целях.

3. Input-инъекции (инъекции в поле ввода)

Существует два основных способа взлома баз данных при помощи инъекций кода:

- SQL-инъекции, применяемые для взлома традиционных СУБД. SQL-инъекции обычно представляют собой внедрение (инъекцию)

неразрешенного или вредоносного кода в поля ввода веб-приложений.

- NoSQL-инъекции, которые используются для взлома платформ Big Data. Инъекции типа NoSQL подразумевают внедрение вредоносного кода в компоненты Big Data (например, в Hive или MapReduce).

4. Хакерские программы

Киберпреступники, профессиональные хакеры применяют передовые методы атаки, сочетающие в себе различные тактические приемы, такие как фишинговые электронные письма и хакерские программы, с целью проникновения в сеть организаций и получения конфиденциальных данных. Легитимные пользователи, не зная об инфицировании своих компьютеров хакерским ПО, могут стать невольными посредниками, при помощи которых хакеры получают доступ к сетям и важным данным.

5. Недостаточные меры по аудиту данных.

Корпоративная информационная система должна включать в себя средства для автоматической регистрации транзакций базы данных, в том числе протоколирования операций с конфиденциальной информацией. Отказ от сбора детальных данных аудита ведет к возникновению серьезных угроз на множестве уровней.

Многие организации используют встроенные в СУБД средства аудита, полагаются на узкоспециализированные решения или проводят аудит в ручном режиме. Однако возможности таких инструментов ограничены – они не позволяют проводить полноценный аудит, выявлять попытки взлома и проводить расследования. Более того, встроенные в СУБД средства часто оказывают излишнюю нагрузку на процессор и жесткий диск сервера, поэтому во многихслучаях функция аудита просто отключается. Наконец, большинство встроенных решений работают лишь на одной, предназначенной для них, платформе. Так, логи Oracle отличаются от логов MS-SQL, а логи MS-SQL отличаются от логов DB2. Это значительно осложняет внедрение однородного, масштабируемого механизма аудита в организациях, оперирующих СУБД различного типа.

Большинство встроенных инструментов аудита не способны определить конечного пользователя, поскольку ассоциируют активность БД с учетными записями клиентских приложений. Отсутствие связи с пользователем, совершившим ту или иную операцию, препятствует ведению отчетности, возможности наблюдения и проведению расследований. К тому же, пользователи, обладающие правами администратора БД (легитимными или полученными в результате взлома), могут отключить встроенный аудит, чтобы скрыть свою вредоносную активность. Именно поэтому необходимо разграничивать функции управления аудитом и администрирование БД и серверной платформы, чтобы добиться четкого разделения зон ответственности.

6. Незащищенность носителей информации.

Носители информации, предназначенные для хранения резервных копий, часто остаютсябез какой-либо защиты. Результатом этого становятся похищения дисков и пленок, содержащихрезервные копии баз данных.

7. Эксплуатация уязвимых, неверно сконфигурированных баз данных

На практике часто встречаются устаревшие версии баз данных и БД с настройками «по умолчанию». К сожалению, обновление баз данных часто игнорируется даже в тех случаях, когда выпускаются патчи и обновления.

8. Неуправляемая конфиденциальная информация

Неучтенные БД могут содержать важную информацию, могут появляться новые базы данных (например, в процессе тестирования системы) – и все это проходит незамеченным службой безопасности компании. Если вовремя не внедрить систему разграничения прав доступа, конфиденциальные данные, содержащиеся в этих базах данных, могут стать уязвимыми к взлому и утечкам.

9. Отказ в обслуживании (DoS).

DoS – это способ атаки информационной системы, в результате которой легитимные пользователи теряют доступ к сетевым приложениям или информации. Существуют различные способы создания DoS-условий. Наиболее популярным способом проведения DoS-атаки на базуданных является провокация перегрузки аппаратных ресурсов сервера, таких как память и процессор, путем его бомбардировки чрезмерно большим количеством запросов или меньшим по количеству запросов, но на обработку которых требуется непропорционально много системных ресурсов. В обоих случаях DoS-атака приводит к одному результату: сервер, столкнувшись с недостатком системных ресурсов, отказывает своим пользователям в обслуживании и в некоторых случаях даже «падает».

10. Недостаток знаний и опыта в сфере информационной безопасности.

Развитие средств внутренней безопасности не успевает за ростом объемов данных, при этом многие организации слишком плохо оснащены и подготовлены для противодействия угрозам. Причиной этого часто является недостаток опыта и квалификации сотрудников в применении решений, улучшении политик или реагировании на инциденты в сфере безопасности.

В связи с повсеместным развитием Интернета наиболее часто атаки производятсяс использованием уязвимостей протоколов сетевого взаимодействия.

Наиболее распространенные атаки:

1. Анализ сетевого трафика

Данный вид атаки направлен в первую очередь на получение пароля и идентификатора пользователя путем "прослушивания сети". Реализуется это с помощью *sniffer* – специальная программа-анализатор, которая перехватывает все

пакеты, идущие по сети. И если протокол, например, FTP или TELNET, передает аутентификационную информацию в открытом виде, то злоумышленник легко получает доступ к учетной записи пользователя.

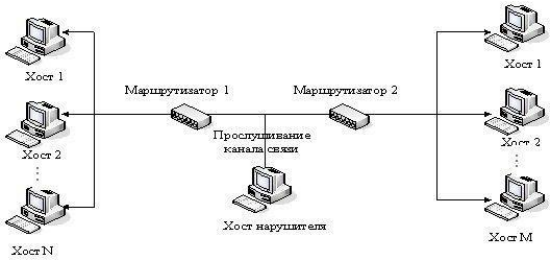

Рис. - Схема реализации угрозы "Анализ сетевого трафика"

2. Сканирование сети

Суть данной атаки состоит в сборе информации о топологии сети, об открытых портах, используемых протоколах и т.п. Как правило, реализация данной угрозы предшествует дальнейшим действиям злоумышленника с использованием полученных в результате сканирования данных.

Угроза выявления пароля

Целью атаки является преодоление парольной защиты и получении НСД к чужой информации. Методов для кражи пароля очень много: простой перебор всех возможных значений пароля, перебор с помощью специальных программ (*атака словаря*), перехват пароля с помощью программы-анализатора сетевого трафика.

3. **Подмена доверенного объекта сети и передача по каналам связи сообщенийот его имени с присвоением его прав доступа.** Доверенный объект – это элемент сети, легально подключенный к серверу.

Такая угроза эффективно реализуется в системах, где применяются нестойкие алгоритмыидентификации и аутентификации хостов, пользователей и т.д.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав *доверенного субъекта* взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени *доверенного субъекта*. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh- службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа, установленные его пользователем для доверенного абонента, к техническому средству ИС – цели угроз.

4. Навязывание ложного маршрута сети

Данная атака стала возможной из-за недостатков протоколов маршрутизации (RIP, OSPF, *LSP*) и управления сетью (ICMP, SNMP), таких как слабая аутентификация маршрутизаторов. Суть атаки состоит в том, что злоумышленник, используя уязвимости протоколов, вносит несанкционированные изменения в маршрутно-адресные таблицы.

5. Внедрение ложного объекта сети

Когда изначально объекты сети не знают информацию друг о друге, то для построения адресных таблиц и последующего взаимодействия, используется *механизм запрос* (как правило, широковещательный) - ответ с искомой информацией. При этом если нарушитель перехватил такой запрос, то он может выдать ложный ответ, изменить таблицу маршрутизации всей сети, и выдать себя за легального субъекта сети. В дальнейшем все пакеты, направленные к легальному субъекту, будут проходить через злоумышленника.

6. Отказ в обслуживании

Этот тип атак является одним из самых распространенных в настоящее время. Целью такой атаки является отказ в обслуживании, то есть нарушение доступности информации для законных субъектов информационного обмена.

Могут быть выделены несколько разновидностей таких угроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИС на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований ко времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по *протоколу ICMP* (Ping *flooding*), шторм запросов на установление TCP-соединений (SYN-*flooding*), шторм запросов к FTP-серверу;
- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение *очередей запросов* на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи либо получают отказ в обслуживании ввиду переполнения *очередей запросов*, дискового пространства памятии т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-*flooding*), шторм сообщений почтовому серверу (*Spam*);
- явный отказ в обслуживании, вызванный нарушением логической связности

между техническими средствами ИС при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-*flooding*) или идентификационной и аутентификационной информации;

- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа "Land", "TearDrop", "Bonk", "*Nuke*", "UDP-*bomb*") или имеющих длину, превышающую максимально допустимый размер (угроза типа "Ping Death"), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Контрольные вопросы

1. Какие события безопасности должны фиксироваться в журнале аудита?
2. Какие параметры определяют политику аудита?
3. Целесообразно ли с точки зрения безопасности компьютерной системы объединение в одном лице функций администратора и аудитора?
4. Целесообразно ли с точки зрения безопасности компьютерной системы разрешать анонимный доступ к ее информационным ресурсам?
5. Как должен передаваться по сети (с точки зрения безопасности компьютерной системы) пароль пользователя (или другая аутентифицирующая информация)?
6. Нужно ли ограничивать права пользователей по запуску прикладных программ и почему?
7. Какое из дополнительных правил ограниченного использования программ кажется Вам наиболее эффективным и почему?
8. Из каких этапов состоит построение политики безопасности для компьютерной системы?
9. К чему может привести ошибочное определение политики безопасности (приведите примеры)?
10. Почему, на Ваш взгляд, многие системные администраторы пренебрегают использованием большинства из рассмотренных в данной работе параметров политики безопасности?

Практическая работа №2. Получение сертификата

Цель занятия: Ознакомить обучающихся с основными понятиями работы в табличном редакторе, работе с БД в электронных таблицах

Содержание и порядок выполнения задания:

Теоретический материал

Что такое SSL-сертификат?

SSL-сертификат – это цифровой сертификат, удостоверяющий подлинность веб-сайта и позволяющий использовать зашифрованное соединение. Аббревиатура SSL означает Secure Sockets Layer – протокол безопасности, создающий зашифрованное соединение между веб-сервером и веб-браузером.

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.

Как работают SSL-сертификаты?

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.

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.

Чтобы просмотреть сведения об SSL-сертификате, можно щелкнуть значок замка, расположенный на панели браузера. Данные, входящие в SSL-сертификат, обычно включают:

- Доменное имя, для которого выпущен сертификат.
- Лицо, организация или устройство, для которого выпущен сертификат.
- Центр сертификации, выдавший сертификат.
- Цифровая подпись центра сертификации.
- Связанные поддомены.
- Дата выдачи сертификата.
- Срок действия сертификата.
- Открытый ключ (закрытый ключ не раскрывается).

Зачем нужен SSL-сертификат

SSL-сертификаты сайтов требуются для обеспечения безопасности данных пользователей, подтверждения прав собственности на сайт, предотвращения создание поддельной версии сайта злоумышленниками и обеспечения доверия со стороны пользователей.

Если использование веб-сайта предполагает вход в систему, ввод личных данных, таких как номера кредитных карт, или просмотр конфиденциальной информации, такой как данные медицинской страховки, или финансовой информации, то важно сохранить конфиденциальность этих данных. SSL-сертификаты помогают сохранить конфиденциальность онлайн-транзакций и

гарантируют пользователям, что веб-сайт является подлинным и безопасным для ввода личных данных.

Для бизнеса более актуален тот факт, что SSL-сертификаты требуются для веб-адресов HTTPS. HTTPS – это безопасная форма HTTP, то есть трафик веб-сайтов HTTPS зашифрован с помощью SSL. Большинство браузеров помечают сайты HTTP, не имеющие SSL-сертификатов, как небезопасные. Это сигнал пользователям о том, что сайт может быть небезопасным, а для компаний это стимул перейти на HTTPS.

SSL-сертификат помогает защитить такую информацию, как:

- Учетные данные для входа в систему.
- Операции по кредитной карте и информацию о банковском счете.
- Личную информацию: полное имя, адрес, дату рождения, номер телефона.
- Юридические документы и контракты.
- Медицинские документы.
- Конфиденциальную информацию.

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)

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.

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.

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. 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.

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. Например, один Wildcard-сертификат для веб-сайта можно использовать для защиты следующих страниц:

- payments.yourdomain.com
- login.yourdomain.com
- mail.yourdomain.com
- download.yourdomain.com
- anything.yourdomain.com

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.

Например:

- example.com

- org
- this-domain.net
- anything.com.au
- example.com
- example.org

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.

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.

Задание.

Составьте по материалам лекции 15 - 20 вопросов с ответами

Как получить SSL-сертификат

SSL-сертификат можно получить непосредственно в центре сертификации. Центры сертификации, иногда также называемые сертифицирующими организациями, ежегодно выдают миллионы SSL-сертификатов. Они играют важную роль в работе интернета и обеспечивают прозрачное и надежное взаимодействие в сети.

Стоимость SSL-сертификата может доходить до сотен долларов, в зависимости от требуемого уровня безопасности. После выбора типа сертификата можно найти издателей сертификатов, предлагающих SSL-сертификаты нужного уровня.

Получение SSL-сертификата включает следующие шаги:

- Подготовка. Настройте сервер, и убедитесь, что ваша запись WHOIS обновлена и соответствует данным, отправляемым в центр сертификации (она должна отображать правильное название и адрес компании и т. д.).
- Создание запроса на подпись SSL-сертификата (CSR) на вашем сервере. С этим действием может помочь ваша хостинговая компания.

- Отправка запроса в центр сертификации для проверки данных о вашем домене и компании.
- Установка полученного сертификата после завершения процесса.

После получения сертификата его необходимо настроить на вашем веб-хосте или серверах, если вы обеспечиваете хостинг веб-сайта самостоятельно.

Скорость получения сертификата зависит от типа сертификата и поставщика сертификатов. Для завершения каждого уровня проверки требуется разное время. Простой SSL-сертификат, подтверждающий домен, может быть выпущен в течение нескольких минут после заказа, а получение сертификата с расширенной проверкой может занять целую неделю.

Можно ли использовать SSL-сертификат на нескольких серверах?

Один SSL-сертификат можно использовать для нескольких доменов на одном сервере. В зависимости от поставщика, можно также использовать один SSL-сертификат на нескольких серверах. Это позволяют мультидоменные SSL-сертификаты, описанные выше.

Как следует из названия, мультидоменные SSL-сертификаты работают с несколькими доменами. Количество доменов остается на усмотрение конкретного центра сертификации. Мультидоменный SSL-сертификат отличается от однодоменного SSL-сертификата, который, как следует из названия, предназначен для защиты одного домена.

Мультидоменные SSL-сертификаты также называются SAN-сертификатами. SAN означает альтернативное имя субъекта. Каждый мультидоменный сертификат имеет дополнительные поля (например, альтернативные имена субъектов), которые можно использовать для перечисления дополнительных доменов, чтобы на них распространялся один сертификат.

Сертификаты унифицированных коммуникаций (UCC) и Wildcard-сертификаты также можно применять на нескольких доменах и, в последнем случае, на неограниченном количестве поддоменов.

Что происходит по истечении срока действия SSL-сертификата?

Срок действия SSL-сертификатов истекает, он не длится вечно. Центр сертификации / Форум браузеров, который де-факто выступает в качестве регулирующего органа для индустрии SSL, заявляет, что срок действия SSL-сертификатов не должен превышать 27 месяцев. По сути, это означает, что SSL-сертификат можно использовать в течение двух лет, плюс до трех месяцев на продление срока действия предыдущего сертификата.

Срок действия SSL-сертификатов истекает, поскольку, как и при любой другой форме аутентификации, информацию необходимо периодически перепроверять и убеждаться в ее актуальности. В интернете все очень быстро меняется, покупаются и продаются компании и веб-сайты. При смене владельцев также меняется информация, относящаяся к SSL-сертификатам. Ограниченный срок действия SSL-сертификатов обеспечивает актуальность и точность информации, используемой для аутентификации серверов и организаций.

Раньше SSL-сертификаты могли выдаваться на срок до пяти лет, который впоследствии был сокращен до трех лет, а в последнее время до двух лет плюс возможность использовать дополнительные три месяца. В 2020 году Google, Apple и

Mozilla объявили, что будут применять годовые SSL-сертификаты, несмотря на то, что это предложение было отклонено Центрами сертификации / Форумом браузеров. Это решение вступило в силу в сентябре 2020 года. Не исключено, что в будущем срок действия SSL-сертификатов сократится еще.

Когда срок действия SSL-сертификата истекает, соответствующий сайт становится недоступным. Когда пользователь открывает веб-сайт в браузере, в течение нескольких миллисекунд проверяется действительность SSL-сертификата (в рамках подтверждения SSL-соединения). Если срок действия SSL-сертификата истек, посетители сайта получат сообщение: «Этот сайт небезопасен. Существуют возможные риски».

У пользователей есть возможность продолжить, однако не рекомендуется делать это, учитывая связанные риски кибербезопасности, в том числе вероятность столкнуться с вредоносными программами. Это существенно влияет на показатель отказов при посещении веб-сайта, поскольку пользователи быстро покидают его.

Осведомленность о сроке истечения SSL-сертификатов является проблемой для крупных предприятий. В то время как малые и средние предприятия имеют один или несколько SSL-сертификатов, крупные предприятия, работающие на различных рынках и имеющие множество веб-сайтов и сетей, имеют также множество SSL-сертификатов. Поэтому причиной того, что компания допустила истечение срока действия своего SSL-сертификата, обычно является недосмотр, а не отсутствие компетентности. Лучший способ для крупных компаний поддерживать осведомленность об истечении срока действия SSL-сертификатов – использовать платформу управления сертификатами. На рынке представлены различные продукты, которые можно найти с помощью онлайн-поиска. Это позволит компаниям просматривать цифровые сертификаты и управлять ими в рамках всей инфраструктуры. При использовании такой платформы важно регулярно входить в систему и проверять, когда необходимо продлить обновления.

Если срок действия сертификата истечет, сертификат станет недействительным, и выполнять безопасные транзакции на веб-сайте станет невозможно. Центр сертификации предложит обновить SSL-сертификат до истечения срока его действия.

Все центры сертификации и службы SSL, используемые для получения SSL-сертификатов, отправляют уведомления об истечении срока действия сертификата с заданной периодичностью, обычно начиная с 90 дней до окончания срока действия сертификата. Постарайтесь, чтобы эти уведомления отправлялись на несколько адресов электронной почты, а не одному человеку, который к моменту отправки уведомления может покинуть компанию или перейти на другую должность. Убедитесь, что соответствующие сотрудники компании включены в список рассылки и своевременно получат уведомление.

Как узнать, есть ли у сайта SSL-сертификат

Самый простой способ узнать, есть ли у сайта SSL-сертификат – обратить внимание на следующие элементы в адресной строке браузера:

- Если веб-адрес начинается с HTTPS, а не с HTTP, значит он защищен с помощью SSL-сертификата.

- Для защищенных сайтов отображается значок закрытого замка, который можно щелкнуть и посмотреть сведения о безопасности. У самых надежных сайтов будут зеленые замки или адресные строки.
- Браузеры также показывают предупреждения, если соединение небезопасно, например красный замок, открытый замок, линию, пересекающую адрес веб-сайта, треугольник-предупреждение над значком замка.

Как обеспечить безопасность онлайн-сеанса

Личные данные и платежные реквизиты можно указывать только на веб-сайтах, защищенных сертификатами с расширенной проверкой или сертификатами, подтверждающие организацию. Сертификаты, подтверждающие домен, не подходят для сайтов электронной коммерции. Сайты, защищенные сертификатами с расширенной проверкой или сертификатами, подтверждающими организацию, можно определить, посмотрев на адресную строку. Для сайтов, защищенных сертификатами с расширенной проверкой, название организации отображается в адресной строке. Для сайтов, защищенных сертификатами, подтверждающими организацию, данные о названии организации, отображаются по щелчку на значке замка. Для сайтов с сертификатами, подтверждающими домен, отображается только значок замка.

Ознакомьтесь с политикой конфиденциальности веб-сайта. Это позволяет понять, как будут использоваться ваши данные. Законопослушные компании обычно прозрачно описывают сбор и действия с данными.

Обратите внимание на сигналы и индикаторы, вызывающие доверие к веб-сайту.

Наряду с SSL-сертификатами, это могут быть логотипы или значки, показывающие репутацию и соответствие веб-сайта определенным стандартам безопасности. Другие признаки, по которым можно оценить сайт, включают проверку физического адреса и номера телефона, ознакомление с политикой возврата товаров и средств, проверку правдоподобности цен – ведь бесплатный сыр может оказаться в мышеловке.

Будьте внимательны к фишинговым атакам.

Иногда злоумышленники создают веб-сайты, имитирующие существующие, чтобы обманом заставить людей сделать покупку или выполнить вход на фишинговый сайт. Фишинговый сайт может получить SSL-сертификат и, следовательно, зашифровать весь трафик, проходящий между сайтом и пользователями. Растущая доля фишинговых атак происходит на HTTPS-сайтах. Происходит обман пользователей, которых успокаивает наличие значка замка.

Чтобы избежать подобных атак:

- Всегда проверяйте, что домен сайта, на котором вы находитесь, написан правильно. Веб-адрес поддельного сайта может отличаться только одним символом, например, amaz0n.com вместо amazon.com. В случае сомнений введите домен прямо в браузере, чтобы убедиться, что вы подключаетесь именно к тому веб-сайту, который собираетесь посетить.
- Никогда не вводите логины, пароли, банковские реквизиты и другую личную информацию на сайте, если вы не уверены в его подлинности.
- Всегда оценивайте, что предлагается на сайте, не выглядит ли он подозрительным и действительно ли вам нужно на нем регистрироваться.

- Убедитесь, что ваши устройства защищены надлежащим образом: Kaspersky Internet Security проверяет веб-адреса по базе фишинговых сайтов и обнаруживает мошенничество независимо от того, насколько безопасным выглядит ресурс.

Угрозы кибербезопасности продолжают расти, но понимание типов SSL-сертификатов, и того, как отличить безопасный сайт от потенциально опасного, поможет интернет-пользователям избежать мошенничества и защитить свои личные данные от киберпреступников.

Задание 2.

Создайте презентацию по материалам лекции