## Лабораторная 24

# 1. Поясните понятия «авторизация», «роль», «привилегия», «ACL».

***Авторизация*** - процедура проверки прав аутентифицированного пользователя.

***Роль*** - набор правил, определяющих, какими привилегиями и по отношению к каким объектам будет обладать пользователь, которому будет назначена эта роль.

***Привилегия*** — полномочие субъекта относительно какого-то объекта

***ACL*** — список управления доступом, который определяет, кто или что может получать доступ к объекту

# 2. Что такое casl?

позволяет определить права доступа в одном месте, для всех пользователей

CASL концентрирует внимание не на том кем является пользователь, а на том что он может делать, т.е. на его возможностях. Это позволяет распределять эти возможности разным ролям или группам пользователей без лишних усилий. Это значит, что мы можем прописать права доступа для авторизированных и не авторизированных пользователей

# 3. Перечислите известные модели управления доступом.

***MAC / DAC (обязательный / дискреционный контроль доступа)***  DAC - позволяет владельцу определять, у кого есть доступ. MAC права доступа определяются администратором или общим правилом.

***IBAC (контроль доступа на основе личности)*** - этот метод фокусируется на личности пользователя как на основе привилегий. Каждому человеку предоставляются определенные права доступа для каждой операции

***RBAC (управление доступом на основе ролей)*** - привилегии сгруппированы по ролям, и каждому пользователю назначается роль.

***ABAC (управление доступом на основе атрибутов)*** эволюционировавшая RBAC - в системах, где существует множество атрибутов, разделяющих доступ к внутренним ресурсам (например, прошел ли пользователь какие-либо тесты и прошел обучение использованию этой части системы и т. Д.), Использование модели RBAC приведет к так называемому взрывному росту ролей. - необходимость определения всех ролей, разделяющих пользователей на основе их атрибутов. ABAC стремится решить эту проблему, предоставляя основу для определения прав доступа на основе различных свойств пользователя.

**Лабораторная 25**

<https://ssl.com.ua/info/what-is-ssl/>

<https://www.kaspersky.ru/resource-center/definitions/what-is-a-ssl-certificate>

Цифровой сертификат — выпущенный удостоверяющим центром электронный или печатный документ, подтверждающий принадлежность владельцу открытого ключа или каких-либо атрибутов

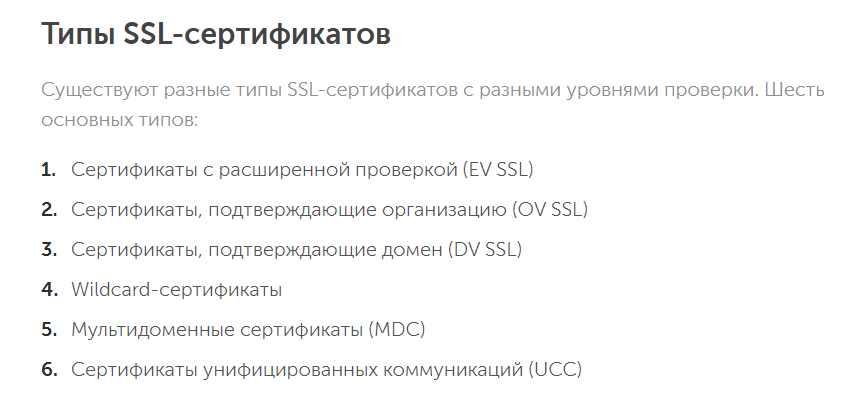
SSL:

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.

**SSL-сертификат** нужен для того, чтобы мошенники не могли перехватить личные данные, которые пользователи вводят у вас на сайте. Личные данные — это логины и пароли от аккаунтов, номера банковских карт, адреса электронной почты и т.д. Это значит, что SSL-сертификат пригодится на сайтах банков, платёжных систем, корпораций, интернет-магазинов, социальных сетей, государственных предприятий, онлайн-форумов и др.

Клиент делает заказ у вас на сайте. Чтобы оплатить товар, он вводит данные кредитной карты. Когда заказ оформлен, информация отправляется на ваш веб-сервер. На этом этапе её могут перехватить мошенники.

Если на сайте есть SSL-сертификат, между браузером клиента и сайтом устанавливается защищённое соединение. В этом случае браузер сначала преобразует номер карты в случайный набор символов и только потом отправляет его на сервер. Расшифровать сообщение получится только специальным ключом, который хранится на сервере. Если мошенники и перехватят информацию, они не поймут, что она означает.



## Лабораторная 26

# 1. Что такое хеш-функция?

# 2. Что такое хеширование?

# 3. Перечислите алгоритмы хеширования.

# 4. Поясните понятие «сеансовый ключ»

# 5. Поясните понятия «публичный» и «секретный» ключи?

# 6. Поясните понятие «дайджест».

# 7. Для чего используется дайджест.

# 8. Поясните принцип работы алгоритма Диффи-Хеллмана.

# 9. Поясните понятие «цифровая подпись», объясните принцип ее применения.