Тема № 4

Аутентификация субъектов и объектов взаимодействия

Занятие № 1

Сетевая аутентификация. Подсистема аутентификации. Протоколы аутентификации.

Цели занятия

Учебные и воспитательные цели:

1. Дать представление обучаемым о сетевой аутентификации, о ее подсистеме, а также рассмотреть протоколы аутентификации, их положительные стороны и недостатки.
2. Добиться понимания курсантами высокой важности и актуальности учебных вопросов, качественное изучение которых окажет положительное влияние на дальнейшее изучение дисциплин по специальности.
3. Воспитать у обучающихся чувство патриотизма, трудолюбия и дисциплинированности в ходе изучения данной дисциплины.
4. Дать направление для самостоятельной подготовки курсантов по теме занятия.

Учебные вопросы

1. Унификация данных сетевой аутентификации.
2. Единые системы аутентификации и авторизации.
3. Аутентификация в клиент-серверных системах.
4. Простейшие протоколы аутентификации. Протоколы RADIUS и TACACS.

Содержание

Литература и другие источники информации

1. Информационная безопасность открытых систем: Учебник для вузов. в 2-ух томах. Том1 – Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников, Н. Г. Милославская, А.И. Толстой, Д.В. Ушаков. – М.: Горячая линия – Телеком, 2006. – 536 с.: ил.

2. Информационная безопасность открытых систем: Учебник для вузов. в 2-ух томах. Том2 – Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д. В. Ушаков. – М.: Горячая линия – Телеком, 2008. – 558 с.: ил.

Учебный вопрос № 1

Учебный вопрос № 1

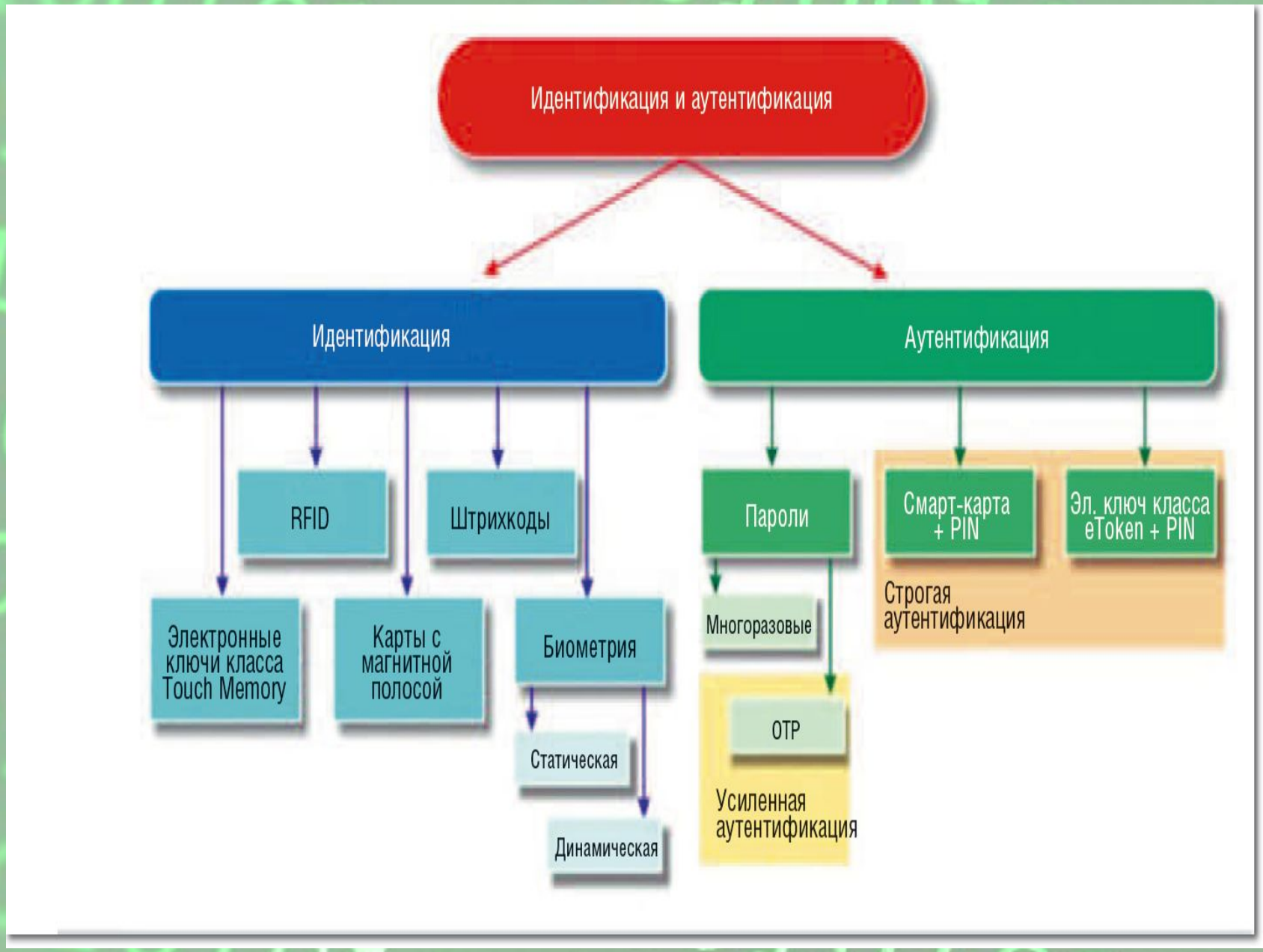
Идентификация в информационных системах — присвоение субъектам и объектам идентификатора и / или сравнение идентификатора с перечнем присвоенных идентификаторов. Например, идентификация по штрих-коду.

Термин «идентификация» в отношении личности пользователей в информационной безопасности часто ошибочно используется вместо понятий аутентификация и авторизация.

Авториза́ция (англ. *Authorization* «разрешение; уполномочивание») — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий. Часто можно услышать выражение, что какой-то человек «авторизован» для выполнения данной операции — это значит, что он имеет на неё право.

Авторизацию не следует путать с **аутентификацией** — процедурой проверки легальности пользователя или данных, например, проверки соответствия введённого пользователем пароля к учётной записи паролю в базе данных, или проверка цифровой подписи письма по ключу шифрования, или проверка контрольной суммы файла на соответствие заявленной автором этого файла. Авторизация же производит контроль доступа к различным ресурсам системы в процессе работы легальных пользователей *после* успешного прохождения ими аутентификации.

Учебный вопрос № 1



Учебный вопрос № 1

Подсистема управления сетевым доступом (одна из 4-х подсистем ПАСЗИ) – осуществляет идентификацию, проверку подлинности и контроль удаленного доступа субъектов в информационную систему: к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям и полям записей.

Сетевая аутентификация – процедура проверки подлинности удалённого пользователя, т.е. его принадлежности предъявляемому им идентификатору (паролю, устройству и т.п.).

Идентификатор присваивается пользователю, процессу, действующему от имени какого-либо пользователя, или программно-аппаратному компоненту и позволяет им назвать себя, т.е. сообщить свое «имя».

После проверки подлинности принимается решение о разрешении доступа к ресурсам системы или отказе в нем.

Учебный вопрос № 1

Односторонняя аутентификация – клиент доказывает свою подлинность серверу.

Двусторонняя (взаимной) аутентификация - и клиент, и сервер доказывают свою подлинность .

3 подхода к аутентификации:

1 «Субъект знает» (нечто, известное субъекту) – претендент обладает некоторой информацией, которой нет у других субъектов ИС (паролями, секретными ключами, PIN-ами, и т.п.) и знание которой он демонстрирует в протоколах аутентификации.

Эффективность парольных систем зависит от секретности, а пароли довольно тяжело хранить в тайне.

2 «Субъект обладает» (нечто, имеющееся у субъекта) – претендент имеет некоторый физический предмет (магнитную карту и т.п.), необходимый для его участия в аутентификации и выполняющий для него вспомогательные криптографические преобразования информации.

Данный тип аутентификации считается достаточно надёжным.

Учебный вопрос № 2

3. «Субъект есть» (нечто, присущее субъекту) – в системе проверяются некоторые признаки, характеризующие человеческую индивидуальность субъекта (биометрические признаки).

Одно из самых удобных решений для пользователя, не требует запоминания паролей и надёжного хранения аппаратных средств.

В случае перехвата идентификационных данных (при дистанционном подключении) – их невозможно заменить.

- **Однофакторная аутентификация** – на основе только одного из вышеперечисленных подходов;
- **Двухфакторная аутентификация** – на основе комбинации двух из трёх вышеперечисленных подходов;
- **Трёхфакторная аутентификация** – использует все три подхода.

Учебный вопрос № 2

Помимо необходимых для аутентификации данных и признаков принадлежности к какой-либо группе и роли, в ИС организации часто содержатся полезные дополнительные сведения о пользователе:

- имя и фамилия,
- должность,
- телефон,
- адрес электронной почты и другие.

Во многих организациях значительная часть времени системных администраторов тратиться на решение задач, связанных с учётными записями и паролями, включая первоначальное создание пользовательских учётных записей при приёме пользователей на работу, удаление – при их увольнении, изменение ролей – при смене должности, переустановку паролей, когда они забываются. Наличие нескольких учётных записей у каждого пользователя увеличивает соответствующую нагрузку на системных администраторов.

Учебный вопрос № 2

Хранилища данных о пользователях либо объединяются в одно целое (и тогда на пользователя приходится одна учётная запись с верными значениями всех атрибутов), либо синхронизируются при помощи метакаталога, в которых разные атрибуты могут иметь разные источники происхождения.

Каталог организации – хранилище данных обо всех пользователях её ИС (в частности, данных, необходимых для аутентификации). Как правило, современные каталоги поддерживают протокол LDAP (Lightweight Directory Access Protocol, облегчённый протокол доступа к каталогам.RFC4511).

Централизованный каталог также предоставляет пользователям ресурсы всех рабочих станций в интрасети, на которые у них есть права, без отдельных затрат на администрирование каждой из них.

Учебный вопрос № 2

С помощью единого каталога несколько приложений (а в идеале все корпоративные приложения) используют одну и ту же учётную запись в каталоге для аутентификации; благодаря этому отпадает необходимость отдельно администрировать данные о пользователях в различных системах.

Метакаталог – средство, позволяющие осуществлять интеллектуальную синхронизацию между разнородными хранилищами данных.

При помощи метакаталога существующие хранилища данных о пользователях могут быть объединены в единую систему каталогов, в которой заведение, редактирование и удаление учётной записи производятся в одной из соединённых систем, а метакаталог распространяет их на остальные системы.

Учебный вопрос № 2

- Единую систему аутентификации чаще всего отождествляют с системой однократной регистрации (Single Sign-On, SSO), предназначенной для снятия необходимости многократно вводить пароли или аутентифицироваться каким-либо иным способом при работе с различными приложениями.

Появляется эффект «слабого звена»: например, при помощи сниффера злоумышленник перехватывает пароль и получает доступ ко всем системам пользователя одновременно.

Наиболее полное решение задачи однократной регистрации осуществляется при использовании прокси-аутентификации. Система предоставляет механизм, с помощью которого программная компонента может запрашивать у клиентской части аутентификационные данные, связанные с рабочей станцией. Такой функцией обладают современные серверные системы.

Учебный вопрос № 2

Традиционно права доступа к ресурсам хранятся вместе с самими ресурсами или системами, отвечающими за предоставление этих ресурсов.

Управление правами конкретного пользователя может требовать работы с несколькими разнородными интерфейсами. Тогда администрирование прав доступа можно упростить, объединяя пользователей в группы и приписывая им роли.

Под группой понимают явно указанный список пользователей.

Группы и роли могут быть организованы в иерархию подгрупп и подролей с наследованием прав доступа. Аналогично ресурсы должны быть организованы в иерархию (типа каталогов файловой системы). Это позволит назначать права доступа сразу к целому классу ресурсов. Графически сведения об установленных правах можно представлять, как матрицу, в которой по горизонтали перечисляются группы, роли и отдельные пользователи, а по вертикали – сами ресурсы. Ячейка этой матрицы содержит информацию о правах доступа: «доступ разрешён» и «запрещён».

Учебный вопрос № 2

Персонализация, или персонификация, пользовательского интерфейса – задача, связанная с созданием единой системы авторизации, поскольку важно не только предоставить пользователю доступ к нужным ему ресурсам, но и сделать этот доступ удобным. С другой стороны, доступ к запрещённым ресурсам должен быть закрыт, а пользователь вообще не должен видеть путей доступа к ним (так, пользователь не должен видеть в приложении кнопок, нажатие на которые приводит к сообщениям типа «Вы не имеете права использовать эту функцию»).

Заключение

Подведение итогов занятия
Выдача задания на самостоятельную подготовку

Вопросы для самостоятельной подготовки:

1. Дайте определение понятию «Аутентификация» и ее цель.
2. Поясните понятие «Сетевая аутентификация» и ее назначение.
3. Сколько существует подходов к аутентификации, описание этих подходов.
4. Односторонняя и двухсторонняя аутентификация.
5. Приведите примеры использования аутентификации в современном мире.