Идентификация и аутентификация сотрудников банков.

Идентификация и аутентификация сотрудников банка.

Москва. 2018

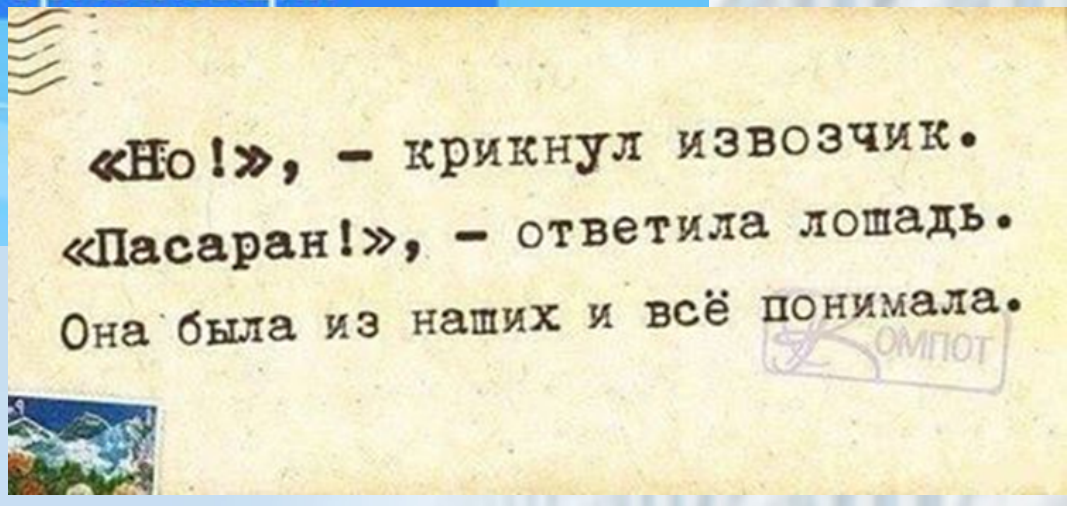
Солонин В.Н. «СДМ-Банк» ПАО


Центр Личностного и Духовного развития «Мозговой Штурм»
представляет:
психокинетическое
СГИБАНИЕ
ЛОЖЕК
На этом семинаре Вы
САМИ согнете ложку
силой СВОЕЙ мысли, если
не получиться, мы вернем
Вам деньги.

ГБПОУ Колледж декоративно-прикладного искусства имени Карла Фаберже

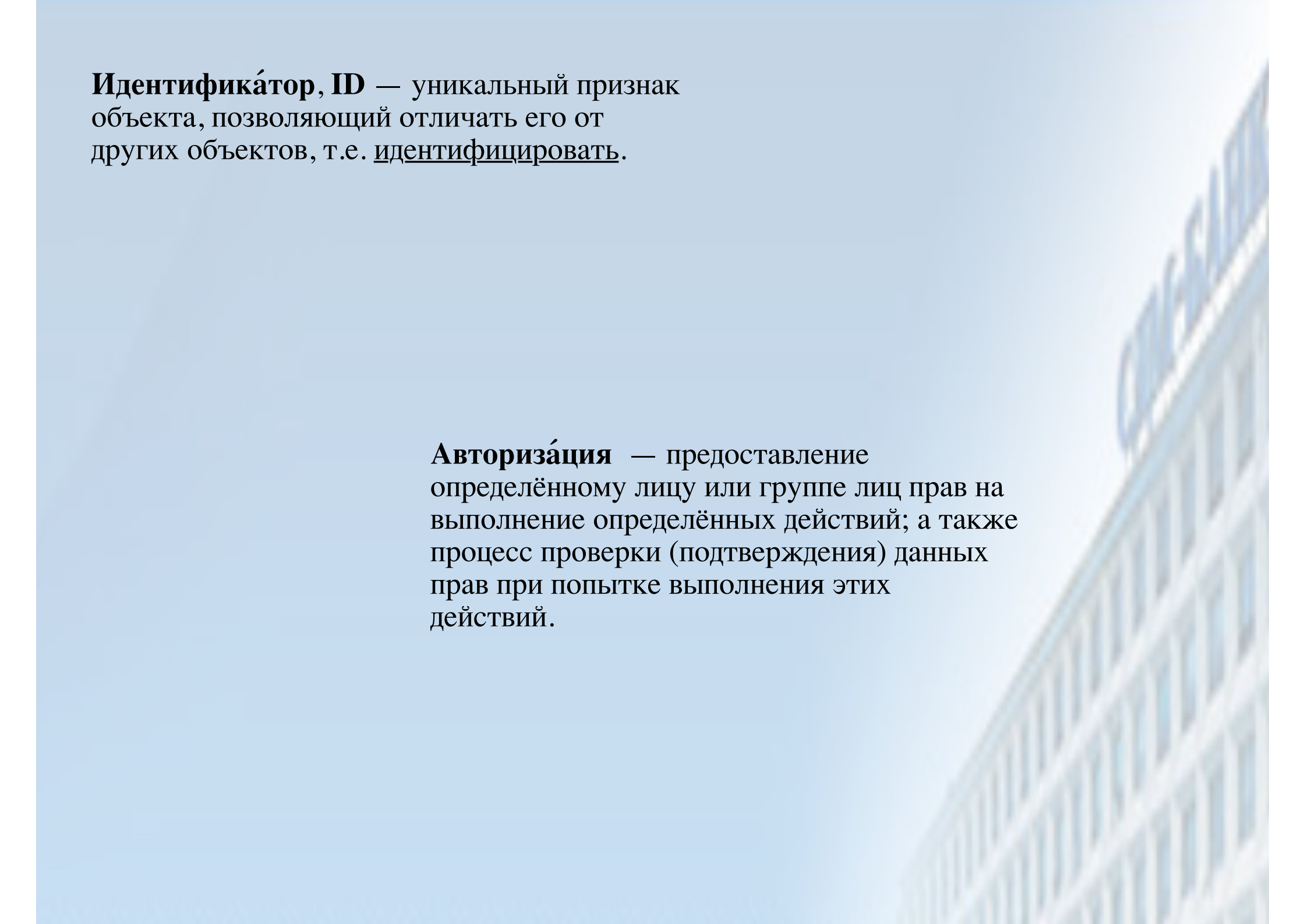
Парольные и не парольные средства аутентификации

МДК.01.01. Обеспечение организации системы безопасности организации



Идентифика́тор, ID — уникальный признак объекта, позволяющий отличать его от других объектов, т.е. идентифицировать.

Авториза́ция — предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий.



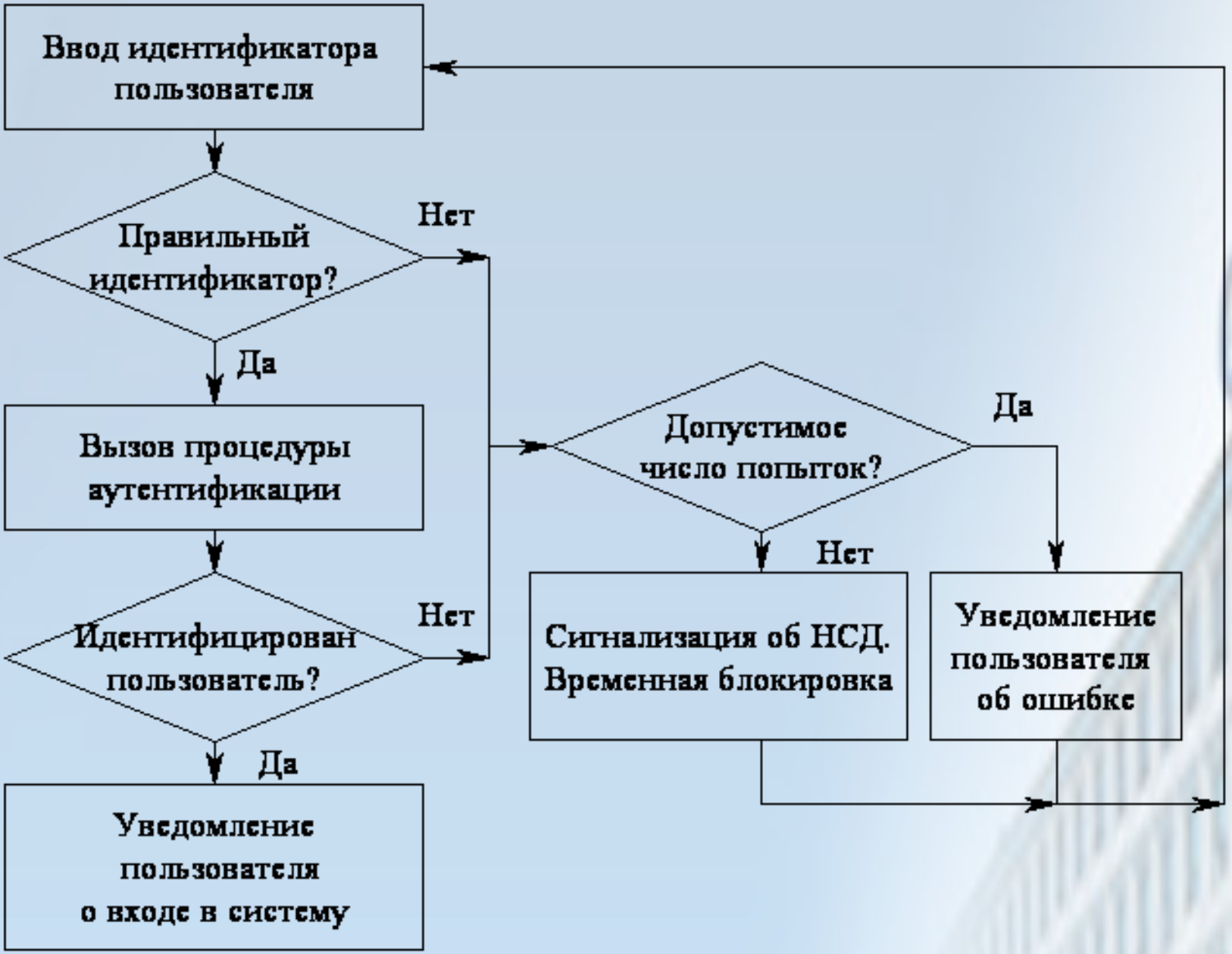
Аутентифика́ция — процедура проверки подлинности, например:

- проверка подлинности пользователя путём сравнения введённого им пароля (для указанного логина) с паролем, сохранённым в базе данных пользовательских логинов;
- подтверждение подлинности электронного письма путём проверки цифровой подписи письма по открытому ключу отправителя;

Факторы аутентификации

1. **Фактор знания.** «Что знаешь только ты?» Нечто, что нам известно, например, какая-либо секретная информация. В привычном случае это пароль, ответ на вопрос.
2. **Фактор владения.** «Что есть только у тебя?» Нечто, чем мы обладаем, например, какой-либо уникальный физический объект. USB Токен, смарт карта.
3. **Фактор сущности.** «Кто ты?» Нечто, что является неотъемлемой частью нас самих. Отпечаток пальца, рисунок радужной оболочки глаза.
4. **Географический фактор.** «Где ты?» Нечто, что определяет наше местонахождение. Географические координаты, IP, присутствие в помещении.

Обычный алгоритм аутентификации



Хороший пароль придумать сложно. Во всем виновато шаблонное мышление

Вспомним простой тест.
Не думая, назовите первое, что придет в голову из категорий:

- 1) фрукт,
- 2) часть лица,
- 3) русский поэт,
- 4) цветок,
- 5) страна.

Это «яблоко», «нос», «Пушкин», «роза» и «Россия»?

Какие часто применяемые атаки на пароль?

1. Кейлогер.
2. Перебор паролей.
3. Перехват трафика.

А НУЖЕН ЛИ ВООБЩЕ ПАРОЛЬ для взлома?

Pass-the-Hash

Эта техника возможна благодаря архитектурным особенностям протокола аутентификации NTLM, разработанного Microsoft в девяностых годах прошлого века. Для того чтобы залогиниться на удаленном хосте, используется хеш пароля, хранящийся в памяти компьютера, с которого происходит аутентификация. Соответственно, его оттуда можно извлечь.

Mimikatz

Для удобной эксплуатации Pass-the-Hash французский исследователь Бенжамен Делпи (Benjamin Delpy) в 2014 году разработал утилиту mimikatz. Она позволяет дампить из памяти clear-text-пароли и NTLM-хеши.

```
Authentication Id : 0 ; 294625 (00000000:00047ee1)
Session           : Interactive from 1
User Name         : Administrator
Domain            : TESTDOMAIN
Logon Server      : WIN-12UU57SPIN9
Logon Time        : 2/1/2016 6:21:21 AM
SID               : S-1-5-21-1100472043-2579244664-3974358937-500
        msv :
         [00010000] CredentialKeys
         * NTLM     : 1543a4536a25d208e652dba231e73cdd
         * SHA1     : 9621d462145820990 5b31ed96fe8f59d899b4ccf
         [00000003] Primary
         * Username : Administrator
         * Domain   : TESTDOMAIN
         * NTLM     : 1543a4536a25d208e652dba231e73cdd
         * SHA1     : 9621d462145820990 5b31ed96fe8f59d899b4ccf
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : TESTDOMAIN
         * Password : Weakpass1
        kerberos :
```

Компания WP Engine провела исследование, в котором проанализировала базу из 10 млн скомпрометированных паролей, созданных самой разношерстной публикой интернета – от генеральных директоров до ученых.

ТОП-50 наиболее часто используемых паролей

1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789
6. 12345
7. 1234
8. 111111
9. 1234567
10. dragon

Наиболее часто использующиеся числа (0–99) в конце пароля

1.	examplepassword**1**	23.84%
2.	examplepassword**2**	6.72%
3.	examplepassword**3**	3.86%
4.	examplepassword**12**	3.55%
5.	examplepassword**7**	3.54%
6.	examplepassword**5**	3.35%
7.	examplepassword**4**	3.19%
8.	examplepassword**6**	3.06%
9.	examplepassword**9**	2.91%
10.	examplepassword**8**	2.89%

Наименее часто использующиеся числа (0–99) в конце пароля

100.	examplepassword**39**	0.15%
99.	examplepassword**49**	0.16%
98.	examplepassword**60**	0.17%
97.	examplepassword**38**	0.18%
96.	examplepassword**37**	0.18%
95.	examplepassword**41**	0.18%
94.	examplepassword**61**	0.18%
93.	examplepassword**46**	0.19%
92.	examplepassword**53**	0.19%
91.	examplepassword**48**	0.19%

Источник: WP Engine

Почему Банки?

Что меняется с добавлением второго фактора? Например Биометрии:

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается база данных характеристик пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются, и результат обработки (биометрический шаблон) заносится в базу данных (исходные данные, такие как результат сканирования пальца или роговицы, обычно не хранятся).

В дальнейшем для идентификации (и одновременно аутентификации) пользователя процесс снятия и обработки повторяется, после чего производится поиск в базе данных шаблонов. В случае успешного поиска личность пользователя и ее подлинность считаются установленными. Для аутентификации достаточно произвести сравнение с одним биометрическим шаблоном, выбранным на основе предварительно введенных данных. Важно то, что результат сравнения носит вероятностный характер.

Что меняется?

Добавляется еще один доверенный участник который проводит аутентификацию пользователя по второму фактору.

В случае со смарт картами – это всем знакомый CA.

Идея

- **Биометрическая аутентификация пользователей**
- Пропуск + Пин-Код (сотрудники не имеющие доступ в финансовую сеть).
- Сканер отпечатка пальцев + Пин-Код (сотрудники работающие в финансовой сети)
- Дополнительно для усиления безопасности может применяться смарт-карта с сертификатом.
- **Сквозная аутентификация в приложениях (Single Sign-On)**
- Один раз авторизовался на компьютере – вход во все системы и приложения (Single Sign-On). При необходимости возможно дополнительное подтверждение .
- **Интеграция системы аутентификации с СКУД**
- Модуль интеграции для СКУД. Если нет отметки о том что пользователь в здании, то доступ на компьютере блокируется.

После утряски и усушки

- **Первый этап**
- Вход в системы с использованием Сертификата и Пин-Кода. Сертификаты ЭП на чипах в пропусках.
- Сквозная аутентификация в приложениях (Single Sign-On)
- Интеграция системы аутентификации с СКУД (доступ к ПК только внутри здания) (IdM)
- Интеграция с кадровой системой, автоматизация создания пользователей в системах.
- Управление паролями без участия пользователей.
- **Второй этап**
- Внедрение электронной подписи (СЭД, Почта и др.)
- **Третий этап**
- Управление правами пользователей во всех системах банка на основе ролевой модели.

Грабли.

- Не все системы умеют 2FA. Дорабатывать либо дорого, либо невозможно.
  - Пароли остаются
    + SSO умеет менять пароль
- Самописное ПО.
  - Пришлось ПО переписать.

Какие цели достигнуты

- Пользователь не знает свой пароль
- Пароль устойчив к взлому за счет использования повышенной сложности
- Во всех системах пользовательские пароли разные
- Учет рабочего времени

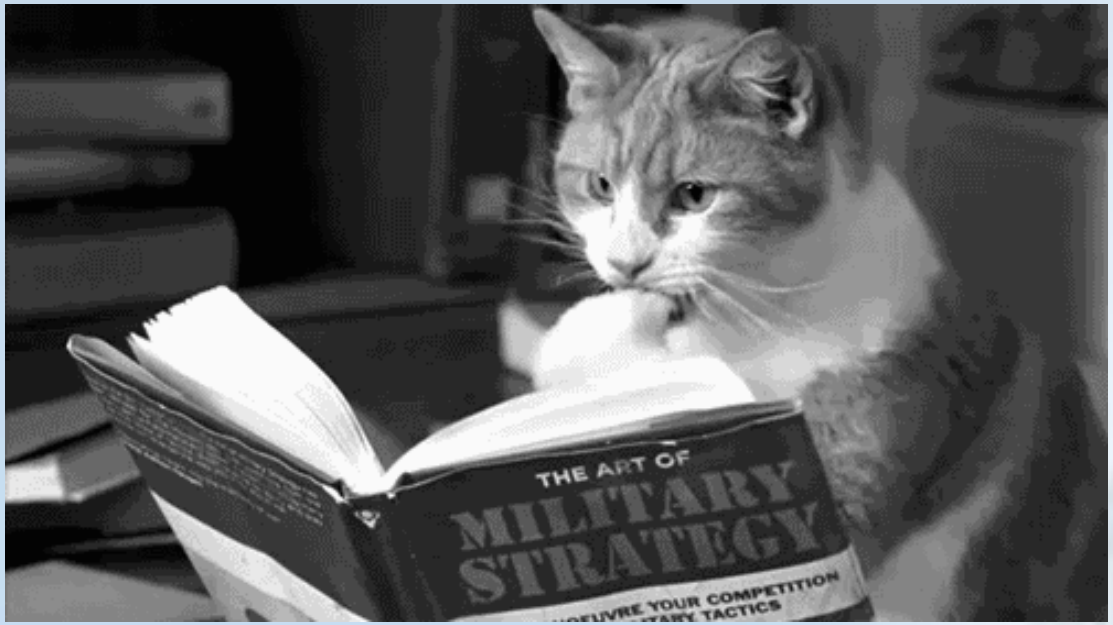
Советы

- Лучше нас самих ТЗ никто не напишет.
- Создайте команду на проект. Включите туда представителей из разных подразделений.
- Мотивируйте на поддержку проекта, как админов так и пользователей.
- Пилот должен быть максимально приближен к целевому внедрению.
- По его окончанию проведите испытания.
- Добейтесь однозначности понимания пунктов ТЗ подрядчиком.

Советы

- Не цепляйтесь за старое. Часто проще создать заново, чем искать ошибки возникшие при миграции.
- Люди не любят менять устоявшийся порядок, проведите рекламную компанию.
- Будьте готовы в сложностям, отделяйте основное от второстепенного.

Конец.



Контакты: solonin@outlook.com