ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ

Государственное бюджетное профессиональное образовательное учреждение г. Москвы Колледж связи № 54 им. П.М.Вострухина

ЛАБОРАТОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

"БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ"

РАЗДЕЛ I. Основы безопасности информационных технологий Тема 7. Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты.

МОСКВА 2016

ЛАБОРАТОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные механизмы защиты информационных систем

МЕХАНИЗМЫ ЗАЩИТЫ ИС

Идентификация и аутентификация

Разграничение доступа пользователей

Криптографическое закрытие данных

Регистрация и оперативное освещение о событиях в системе

Контроль целостности и аутентичности данных

Резервирование и резервное копирование

Фильтрация трафика и трансляция адресов

Обнаружение вторжений (атак)

Выявление и нейтрализация действий вирусов

Затирание остаточной информации

Выявление уязвимостей системы

Маскировка и создание ложных объектов

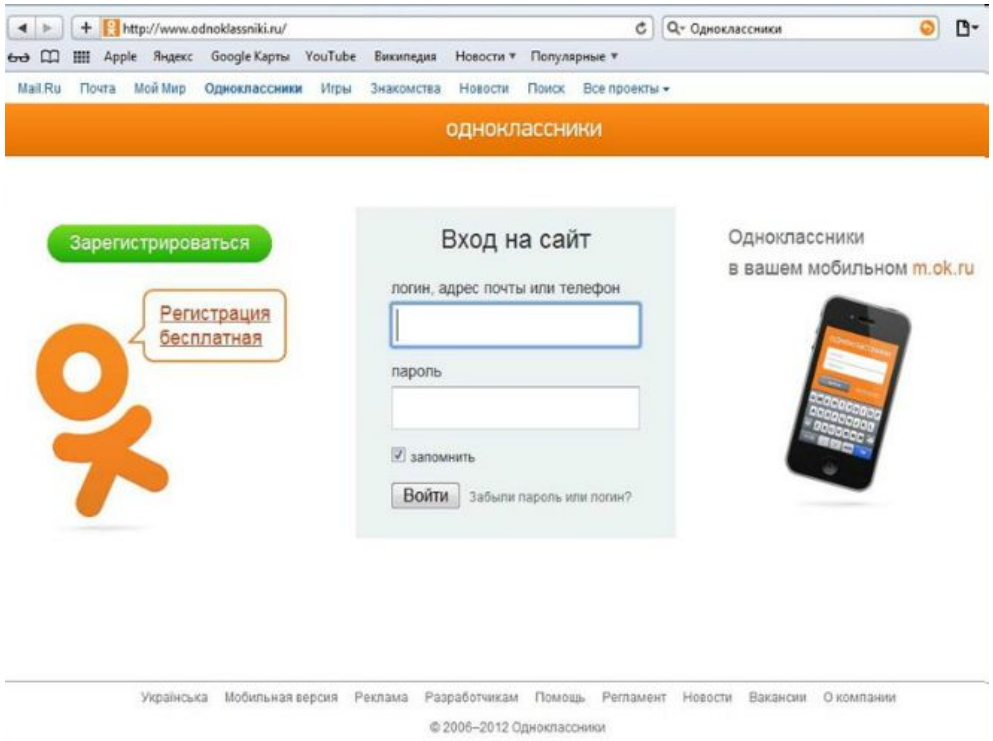
Страхование рисков

Лаборатория Информационной Безопасности

1. Идентификация и аутентификация

Идентификация

Идентификация - присвоение пользователям идентификаторов (уникальных имен или меток), под которыми система "знает" пользователя. Кроме идентификации пользователей, может проводиться идентификация групп пользователей, ресурсов ИС и т.д. Идентификация нужна и для других системных задач, например, для ведения журналов событий. В большинстве случаев идентификация сопровождается аутентификацией.



Аутентификация

Аутентификация - установление подлинности - проверка принадлежности пользователю предъявленного им идентификатора. Например, в начале сеанса работы в ИС пользователь вводит имя и пароль. На основании этих данных система проводит идентификацию (по имени пользователя) и аутентификацию (сопоставляя имя пользователя и введенный пароль).

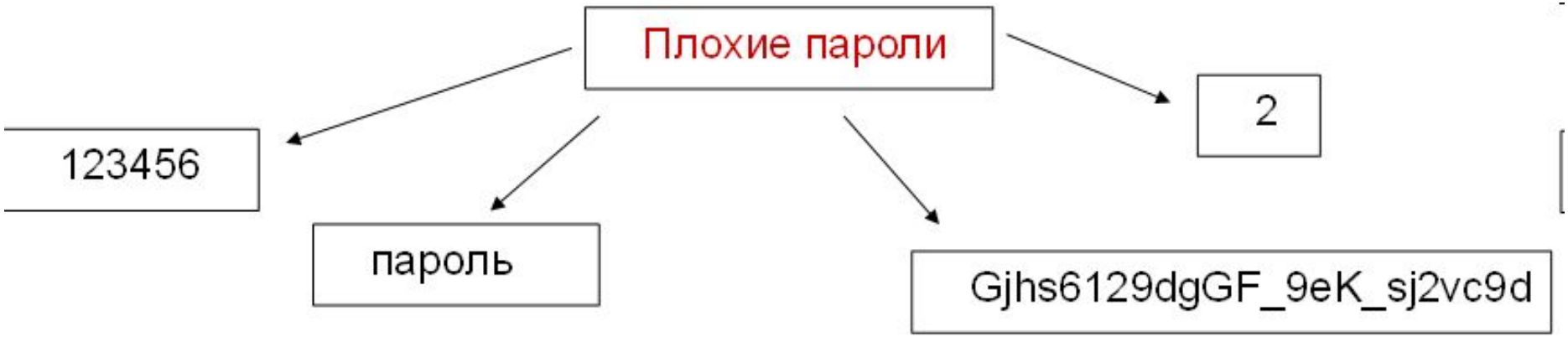
Пароли

Компания SplashData опубликовала свой ежегодный рейтинг самых распространенных паролей, найденных на просторах интернета. В 2013 году большая часть паролей в базе появилась благодаря утечке, допущенной партнером Adobe — консалтинговой компанией Stricture Consulting Group.

Будьте осторожны и не используйте такие простые пароли, если не хотите, чтобы ваш аккаунт в соц. сети, почта или личная SMS-переписка оказались в руках у посторонних людей!

Лаборатория Информационной Безопасности

Пароли



"2" - один символ, легко перебрать.

"123456" - один из популярных паролей (еще примеры - 123; 111; qwerty; qazwsx; qazwsxedc; password; "ваш логин"; "номер телефона" и т.д.).

"пароль" - словарное слово, после перебора популярных паролей, перебирают слова из словаря.

"Gjhs6129dgGF_9eK_sj2vc9d" - пароль очень сложный, его не запомнят, а запишут и приклеят к монитору, пароль должен быть только в голове (или в сейфе).

Лаборатория Информационной Безопасности

2. Разграничение доступа пользователей

Разграничение доступа пользователей

Разграничение (контроль) доступа к ресурсам АС – это такой порядок использования ресурсов автоматизированной системы, при котором *субъекты* получают доступ к *объектам* системы в строгом соответствии с установленными правилами.

Объект – это пассивный компонент системы, единица ресурса автоматизированной системы (устройство, диск, каталог, файл и т.п.), доступ к которому регламентируется правилами разграничения доступа.

Субъект – это активный компонент системы (пользователь, процесс, программа), действия которого регламентируются правилами разграничения доступа.

Концепция единого диспетчера доступа

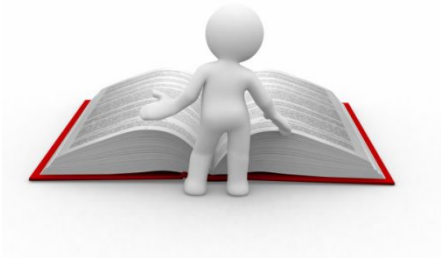
Правила разграничения доступа

Субъект доступа

ДИСПЕТЧЕР ДОСТУПА

Объект доступа

Журнал регистрации



Функции диспетчера

Диспетчер доступа выполняет следующие основные функции:

• проверяет права доступа каждого субъекта к конкретному объекту на основании информации, содержащейся в базе данных системы защиты (правил разграничения доступа);

• разрешает (производит авторизацию) или запрещает (блокирует) доступ субъекта к объекту;

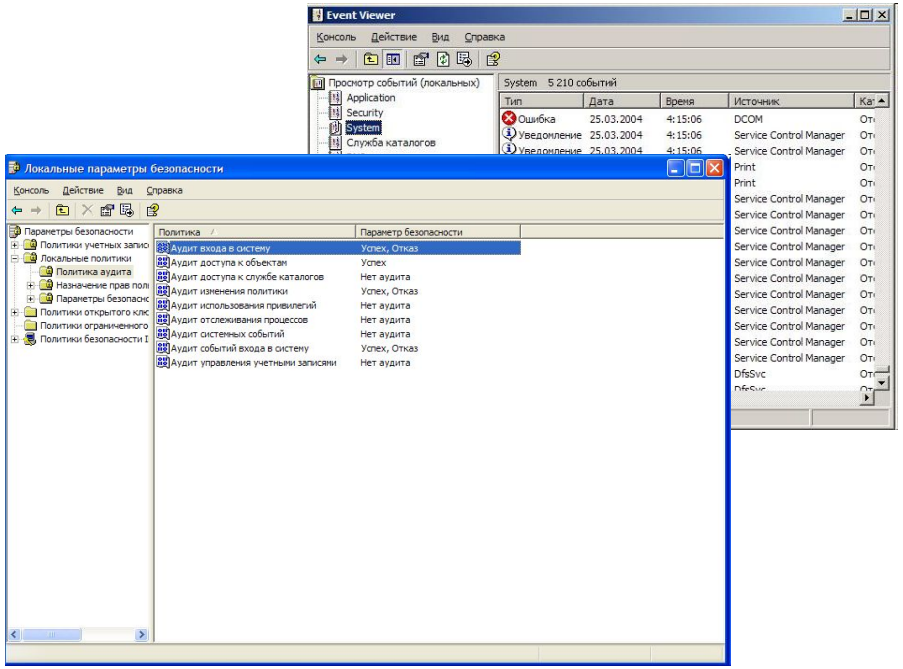
• при необходимости регистрирует факт доступа и его параметры в системном журнале (в том числе попытки несанкционированного доступа с превышением полномочий).

3. Регистрация и оперативное оповещение о событиях безопасности

Регистрация и оперативное оповещение о событиях безопасности

Механизмы регистрации предназначены для получения и накопления (с целью последующего анализа) информации ***о состоянии ресурсов*** системы и ***о действиях субъектов***, признанных администрацией АС потенциально опасными для системы.

Анализ собранной средствами регистрации информации позволяет выявить ***факты совершения*** нарушений, ***характер воздействий*** на систему, определить, ***как далеко зашло нарушение***, подсказать ***метод его расследования*** и ***способы поиска*** нарушителя и исправления ситуации.



Лаборатория Информационной Безопасности

Регистрация и оперативное оповещение о событиях безопасности

При регистрации событий безопасности в системном журнале обычно **фиксируется следующая информация**:

• дата и время события;

• идентификатор субъекта (пользователя, программы), осуществляющего регистрируемое действие;

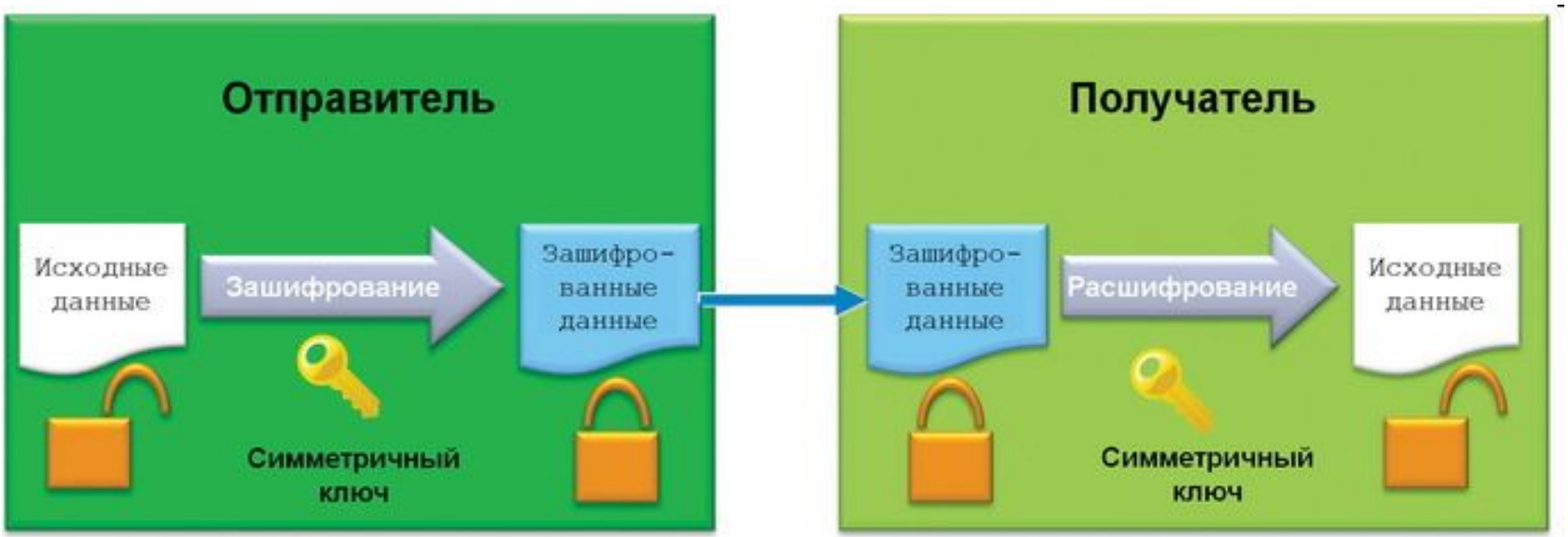
• действие (если регистрируется запрос на доступ, то отмечается объект и тип доступа).

4. Криптографические методы защиты информации

Криптографические методы защиты основаны на возможности осуществления некоторой операции преобразования информации, которая может выполняться одним или несколькими пользователями АС, обладающими некоторым секретом, без знания которого (с вероятностью близкой к единице за разумное время) невозможно осуществить эту операцию.

Криптография с симметричными ключами

В криптографии с симметричным ключом оба участника обмена имеют один и тот же ключ, называемый «секретным» (или закрытым), который используется как для зашифровывания, так и для расшифровывания сообщений



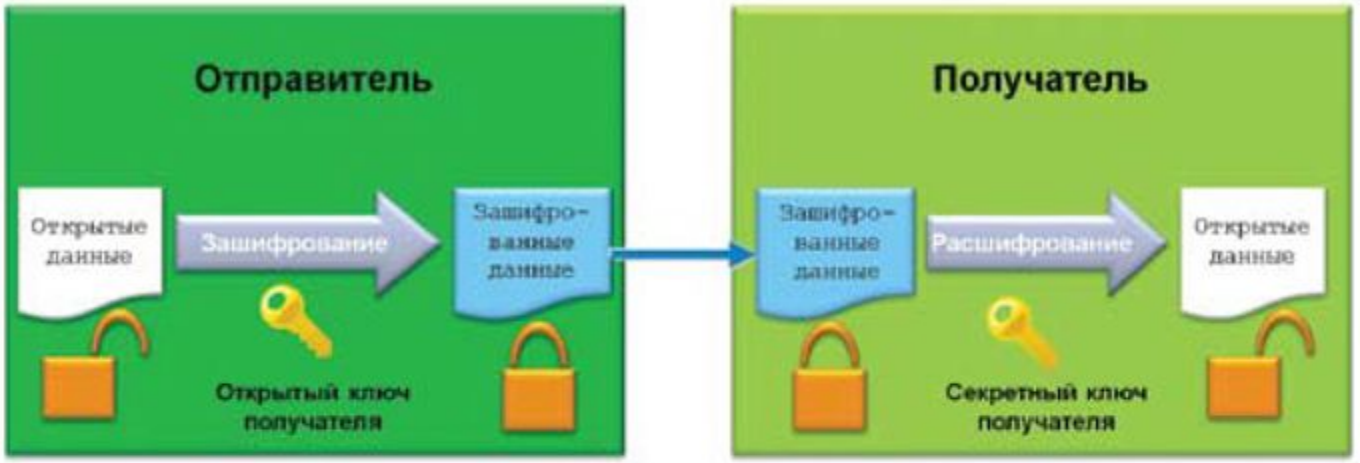
Этот закрытый ключ необходимо держать в секрете, чтобы предотвратить возможность расшифровать и прочитать передаваемые сообщения со стороны третьих лиц (называемых нарушителями).

Термин **«симметричный»** применяется постольку, поскольку пользователи на обеих сторонах канала обмена данными используют один и тот же ключ.

Симметричный ключ также называется парным, поскольку служит для шифрования сообщений, передаваемых между двумя пользователями.

Основной проблемой в этой схеме является защищенная передача секретного ключа. Канал, с помощью которого осуществляется такая передача, называется доверенным каналом.

Криптография с ассиметричными ключами



а)

б)

Криптография с ассиметричными ключами

Криптография с асимметричным ключом использует пару ключей, находящихся в такой математической зависимости, что информацию, зашифрованную одним ключом, можно расшифровать только другим ключом.

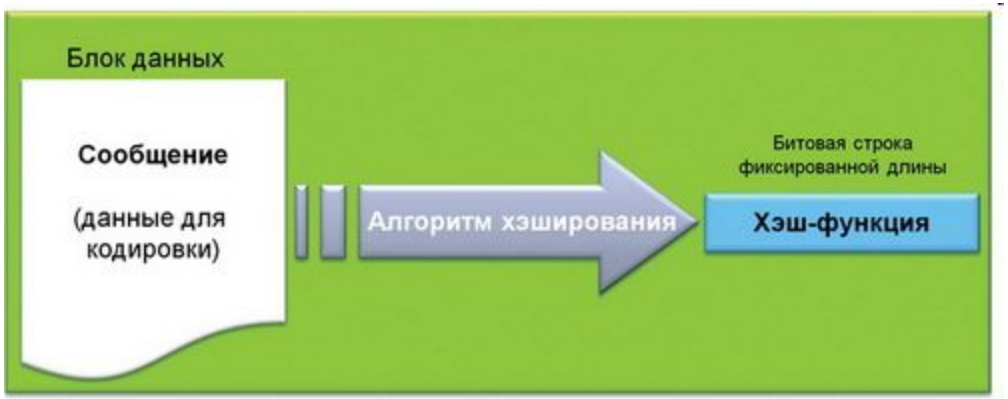
Один из этих ключей называется **открытым или публичным**, а второй - **закрытым или секретным**. Оба ключа создаются одновременно по особому алгоритму, который гарантирует, что по одному ключу крайне трудно получить другой ключ.

Секретность шифрования обеспечивается исключительно надежностью хранения закрытого ключа, которая может быть обеспечена относительно простыми способами. Открытый же ключ может распространяться свободно.

Зашифрованное открытым ключом сообщение передается по открытому каналу владельцу секретного ключа. Только пользователь закрытого ключа, созданного в паре с открытым, которым было зашифровано сообщение, сможет его прочитать.

Функция хэширования (hash function)

Одним из типов криптографических алгоритмов, использующихся в асимметричной криптографии, являются функции хэширования или хэш-функции. Функция хеширования применяется к данным для получения последовательности битов фиксированной длины, уникальной для каждого сообщения, или блока данных - значения хэша (hash value).



Хэширование используется для формирования электронной цифровой подписи, обеспечения целостности данных, невозможности отказа от авторства, аутентификации сообщений и других видов аутентификации.

5. Контроль целостности программных и информационных ресурсов

Контроль целостности программных и информационных ресурсов

Механизм контроля целостности ресурсов системы предназначен для своевременного обнаружения модификации ресурсов системы. Он позволяет обеспечить правильность функционирования системы защиты и целостность обрабатываемой информации.

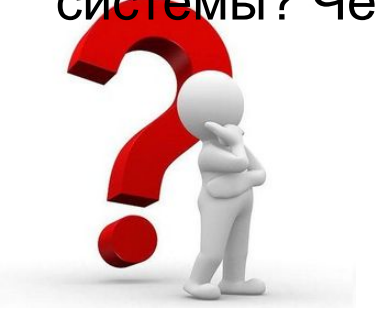
Контроль целостности программ, обрабатываемой информации и средств защиты, **должен обеспечиваться**:

- средствами разграничения доступа, запрещающими модификацию или удаление защищаемого ресурса;
- средствами сравнения критичных ресурсов с их эталонными копиями (и восстановления в случае нарушения целостности);
- средствами подсчета контрольных сумм (сигнатур, имитовставок и т.п.);
- средствами электронной цифровой подписи.

Контрольные вопросы

Контрольные вопросы:

1. Назовите механизмы защиты информационных систем.
2. Что такое идентификация и аутентификация?
3. Раскройте смысл механизма защиты «Разграничение доступа пользователя». В чем заключается концепция единого диспетчера доступа?
4. Раскройте смысл механизма защиты «Регистрация и оперативное оповещение о событиях безопасности».
5. На чем основаны криптографические методы защиты?
6. Раскройте сущность метода криптографии с симметричными ключами.
7. Раскройте сущность метода криптографии с ассимметричными ключами.
8. Что такое функция хэширования?
9. Для чего предназначен механизм контроля целостности ресурсов системы? Чем обеспечивается контроль целостности программ?



Лаборатория Информационной Безопасности

Спасибо за внимание!

Лаборатория Информационной Безопасности