

*Безопасность интернет проекта.
Основные угрозы сети*



Цель урока

- Узнать об основных видах угроз сети
- Узнать какие способы защиты угроз сети

Ключевые слова

- *Биометрические системы защиты*
 - *Проактивная защита*

Сайты сегодня – набор запчастей

Большая часть современных сайтов - набор запчастей.

- **низкий уровень стандартной разработки**
- **отсутствие единой концепции безопасности**
- **несколько аккаунтов для одного пользователя**
- **не обновляемое ПО, особенно после модификации**



Разработчики интернет-приложений зачастую не задумываются о безопасности.



Каждый год в мире потери от преднамеренного нанесения вреда ИТ системам компании теряют огромные средства.

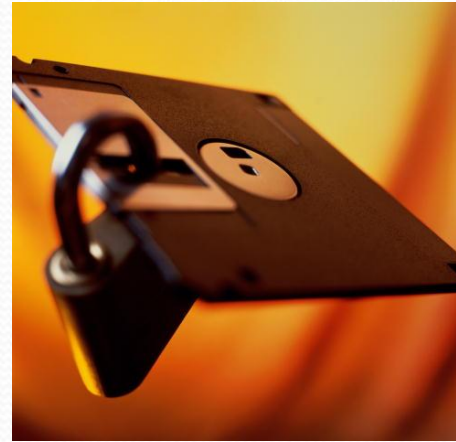
В результате компании непрерывного цикла могут пострадать вплоть до банкротства.

Виды защиты

- *Защита с использованием паролей*
- *Биометрические системы защиты*
 - *Проактивная защита*

Защита с использованием паролей

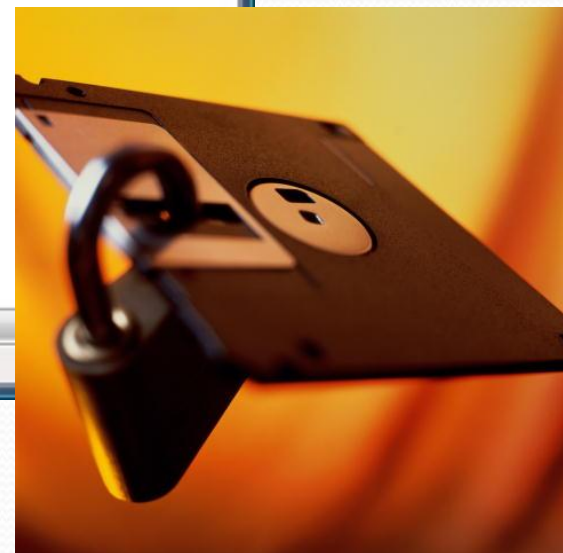
- Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются **пароли**.
- Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели **правильный пароль**.
- При этом может производиться регистрация всех попыток несанкционированного доступа.



● Защита с использованием пароля используется при загрузке операционной системы (при загрузке системы каждый пользователь должен ввести свой пароль)



От несанкционированного доступа может быть защищен каждый диск, папка или файл локального компьютера. Для них могут быть установлены определенные права доступа (полный доступ, изменение, чтение, запись и др.)



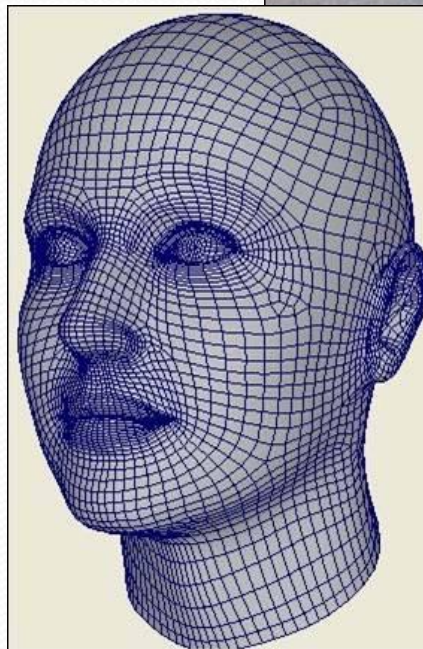
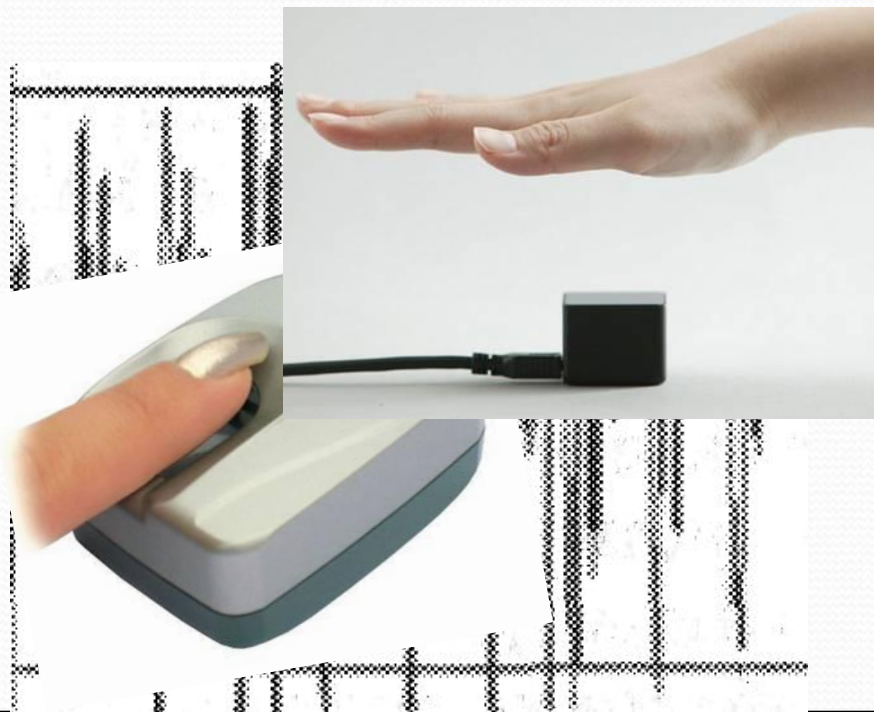
Биометрические системы защиты

- В настоящее время часто используются биометрические системы идентификации.
- Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утраченными и подделанными.



К биометрическим системам защиты информации относятся системы идентификации:

- по отпечаткам пальцев;
- по характеристикам речи;
- по радужной оболочке глаза;
- по изображению лица;
- по геометрии ладони руки.



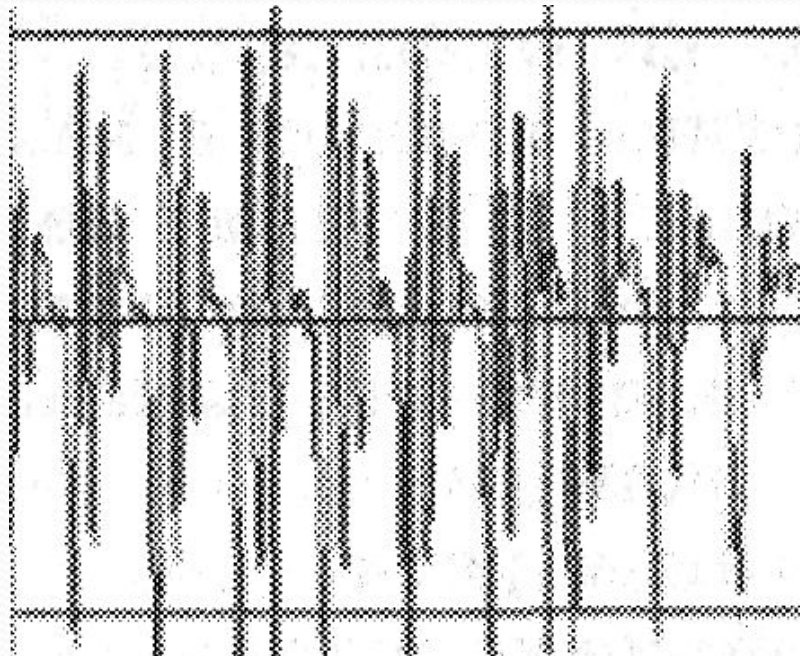
Идентификация по отпечаткам пальцев.

- Оптические сканеры считывания отпечатков пальцев устанавливаются на ноутбуки, мыши, клавиатуры, флэш-диски, а также применяются в виде отдельных внешних устройств и терминалов (например, в аэропортах и банках)
- Если узор отпечатка пальца не совпадает с узором допущенного к информации пользователя, то доступ к информации невозможен.



Идентификация по характеристикам речи.

- Идентификация человека по голосу — один из традиционных способов распознавания. Голосовая идентификация бесконтактна и существуют системы ограничения доступа к информации на основании частотного анализа речи



Идентификация по радужной оболочке глаза.

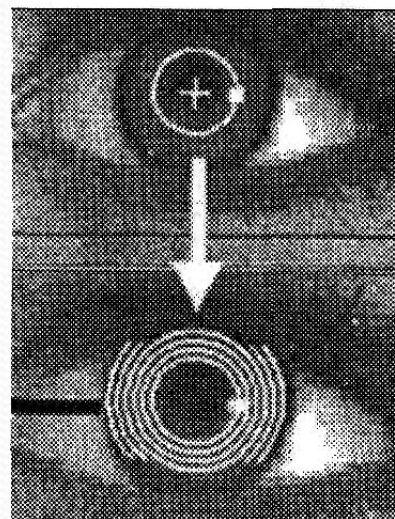
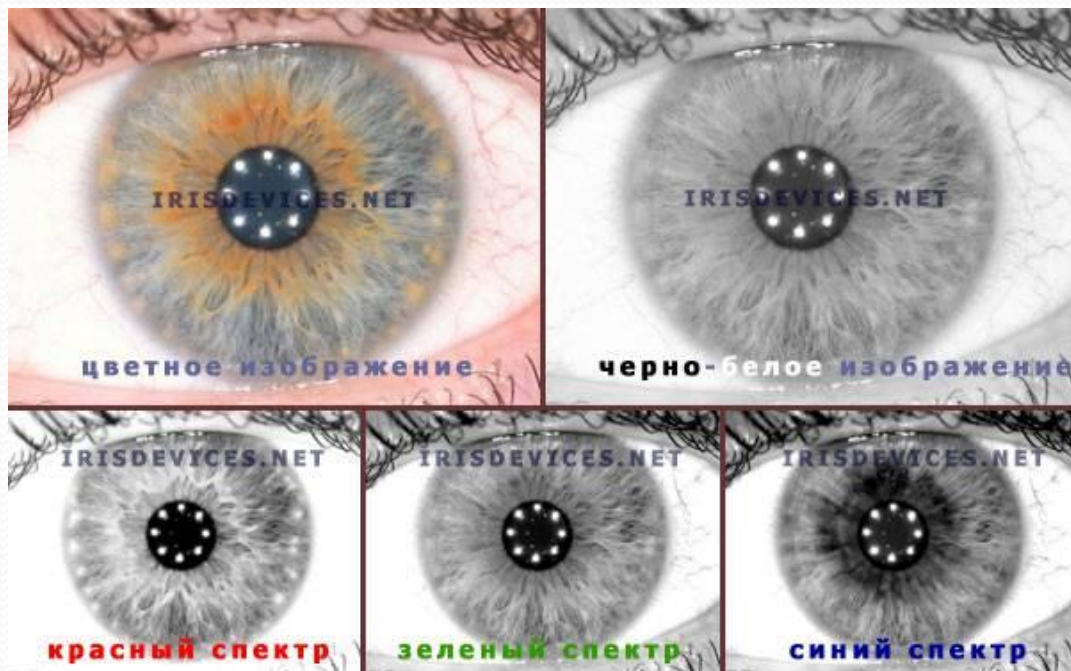
- Радужная оболочка глаза является уникальной для каждого человека биометрической характеристикой.
- Она формируется в первые полтора года жизни и остается практически неизменной в течение всей жизни.



Идентификация по радужной оболочке глаза.

- Изображение глаза выделяется из изображения лица и на него накладывается специальная маска штрих-кодов.

- Результатом является матрица, индивидуальная для каждого человека



Идентификация по изображению лица.

- Для идентификации личности часто используется технологии распознавания по лицу.
- Они ненавязчивы, так как распознавание человека происходит на расстоянии, без задержек и отвлечения внимания и не ограничивают пользователя в свободе перемещений.
- В настоящее время идет выдача новых загранпаспортов, в микросхеме которых хранится цифровая фотография владельца.



Идентификация по ладони руки.

В биометрике в целях идентификации используется простая геометрия руки — размеры и форма, а также некоторые информационные знаки на тыльной стороне руки.

(образы на сгибах между фалангами пальцев, узоры расположения кровеносных сосудов).

Сканеры идентификации по ладони руки установлены в некоторых аэропортах, банках и на атомных электростанциях



Закрепление материала:

- Как защищается информация в компьютере с использованием паролей?
- Какие существуют биометрические методы защиты информации?

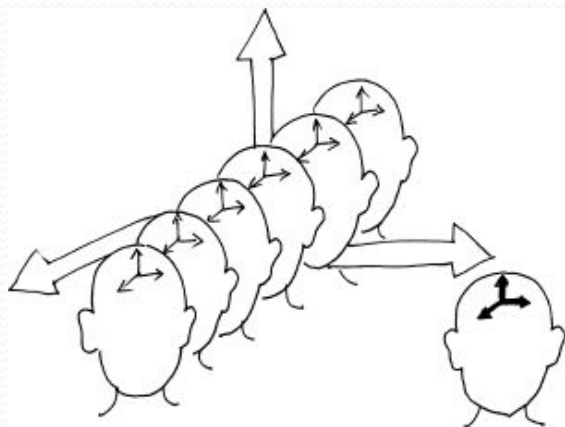


О безопасности сайта думают в последнюю очередь!

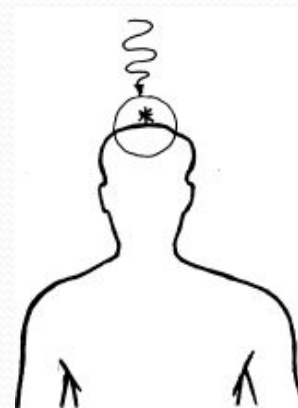
- индивидуальные разработчики думают о безопасности сайтов в самую последнюю очередь
- клиенты не готовы платить за безопасность интернет-проектов
- подразумевается, что разработчик должен этим заниматься, но у него не остается ни времени, ни бюджета

Психология хакера и разработчика

Психология хакера и разработчика принципиально отличаются:



*Как мыслит
разработчик...*



*... и как мыслит
хакер*

Ошибки бывают у всех, даже у профессиональных разработчиков.

Хостинг часто не защищен

- зачастую уровень администрирования серверов и хостинга *критически низкий*
- редко используются системы автоматического мониторинга



Категории хакеров

Студенты, ИТ специалисты начального уровня



- пробуют силы на первых попавшихся сайтах
- нет понимания последствий для жертвы
- нет осознания юридической личной ответственности
- редко зарабатывают на хакерстве как на бизнесе

Профессиональные специалисты



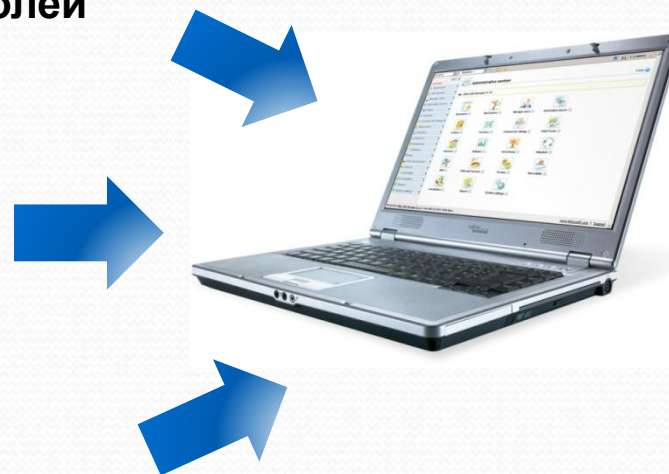
- прекрасный технический багаж
- никогда не светятся в тусовках, не кривляются
- делают только на заказ и только за деньги
- активно работают на службы безопасности крупных компаний

Обычный студент может пользоваться самыми банальными методами.

Комплекс проактивной защиты сайта

Проактивная защита – это комплекс технических и организационных мер, которые объединены общей концепцией безопасности и позволяют значительно расширить понятие защищенности и реакции веб-приложения на угрозы.

- Аутентификация и система составных паролей
- Технология защиты сессии пользователя
- Проактивный фильтр защиты от атак
- Активная реакция на вторжение
- Контроль целостности системы
- Защита от фишинга
- Шифрование данных



Web Application Fire Wall

Основан на анализе и фильтрации всех данных, поступающих от пользователей через переменные и куки.

- XSS - cross site scripting (CSS)
 - SQL инъекции
 - часть атак, связанных с обходом каталогов (в том числе PHP source code injection)
-
- Экранирует приложение от наиболее активно используемых атак
 - Фиксирует попытки атаки в журнале
 - Информировывает администратора о случаях вторжения



Способы взлома веб-приложений

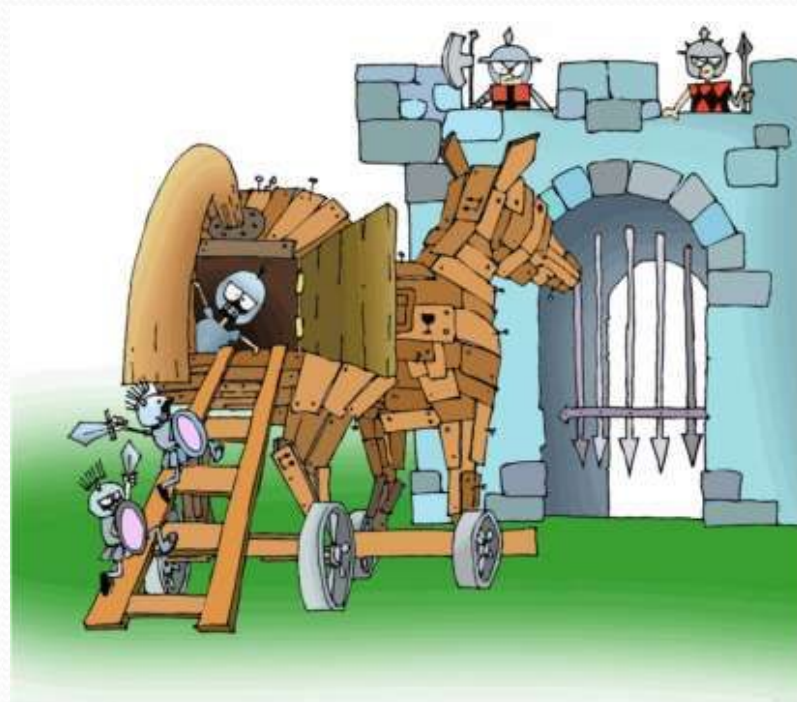
Атаки непосредственно на веб-приложения:

- SQL инъекция
- Внедрение в имя файла
- Внедрение в system и т.п.
- Подбор реквизитов доступа
- Логические ошибки

Атаки на клиентов веб-приложения:

- XSS
- CSRF
- Социальная инженерия
- Фишинг

Обычные ДОС атаки, ДДОС атаки



Сайты – основной способ распространения вирусов

Способы распространения вирусов через веб:

iframe и JavaScript

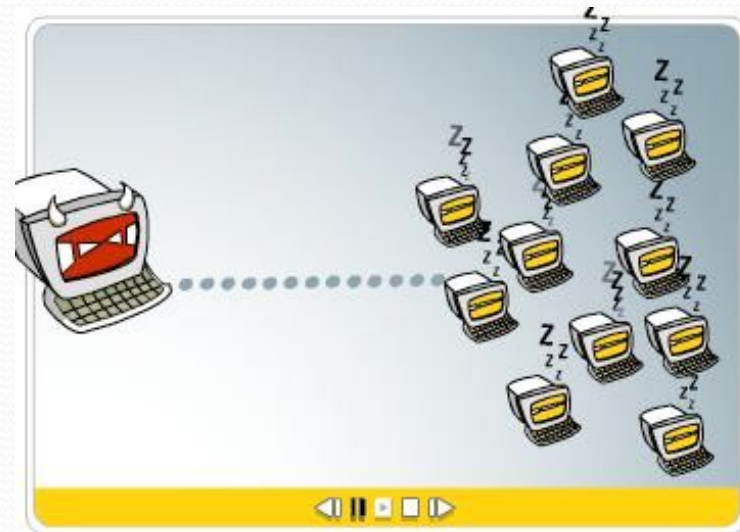
На самом деле, способ даже один, так как все JavaScript, как правило в конце концов «рисуют» iframe.



Бот-сети и трояны

Ботнет (бот-сеть) — это некоторое количество компьютеров (100 - 100000 >) - ботов - подключенных к сети интернет, и подчиняющихся командам центра управления.

Бот (или компьютер-зомби) — это компьютер, на котором установлено вредоносное программное обеспечение — троян, имеющий функционал БОТ-клиента.



Строго говоря, троян может быть и просто «трояном», не делающим компьютер частью зомби сети. Тем не менее, и способы заражения и опасность от заражения обычных троянов, и троянов-бот-клиентов совершенно одинаковые.

Варианты установки троянов на компьютер

- уязвимости в системном ПО
- через веб-сайты
- запуск исполняемого файла с вирусом
- санкционированный доступ к компьютеру (крайне редко)
- подбор слабого административного пароля (редко)
- ручной взлом



Механизмы защиты от троянов

- регулярно обновлять системное ПО
- регулярно обновлять все прикладное ПО
- с подозрением относиться ко всем исполняемым файлам
- не предоставлять никому доступа к компьютеру
- использовать сложные пароли для все аккаунтов удаленного доступа
- уделять внимание защите всех компонентов системы

Веб-антивирус

В платформу «1С-Битрикс» встроена система противодействия заражениям сайтов, которая:

- выявляет в html-коде потенциально опасные участки
- определяет 90% заражений сайта
- «белый список» для отсеечения ложно положительных срабатываний



Веб-антивирус ни в коем случае не является заменой персонального антивируса!

Аутентификация и система одноразовых паролей OTP

Надежная аутентификация пользователя с использованием одноразовых паролей (OTP)

Система одноразовых паролей дополняет стандартную систему авторизации и позволяет значительно усилить систему безопасности интернет-проекта.

При авторизации на сайте пользователь в дополнение к паролю дописывает одноразовый пароль.

eToken
YOUR KEY TO SECURITY



Инструменты безопасности в «1С-Битрикс»

- Аутентификация и система составных паролей
- Технология защиты сессии пользователя
- Проактивный фильтр защиты от атак
- Активная реакция на вторжение
- Контроль целостности системы
- Защита от фишинга
- Шифрование данных
- Групповые политики безопасности
- Защита при регистрации и авторизации
- Журнал событий
- Веб-антивирус





ДОМАШНЕЕ ЗАДАНИЕ



- Технология сети Ethernet.
- Возникновение коллизии.

- Инкапсуляция
- Деинкапсуляция

- <http://ru.wikibooks.org/>
- <http://ppt4web.ru/search.html>