Операционные системы: безопасность

Основы безопасности

Безопасность в целом

- Безопасность - состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

- Жизненно важные интересы - совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

- К основным объектам безопасности относятся: личность - ее права и свободы; общество - его материальные и духовные ценности; государство - его конституционный строй, суверенитет и территориальная целостность.

* Закон РФ от 5 марта 1992 г. N 2446-I "О безопасности", статья 1

Безопасность в ИТ

Безопасность – одна из наиболее актуальных проблем в области ИТ в настоящее время, ввиду сильной зависимости повседневной деятельности и бизнеса от компьютерных технологий и ввиду резко возрастающего числа сетевых атак (киберпреступности). Особенно важна безопасность для операционных систем и сетей как основных объектов атак.

Угрозы безопасности ОС

- Угрозы безопасности ОС существенно зависят от условий эксплуатации системы, от того, какая информация хранится и обрабатывается в системе, и т. д. Например, если ОС используется для организации электронного документооборота, наиболее опасны угрозы, связанные с несанкционированным доступом (НСД) к файлам. Если же ОС используется как платформа провайдера Internet-услуг, очень опасны атаки на сетевое программное обеспечение ОС.

Классификация угроз безопасности ОС по цели атаки

- несанкционированное чтение информации;
- несанкционированное изменение информации;
- несанкционированное уничтожение информации;
- полное или частичное разрушение ОС.

Классификация угроз безопасности ОС по принципу воздействия на операционную систему

- использование известных (легальных) каналов получения информации; например угроза несанкционированного чтения файла, доступ пользователей к которому определен некорректно, т. е. разрешен доступ пользователю, которому согласно политике безопасности доступ должен быть запрещен;
- использование скрытых каналов получения информации; например угроза использования злоумышленником недокументированных возможностей ОС;
- создание новых каналов получения информации с помощью программных закладок.

Классификация угроз безопасности ОС по типу используемой злоумышленником уязвимости защиты

- неадекватная политика безопасности, в том числе и ошибки администратора системы;
- ошибки и недокументированные возможности программного обеспечения ОС, в том числе и так называемые люки - случайно или преднамеренно встроенные в систему «служебные входы», позволяющие обходить систему защиты;
- ранее внедренная программная закладка.

Задачи безопасности

- Конфиденциальность данных
- Целостность данных
- Работоспособность системы
- Исключение постороннего доступа

Конфиденциальность данных (data confidentiality)

- **Задача направлена на сохранение секретности соответствующих данных.**
- Данные должны быть доступны лишь определенному кругу лиц. Система должна гарантировать невозможность допуска к данным лиц, не имеющих на это права. Как минимум, владелец должен иметь возможность определить, кто и что может просматривать, а система должна обеспечить выполнение этих требований, касающихся в идеале отдельных файлов.

Целостность данных (data integrity)

- **Задача означает, что пользователи, не обладающие соответствующими правами, не должны иметь возможности изменять какие-либо данные без разрешения их владельцев.**
- В этом случае изменение данных включает в себя не только внесение в них изменений, но и их удаление или добавление ложных данных. Если система не может гарантировать, что заложенные в нее данные не будут подвергаться изменениям, пока владелец не решит их изменить, то она потеряет свою роль информационной системы.

Работоспособность системы (system availability)

- **Задача означает, что никто не может нарушить работу системы и вывести ее из строя.**
- Атаки, вызывающие отказ от обслуживания (denial of service, DOS), приобретают все более распространенный характер.

Исключение постороннего доступа

- Посторонние лица могут иногда взять на себя управление чьими-нибудь домашними компьютерами (используя вирусы и другие средства) и превратить их в **зомби (zombies)**, моментально выполняющих приказания посторонних лиц.
- Часто зомби используются для рассылки спама, поэтому истинный инициатор спам-атаки не может быть отслежен.

Задачи и угрозы безопасности

Задачи	Угрозы
Конфиденциальность данных	Незащищенность данных
Целостность данных	Подделка данных
Работоспособность системы	Отказ от обслуживания
Исключение постороннего доступа	Переход системы под управление вирусами

Злоумышленники

- **Злоумышленник** - субъект, оказывающий на информационный процесс воздействия с целью вызвать его отклонение от условий нормального протекания.
- Злоумышленники действуют двумя различными способами. Пассивным злоумышленникам нужно лишь прочитать файлы, к которым у них нет прав доступа. Активные злоумышленники хотят внести в данные несанкционированные изменения.
- При разработке системы, защищенной от злоумышленников, важно понимать, от какой разновидности злоумышленников создается защита.

Категории злоумышленников (1)

- **Праздное любопытство пользователей**, не имеющих специального технического оснащения.
- У многих людей на столе стоит персональный компьютер, подключенный к серверу с файлами общего пользования, и в соответствии с человеческой натурой, кое-кто из них, не имея препятствий на своем пути, станет читать чужую электронную почту и другие файлы.

Категории злоумышленников (2)

- **Шпионаж внутри коллектива**. Студенты, системные программисты, операторы и другие представители технического персонала зачастую испытывают личную потребность во взломе системы безопасности локальных компьютерных систем.
- Они, как правило, имеют высокую квалификацию и не жалеют времени на подобные проделки.

Категории злоумышленников (3)

- **Вполне определенные попытки обогатиться**. Некоторые банковские программисты пытались обокрасть свой банк. Схемы их действий варьировались от изменения программного обеспечения для получения прибыли за счет округления сумм в меньшую сторону и присвоении долей копеек, выкачивания средств со счетов, не используемых годами, и до вымогательства («Заплатите, или я испорчу весь банковский учет»).

Категории злоумышленников (4)

- **Коммерческий или военный шпионаж.** Шпионаж относится к серьезной и хорошо проплачиваемой попытке, предпринимаемой конкурентом или другой страной, совершить кражу программ, производственных секретов, идей, имеющих патентную ценность, технологий, схемных решений, бизнес планов и т. д. Зачастую эти попытки будут включать перехват сообщений или даже установку антенн, направленных на компьютер для приема его электромагнитного излучения и т.п.

Вирусы, как угроза для ПО

- **Компьютерный вирус** — это специальная программа, способная самопроизвольно присоединяться к другим программам и при запуске последних выполнять различные нежелательные действия: порчу файлов и каталогов; искажение результатов вычислений; засорение или стирание памяти; создание помех в работе компьютера. Наличие вирусов проявляется в разных ситуациях.
- Некоторые программы перестают работать или начинают работать некорректно.
- На экран выводятся посторонние сообщения, сигналы и другие эффекты.
- Работа компьютера существенно замедляется.
- Структура некоторых файлов оказывается испорченной.

* Использовано изображение с сайта:

Случайная утрата данных

Кроме угроз, исходящих от злоумышленников, ценным данным угрожает также и случайная утрата. К наиболее частым причинам относятся следующие:

1. Форс-мажорные обстоятельства: пожары, наводнения, землетрясения, войны, массовые беспорядки или «крысы, прогрызшие ленты с резервными копиями».
2. Ошибки в аппаратном или программном обеспечении: сбои центрального процессора, нечитаемые диски или ленты, ошибки передачи данных, ошибки в программах.
3. Человеческие ошибки: ввод неправильных данных, неправильная носителя, запуск не той программы, утрата носителя и некоторые другие ошибки.

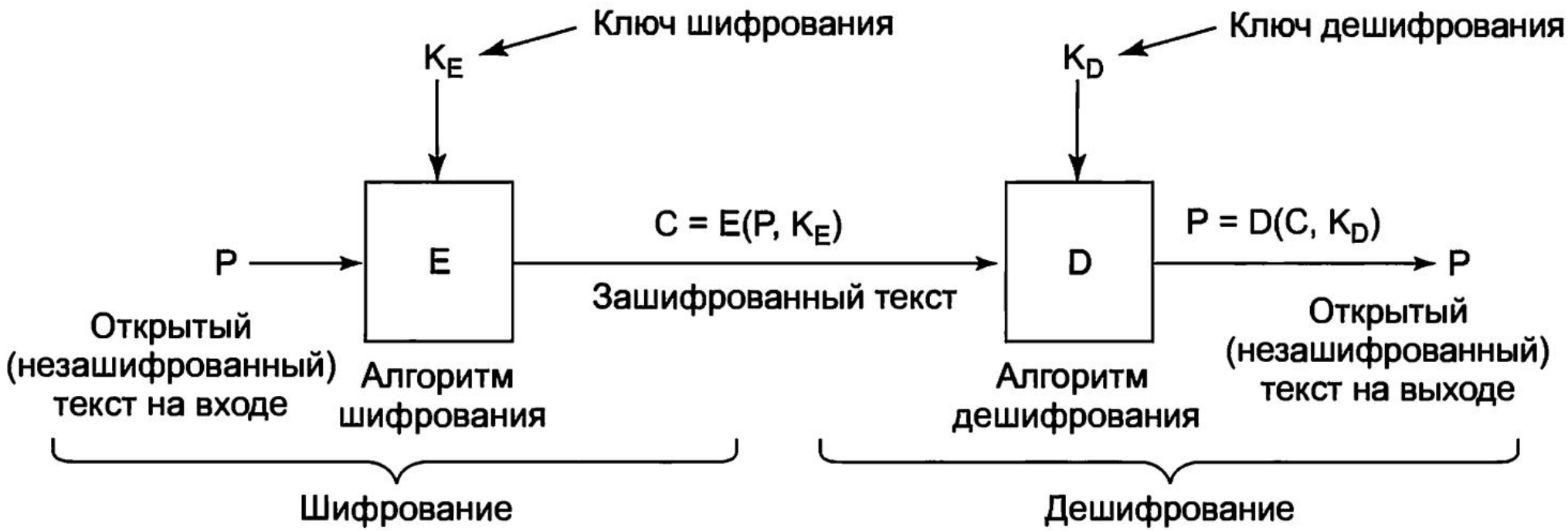
Защита данных с помощью криптографии

- Криптография в переводе с греческого означает "тайнопись". В настоящее время криптография занимается поиском и исследованием математических методов преобразования информации.
- Замысел криптографии заключается в том, чтобы закодировать открытый текст (plaintext) — сообщение или файл, превратив его в зашифрованный текст (ciphertext), чтобы о том, как его снова превратить в открытый текст, знали только те, кто имеет на это право. Для всех остальных зашифрованный текст будет лишь непонятным набором битов.
- Как бы странно это ни звучало, но алгоритмы (функции), используемые для шифрования и дешифрования, должны всегда быть открытыми. Попытка хранить их в секрете практически никогда не срабатывает и создает у людей, пытающихся сохранить секреты, ложное чувство безопасности. В коммерции такая тактика называется безопасностью за счет неизвестности (security by obscurity) и используется только дилетантами.

Задачи криптографии

- До начала XX века криптографические методы применялись лишь для шифрования данных с целью защиты от несанкционированного доступа. В двадцатом веке в связи с развитием техники передачи информации на дальние расстояния интерес к криптографии значительно возрос. Благодаря созданию новых криптографических методов расширился и спектр задач криптографии.
- В настоящее время считается, что криптография предназначена решать следующие задачи:
  - собственно шифрование данных с целью защиты от несанкционированного доступа;
  - проверка подлинности сообщений: получатель сообщения может проверить его источник;
  - проверка целостности передаваемых данных: получатель может проверить, не было ли сообщение изменено или подменено в процессе пересылки;
  - обеспечение невозможности отказа, то есть невозможности как для получателя, так и для отправителя отказаться от факта передачи.

Взаимоотношения между открытым и зашифрованным текстом



Шифрование

- Существует два основных типа шифрования: с секретным ключом и с открытым ключом. При шифровании с секретным ключом требуется, чтобы все стороны, имеющие право на прочтение информации, имели один и тот же ключ. Это позволяет свести общую проблему безопасности информации к проблеме обеспечения защиты ключа. Шифрование с открытым ключом является наиболее широко используемым методом шифрования. Он обеспечивает конфиденциальность информации и гарантию того, что информация остается неизменной в процессе передачи.

Шифрование с секретным ключом

- Шифрование на секретном ключе также называется симметричным шифрованием, так как для шифрования и дешифрования данных используется один и тот же ключ.
- Шифрование с секретным ключом обеспечивает конфиденциальность информации в зашифрованном состоянии. Расшифровать сообщение могут только те лица, которым известен ключ. Любое изменение в сообщении, внесенное во время передачи, будет обнаружено, так как после этого не удастся правильно расшифровать сообщение. Шифрование с секретным ключом не обеспечивает аутентификацию, поскольку любой пользователь может создавать, шифровать и отправлять действительное сообщение.
- В общем, шифрование с секретным ключом быстро и легко реализуется с помощью аппаратных или программных средств.

Шифрование с открытым ключом

- Чтобы получить начальное представление о шифровании с открытым ключом, рассмотрим следующие два вопроса:
- Вопрос 1: Сколько будет 314159265358979 x 314159265358979?
- Вопрос 2: Чему равен корень квадратный из 3912571506419387090594828508241?
- Способ работы шифрования с открытым ключом заключается в том, что все получают пару (открытый ключ, закрытый ключ), а открытый ключ публикуется. Открытый ключ является ключом шифрования, а закрытый — ключом дешифрования. Обычно генерация ключей происходит в автоматическом режиме, возможно, с использованием выбранного пользователем пароля в качестве передаваемого алгоритму начального числа. Для отправки пользователю секретного сообщения корреспондент зашифровывает текст этого сообщения открытым ключом получателя. Поскольку закрытый ключ есть только у получателя, только он в состоянии расшифровать сообщение.

Хеш-функции

- Криптографическая хеш-функция (хеш) - это математический алгоритм, преобразовывающий произвольный массив данных в состоящую из букв и цифр строку фиксированной длины.

Основные принципы хеширования:

- при хешировании одинаковых данных получается одинаковое значение хеша (хеш-кода);
- разные данные преобразуются в разные хеш-коды (хеш-суммы);
- криптостойкость хеш-функции заключается в стойкости к восстановлению хешируемых данных и стойкости к коллизиям преобразования.

Цифровые подписи

- Электронно-цифровая подпись (ЭЦП) - это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе

Криптографический процессор

- Для всех систем шифрования необходимы ключи. Если ключи скомпрометированы, то скомпрометирована и вся основанная на их использовании система безопасности.
- Одним из предложений промышленности стала микросхема под названием модуль надежной платформы (Trusted Platform Module (TPM)), представляющая собой криптографический процессор, имеющий в своем составе энергонезависимую память для хранения ключей. TPM способен выполнять такие криптографические операции, как шифрование блоков открытого текста или дешифрование блоков зашифрованного текста в оперативной памяти. Также он может проверять цифровые подписи. За счет выполнения всех этих операций специализированной аппаратурой существенно повышаются скорость работы и вероятность их более широкого применения.

Физическая защита материального носителя информации от противника

- В качестве носителя данных может выступать бумага, компьютерный носитель (DVD-диск, флэш-карта, магнитный диск, жесткий диск компьютера и т.д.). Для реализации этого способа необходим надежный канал связи, недоступный для перехвата. В различное время для этого использовались почтовые голуби, специальные курьеры, радиопередачи на секретной частоте. Методы физической защиты информации используются и в современных автоматизированных системах обработки данных. Так, например, комплексные системы защиты информации невозможны без систем ограждения и физической изоляции, а также без охранных систем.

Стенографическая защита информации

- Этот способ защиты основан на попытке скрыть от противника сам факт наличия интересующей его информации. При стенографическом методе защиты от противника прячут физический носитель данных или маскируют секретные сообщения среди открытой, несекретной информации.

Идентификация и аутентификация, управление доступом

- Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов.
- Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова " аутентификация " иногда используют словосочетание "проверка подлинности".

Парольная аутентификация

- Главное достоинство парольной аутентификации – простота и привычность. Пароли давно встроены в операционные системы и иные сервисы. При правильном использовании пароли могут обеспечить приемлемый для многих организаций уровень безопасности. Тем не менее, по совокупности характеристик их следует признать самым слабым средством проверки подлинности.

Повышение надежности паролей:

- наложение технических ограничений (пароль должен быть не слишком коротким, он должен содержать буквы, цифры, знаки пунктуации и т.п.);
- управление сроком действия паролей, их периодическая смена;
- ограничение доступа к файлу паролей;
- ограничение числа неудачных попыток входа в систему (это затруднит применение "метода грубой силы");
- обучение пользователей;
- использование программных генераторов паролей (такая программа, основываясь на несложных правилах, может порождать только благозвучные и, следовательно, запоминающиеся пароли).

Перечисленные меры целесообразно применять всегда, даже если наряду с паролями используются другие методы аутентификации.

Аутентификация с использованием паролей

- ОС ведет реестр пар: имя пользователя : пароль

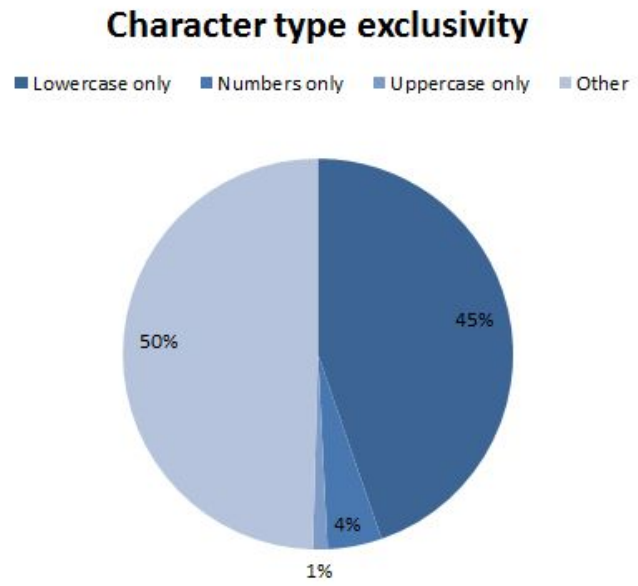
LOGIN: math **PASSWORD: Brain!-34!@** **Успешно!**	**LOGIN: MATH** **INVALID LOGIN NAME** **LOGIN:**	**LOGIN: MATH** **PASSWORD: SGD45gg)** **INVALID LOGIN NAME** **LOGIN:**

Обойти парольную защиту можно загрузившись в BIOS (UEFI), и из него загрузиться с загрузочного носителя.

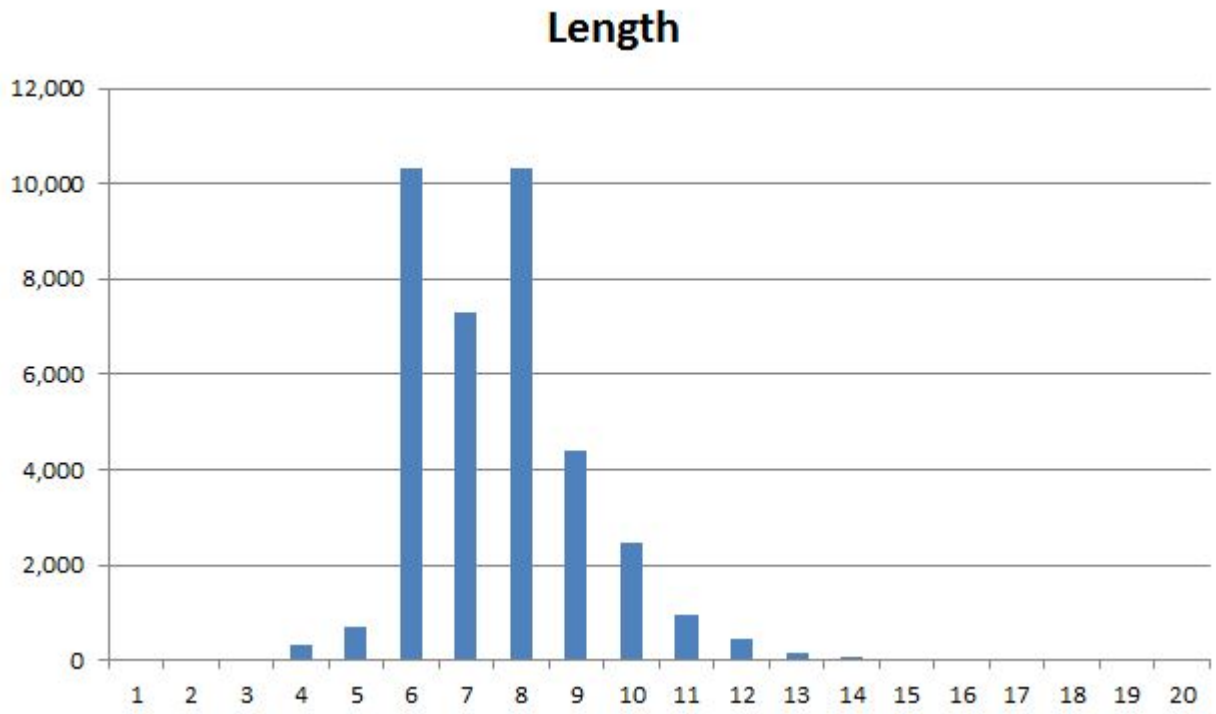
Как взломщикам удается проникнуть в систему?

Подбор имени, пароля:

- Полный перебор



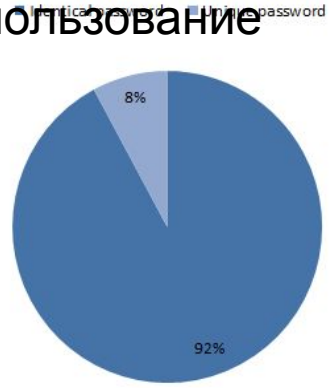
Используемые символы



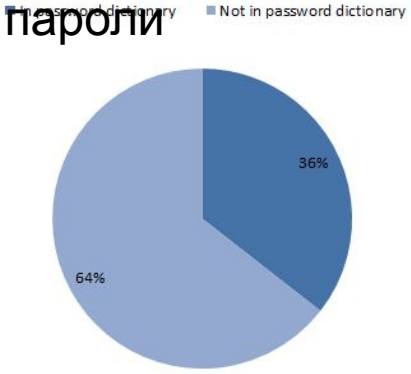
Статистика паролей пользователей Sony Pictures, 2011

Уникальные пароли…

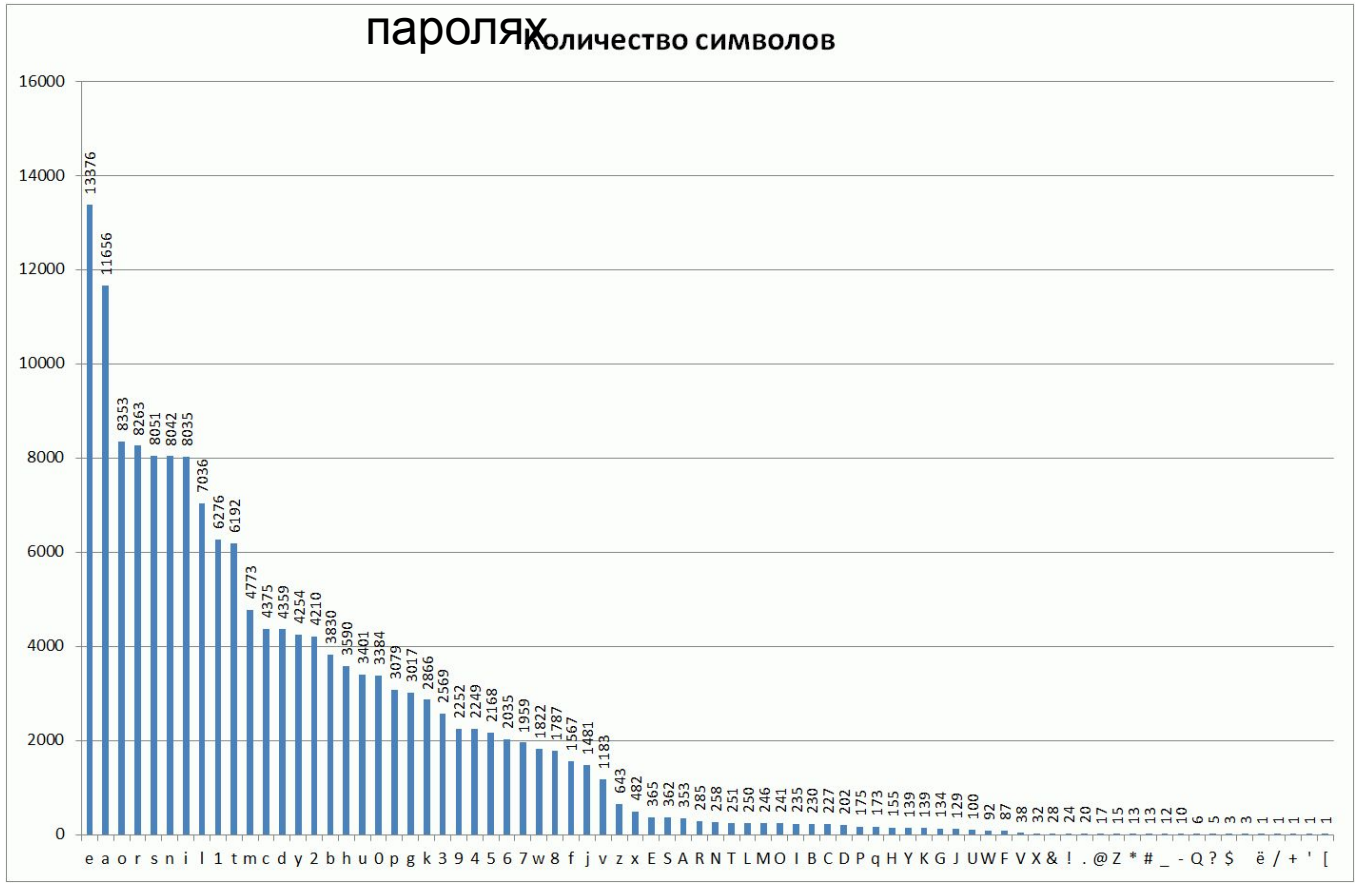
Повторное использование



Словарные пароли



Преобладание символов в паролях



*Использовано изображение

Проблемы безопасности

- Безопасность (security) – это защита от внешних атак. В настоящее время наблюдается значительный рост числа самых разнообразных атак хакеров, угрожающих целостности информации, работоспособности компьютерных систем и зависящих от них компаний, благосостоянию и личной безопасности людей. Для защиты от атак необходимы специальные меры безопасности, компьютерные технологии и инструменты.
- В любой компьютерной системе должна быть реализована подсистема безопасности, которая должна проверять внешнее окружение системы и защищать ее от:
  - Несанкционированного доступа
  - Злонамеренной модификации или разрушения
  - Случайного ввода неверной информации.

Спасибо за внимание!

Ваши вопросы можно задать в ВКС Zoom, либо по почте slv@icc.ru