ТЕЗАУРУС

Справочник от Чарли Чаплина

- А -

❖**Аккаунт** — означает «учётная запись» и представляет собой набор данных о пользователе, которые тот вводит и хранит на каком-либо сайте или интернет-сервисе.

❖**Антивирусная программа** — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных программ и восстановления заражённых такими программами файлов, а также для профилактики — предотвращения заражения файлов.

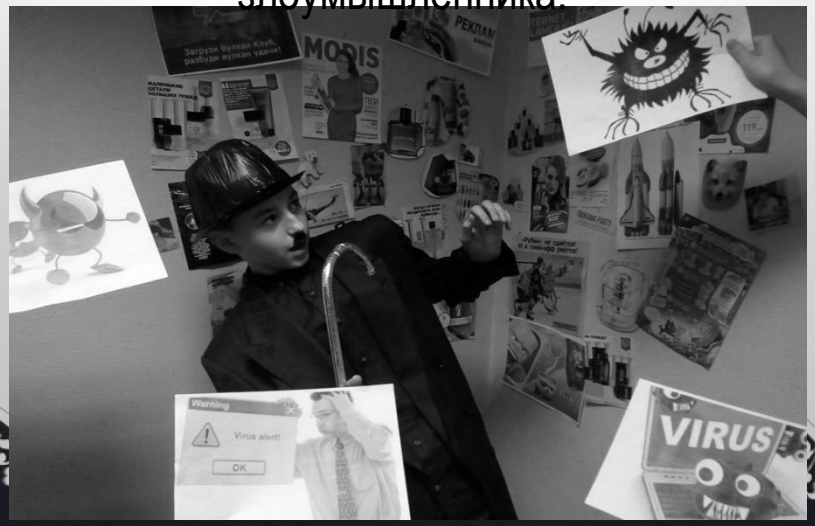
- Б -

❖**База данных** — специальное программное обеспечение, предназначенное для организации хранения и доступа к данным (информации). Большинство современных сайтов хранятся именно в базах данных, расположенных на своих серверах.

❖**Бан (от англ. ban — запрещать)** — один из принятых в Интернете способов контроля за действиями пользователей. Как правило, бан заключается в лишении или ограничении каких-либо прав пользователя (обычно запрет на комментирование и возможность входа в свой аккаунт).

❖ **Безопасность** – отсутствие угроз, либо состояние защищенности от угроз.

❖**Bot-сеть-** это полноценная сеть в Интернет, которая подлежит администрированию злоумышленником и состоящая из многих инфицированных компьютеров, которые взаимодействуют между собой. Контроль над такой сетью достигается с использованием вирусов или троянов, которые проникают в систему. При работе, вредоносные программы никак себя не проявляют, ожидая команды со стороны злоумышленника.



❖**«Брачные мошенничества»** Типичный механизм: с использованием сети Интернет преимущественно на сайтах знакомств преступники выбирают жертву, налаживают с ним электронную переписку от имени девушек, обещая приехать с целью создания в будущем семьи. Затем под различными предлогами «невесты» выманивают деньги (на лечение, покупку мобильного телефона, приобретение билетов, оплаты визы и т.д.).

❖ **Бэкдоры (Backdoor)-** это утилиты скрытого администрирования позволяют, обходя системы защиты, поставить компьютер установившего пользователя под свой контроль. Программа, которая работает в невидимом режиме, дает хакеру неограниченные права для управления системой. С помощью таких backdoor-программ можно получить доступ к персональным и личным данным пользователя.

- В -

❖**Взлом** - это акт получения программного несанкционированного доступа к компьютеру, которые иначе недоступны. Взлом паролей, приводящий к нарушению конфиденциальности электронной почты является угрозой для общения через Интернет. Интернет преступления относятся к уголовным видам деятельности, которые осуществляются через Интернет.

-3 -

❖**Защи́та персона́льных да́нных** — комплекс мероприятий технического, организационного и организационно-технического характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

❖**Зомби** - это инфицированный компьютер, который инфицирован вредоносными программами. Такой компьютер позволяет хакерам удаленно администрировать систему и с помощью этого совершать различные нужные действия

❖**Загрузочные вирусы-** это нередко главный загрузочный сектор вашего HDD поражается специальными загрузочными вирусами. Вирусы подобного типа заменяют информацию, которая необходима для беспрепятственного запуска системы. Одно из последствий действия таковой вредоносной программы это невозможность загрузки операционной системы...

– И –

- **Информационная безопасность** - процесс обеспечения конфиденциальности, целостности и доступности информации.

- **Интернет - мошенничество** - один из видов кибер преступлаений, целью которого является обман пользователей. Хищение конфидециальных данных может привести к тому, что хакер незаконно получает доступ и каким - либо образом использует Вашу личную информацию, что предполагает мошенничество или обман. Уголовный кодекс РФ Статья 159. Мошенничество

– К –

❖**Компьютерный вирус** - это обычная программа, которая обладает самостоятельно прикрепляться к другим работающим программам, таким образом, поражая их работу. Вирусы самостоятельно распространяют свои копии, это значительно отличает их от троянских программ.

❖**Конфиденциа́льность** (от лат. confidentia — доверие) — необходимость предотвращения разглашения, утечки какой-либо информации.

❖**Кликфрод** (click fraud) — мошеннические действия с кликами. Используется мошенниками в рекламе. Обычно клики выполняют программы, тем самым накручивая количество кликов. За каждый клик идёт оплата.

❖**Крякнуть** — взломать программу.

- Л -

❖**Личер** — человек, который только скачивает, а сам не раздаёт. Имеется ввиду торренты.

❖**Линкопомойка** — сайт созданный специально для размещения ссылок, никакой полезной инфы на нём нет.

❖**Лузер** — оскорбительное выражение (англ. loser — проигравший, созвуч. с англ. User) ❖.

❖**Ловушки** Honeypot (горшочек меда) – это сетевая служба, которая имеет задачу наблюдать за всей сетью и фиксировать атаки, при возникновении очага. Простой пользователь совершенно не догадывается о существовании такой службы. Если же хакер исследует и мониторит сеть на наличие брешей, то он может воспользоваться услугами, которые предлагает такая ловушка

❖**Личное оскорбление** – противоправное действие против достоинства человека, совершенное правонарушителем по отношению к пострадавшему без присутствия свидетелей.

❖**Логин** – это ваш уникальный идентификатор, по которому вас распознает система и пользователи. В большей части форумов логином также является ваш никнейм – псевдоним, который выводится в качестве отображения автора сообщения или поста. Эта часть профиля должна быть уникальной для каждого посетителя.

- М -

❖**Макровирусы** - это очень маленькие программы, которые написаны на макроязыке приложений. Такие программки распространяются только среди тех документов, которые созданы именно для этого приложения. Для активации таких вредоносных программ необходим запуск приложения, а также выполнение инфицированного файла-макроса.

❖**Мошенническая рассылка** - с увеличением использования системы электронной почты, ее потребностей в области безопасности также выросли. Мошенники начали манипуляции с системами электронной почты для нарушения безопасности.

- Н -

❖**Накрутка** (кликов, показов и т.п.) — искусственное увеличение количества кликов, показов — то есть тех действий, за которые платятся деньги. Накрутка жестоко карается всеми без исключения сервисами Интернета, вне зависимости от способа заработка.

❖**Hoax** (дословно шутка, ложь, мистификация, шутка, обман) Уже на протяжении нескольких лет многие пользователи сети Интернет получают электронные сообщения о вирусах, которые распространяются якобы посредством e-mail. Подобные предупреждения массово рассылаются со слезной просьбой отправить их всем контактам из вашего личного листа.

– О –

❖**Оскорбление** – целенаправленное действие одного/нескольких человек ради унижения достоинства, чести, веры иного лица или нескольких

❖**Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

- П -

❖**Пароль** – это кодовая фраза, при правильном вводе которой система распознает вас и переводит на свой профиль форума или сайта. Пароль у каждого свой, но они могут быть одинаковы или похожи друг на друга.

❖**Персона́льные да́нные** (или личные данные) — любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

❖**Полиморфные вирусы** – это вирусы, использующие маскировку и перевоплощения в работе. В процессе они могут изменять свой программный код самостоятельно, а поэтому их очень сложно обнаружить, потому что сигнатура изменяется с течением времени.

- Р -

❖**Рекламные программы-** под рекламными и информационными программами понимаются такие программы, которые, помимо своей основной функции, также демонстрируют рекламные баннеры и всевозможные всплывающие окна с рекламой. Такие сообщения с рекламой порой бывает достаточно нелегко скрыть или отключить.

❖**Руткит** – это определенный набор программных средств, который скрыто устанавливается в систему пользователя, обеспечивая при этом сокрытие личного логина киберпреступника и различных процессов, при этом делая копии данных.

- С -

❖**Спам** (англ. spam) — массовая рассылка рекламы или иного вида сообщений лицам, не желающим их получать. Существует также понятие, как спам на сайте. Это означает, что на сайте (странице сайта) обнаружено нежелательное (скрытое) содержимое, которое не видит посетитель сайта, но которое повышает рейтинг сайта в различных поисковых системах. Относится к «черной раскрутке» сайтов.

❖**Свопинг** — самоё «чёрное» из всего «чёрного» SEO. Замена текста на странице, которая занимает верхние позиции в выдаче, на другой совершенно отличающийся по тематике от той, на которую пришёл пользователь.

- Т -

❖**Террористическая деятельность** - Организация, планирование, подготовка, финансирование и реализация террористического акта, а также пособничество в этом - Пропаганда идей терроризма, распространение материалов или информации, призывающих к осуществлению террористической деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности

❖**Троянские программы** - это программы, которые должны выполнять определенные полезные функции, но после запуска таких программ выполняются действия другого характера (разрушительные). Трояны не могут размножаться самостоятельно, и это основное их отличие их от компьютерных вирусов.

– Ф –

❖**Фарминг** - это скрытая манипуляция host-файлом браузера для того, чтобы направить пользователя на фальшивый сайт. Мошенники содержат у себя сервера больших объемов, на таких серверах хранятся большая база фальшивых интернет-страниц. При манипуляции host-файлом при помощи трояна или вируса вполне возможно манипулирование зараженной системой.

❖**«Фишинг»** Является наиболее опасным и самым распространённым способом мошенничества в интернете. Суть заключается в выманивании у жертвы паролей, пин-кодов, номеров и CVV-кодов. Схем, которые помогают мошенникам получить нужные сведения, очень много.

– Э –

❖**Эксплойт** (дословно брешь в безопасности) – это такой скрипт или программа, которые используют специфические дырки и уязвимости ОС или какой-либо программы. Подобным образом в систему проникают программы, с использованием которых могут быть получены права доступа администратора.

❖**ЭКСТРЕМИЗМ** - насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации - публичное оправдание терроризма и иная террористическая деятельность - возбуждение социальной, расовой, национальной или религиозной розни - пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии - нарушение прав, свобод и законных интересов человека и гражданина в зависимости от тех же признаков - организация и подготовка указанных деяний, а также подстрекательство к их осуществлению

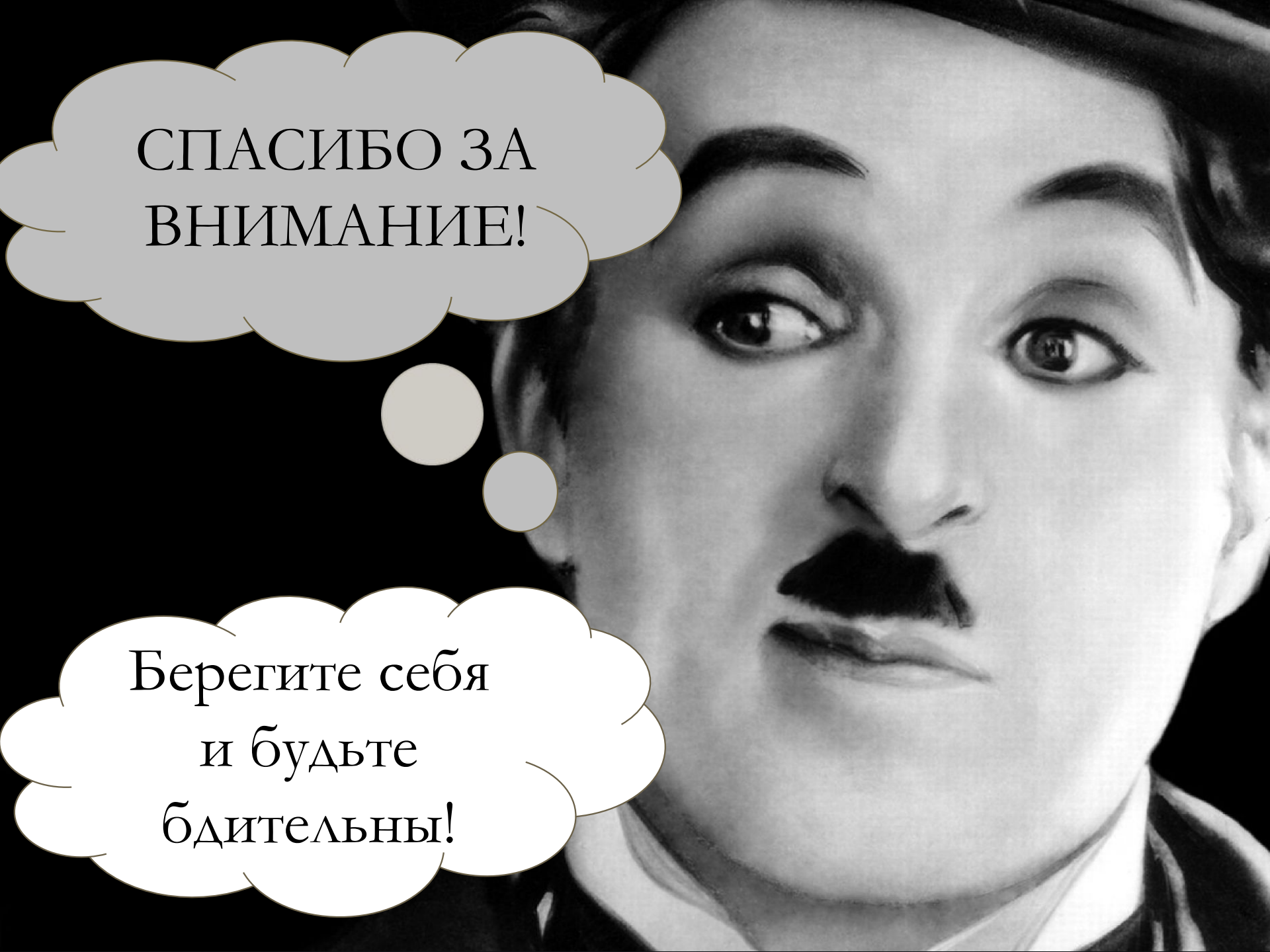
«ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В ИНТЕРНЕТЕ»

- **Ограничь список друзей**. У тебя в друзьях не должно быть случайных и незнакомых людей;
- **Защищай свою частную жизнь.** Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
- **Защищай свою репутацию** - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
- Если ты говоришь с людьми, которых не знаешь, **не используй свое реальное имя** и другую личную информации: имя, место жительства, место учебы и прочее;
- **Избегай размещения фотографий в Интернете**, где ты изображен на местности, по которой можно определить твое местоположение;
- При регистрации в социальной сети **необходимо использовать сложные** пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
- Для социальной сети, почты и других сайтов **необходимо использовать разные пароли**. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

ИСПОЛЬЗУЕМЫЕ ИСТОЧНИКИ:

- https://open-lesson.net/5759/ bezopasnyy_internet.doc
  https://ru.m.wikipedia.org/wiki/Антивирусная_программа
  http://seoslim.ru/voprosy-i-otvety/chto-takoe-login-i..
  http://ugolovnyi-expert.com/moshennichestvo-v-interne..
  http://www.aif.ru/dontknows/eternal/chto_takoe_akkaun..

- https://www.isuct.ru/e-publ/portal/node/247
  http://www.pointlane.ru/personal/ https://мвд.рф/document/1910260
  http://ug-ur.com/prestuplenie/protiv-svobody-chesti-i..


СПАСИБО ЗА ВНИМАНИЕ!
Берегите себя и будьте бдительны!