ЦИФРОВОЙ СЛЕД В ИНТЕРНЕТЕ

ПЕРСОНАЛЬНЫЕ ДАННЫЕ ФИЗИЧЕСКИХ ЛИЦ

- Фамилия, имя и отчество;
- Дата рождения;
- Место рождения;
- Гражданство;
- Информация о регистрации по месту жительства или месту проживания
- Свидетельство о смерти или объявлении лица физического лица умершим, без вести пропавшим, недееспособным или ограничено дееспособным;
- Сведения о семейном положении (о супруге, детях и родителях);
- Информация об образовании;
- Сведения о пенсии;
- Сведения о ежемесячных страховых выплатах;
- Сведения о налоговых обязательствах.

КАК ПРЕДОТВРАТИТЬ КРАЖУ ПЕРСОНАЛЬНЫХ ДАННЫХ

- Пользуйтесь не простыми паролями
- Используйте одноразовые пароли. Никому не сообщайте пароли, пин-коды и коды из SMS, которые приходят на мобильный номер.
- Завидите для интернет покупок отдельную карту
- Не совершайте платежи с других компьютеров
- Не сообщайте свои пароли даже «Службе безопасности»
- Не доверяйте объявлениям о подозрительных дешевых товарах
- Не указывайте свой мобильный телефон на незнакомых сайтах

КАК ПРЕДОТВРАТИТЬ КРАЖУ ПЕРСОНАЛЬНЫХ ДАННЫХ

- Работайте на компьютере под учетной записью с ограниченными правами
- Регулярно выполняйте обновления программного обеспечения
- Используйте антивирусные программы
- Установите VPN
- Удаляйте историю и cookies-файлы в браузере
- Ограничивайте доступ к своим персональным папкам и файлам
- Грамотно удаляйте файлы (CCleaner, Advanced SystemCare)
- Уничтожайте не нужные документы
- В банкоматах обращайте внимание на слот приема карты
- Прирывайте панель пин-кода руками при вводе его в банкоматах или терминалах;
- При потере карты, сразу блокируйте ее через услуги банка
- Не оставляйте вещи без присмотра

ИНТЕРНЕТ ЗНАКОМСТВА

ЗНАКОМСТВО В СОЦИАЛЬНЫХ СЕТЯХ

Поддельные сайты знакомств.
Сайты знакомств не застрахованы от мошенников, но если ещё при регистрации в анкете много вопросов про личные финансы, то стоит остерегаться.

Большие проблемы с правописанием – ещё одна причина насторожиться.

Ссылки на спам-сайты, на порно сайты – признак того, что профиль может оказаться мошенническим.

КИБЕРБУЛЛИНГ

КИБЕРБУЛЛИНГ

Намеренные оскорбления, угрозы, диффамации и сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени.

Типичные действия, осуществляемые при травле – это распространение заведомо ложной информации (слухов и сплетней) о человеке, насмешки и провокации, прямые оскорбления и запугивание, социальная изоляция (бойкот и демонстративное игнорирование), нападки, ущемляющие честь и достоинство человека, причинение материального или физического вреда.

К формам психологического давления, присущего традиционной травле, добавляются возможности всемирной паутины, благодаря чему она приобретает следующие функции:

- Круглосуточное вмешательство в личную жизнь. Травля не имеет временного или географического ограничения. Нападки не заканчиваются после школы или рабочего дня. Киберхулиган (моббер) круглосуточно имеет прямой доступ через технические средства к жертве: мобильный телефон или профиль в социальных сетях и электронную почту. Благодаря постоянным номерам и учётным записям жертва не защищена от нападок и дома.
- Неограниченность аудитории, быстрота распространения информации. Сообщения или изображения, пересылаемые электронными техническими средствами, очень трудно контролировать, как только они оказались онлайн.
- Анонимность преследователя. Киберпреступник не показывает себя своей жертве, может действовать анонимно, что обеспечивает ему – пусть и кажущуюся – безопасность и нередко увеличивает срок его негативной «кибер-активности». Незнание жертвой, кем является тот, «другой», кто её третирует, может запугать её и лишить покоя.

ЧЕМ ОПАСНА?

- Кибербулинг может показаться менее серьёзным явлением, чем реальная агрессия. Но последствия кибербулинга бывают очень тяжёлыми, в их список могут входить не только негативные эмоции (стыд, страх, тревога), но и суицидальные попытки и завершенные суициды.
- Агрессия в сети может быть более опасной, т.к. агрессор не знает, когда нужно вовремя прекратить.
- Снижение самооценки, проблемы в семье, проблемы с успеваемостью, насилием в школе и т.д.

КАК ОСТАНОВИТЬ КИБЕР-ТРАВЛЮ?

- Важно удалить личную информацию из открытых источников (адрес, улица, дом, квартира).
- В социальных сетях есть такая опция, как бан. Можно пожаловаться администрации, и агрессора заблокируют.
- Игнорирование сообщений от агрессора. Есть шанс, что ему это надоест, поскольку он не получает от жертвы необходимой ему реакции: страха и тревоги.
- Не бояться рассказать о травле в интернете.
- В сложных случаях нужно делать скриншоты переписки с оскорблениями и угрозами и обращаться в полицию.

ВЫСКАЗЫВАНИЯ В ИНТЕРНЕТЕ

ПОЧЕМУ ЭТО ВАЖНО?

От интереса борцов с экстремизмом не застрахован никто. Вот несколько примеров наказаний за высказывания в сети.

В 2011 году жителя Татарстана оштрафовали за лайк под скриншотом кадра из фильма «Американская история Х» про неонацистов (сам фильм не запрещён в РФ).

В 2013 году жительница Первоуральска получила 120 часов обязательных работ за комментарий под записью о встрече Нового года, где она назвала праздник «древним кельтским ритуалом».

В 2015 году журналистку из Смоленска оштрафовали на 1000 рублей за демонстрацию нацистской символики: девушка выложила фото своего двора времён войны и проглядела там флаг гитлеровской Германии. В том же году анархистку из города Иваново оштрафовали на 100 тыс. рублей за репост записи с призывом протестовать против существующего политического режима.

КАК ПОЯВЛЯЮТСЯ ТАКИЕ ДЕЛА?

По доносу

Многие уголовные и административные дела за высказывания в интернете появляются после доносов. Их пишут «верующие», чьи чувства якобы были оскорблены, профессиональные борцы с инакомыслием и просто «бдительные граждане». В таком случае доносчик получает статус «заявителя», и его данные фигурируют в материалах следствия.

От полицейских

В роли инициатора уголовного дела могут выступать сами правоохранители. Уголовно-процессуальный кодекс предусматривает возбуждение дела на основании рапорта об обнаружении признаков преступления (ст.140). В этом случае, даже если в основу дела и был положен донос, узнать об этом не получится. Теоретически возможна ситуация, когда некий следователь для повышения статистики раскрываемости сам просматривает страницы в соцсетях, находит контент, который, по его мнению, может стать поводом для обвинения, и пишет рапорт.

КАК И КТО РЕШАЕТ, ЧТО ОПУБЛИКОВАННОЕ - ЭКСТРЕМИЗМ?

Актуальный список признанных экстремистскими материалов доступен на сайте Министерства Юстиций Российской Федерации. Однако иногда написанное вами (процитированное, выложенное в сети) не является изначально экстремистским материалом. Чтобы признать его таковым, следствие должно провести экспертизу. Главным критерием для определения статьи, по которой могут привлечь за экстремизм – умысел.

Следствию предстоит доказать, что действие было произведено умышленно, то есть с целью возбудить ненависть или вражду. Для этого собирают доказательства. Ими могут быть, например, комментарии автора публикации в духе «вот книга, которая подскажет, как правильно действовать» или другие выражения поддержки написанного в экстремистском произведении. Для того, чтобы доказать умысел, следователи могут изучать иные публичные высказывания подозреваемого и в качестве довода использовать даже его «лайк» под комментарием другого человека, который одобрил содержание экстремистской книги.

Таким образом, потенциально любой текст или картинка могут быть признаны разжигающими ненависть или оскорбляющими чувства верующих.

ПРИЗНАЛИ ВИНОВНЫМ, ЧТО ТЕПЕРЬ?

Вашу технику уничтожат. Если суд признает вашу вину в экстремизме, вам грозит не только наказание, предусмотренное соответствующей статьей УК. Иногда судьи приговаривают к уничтожению «орудия преступления». Такой случай произошёл, например в Екатеринбурге. Компьютера и мыши лишилась осуждённая по 282 статье жительница Екатеринбурга, которая делала репосты публикации об украинском конфликте.

Вы лишитесь сбережений и возможности получать деньги через банк. Серьёзное последствие – включение в так называемый «список Росфинмониторинга». Его фигуранты не могут совершать практически никакие банковские операции на территории России, их счета блокируют, им не перечисляют в полной мере социальные выплаты. Причём попасть в «перечень» можно даже будучи подозреваемым по делу об экстремизме. Закон предусматривает исключение из списка фигурантов, в отношении которых прекращают уголовные дела и тех, у которых погашены судимости, но на деле выйти из этого перечня бывает очень трудно.

- Каких слов и призывов точно стоит избегать в своих публикациях?

Хотите написать что-то рискованное – делайте это с умом.

Что точно не стоит публиковать, так это призывы к нанесению вреда здоровью и имуществу и т.д.

- Что нужно учитывать, прежде чем оставлять потенциально экстремистский/оскорбительный комментарий, картинку в интернете? С чем сверяться?

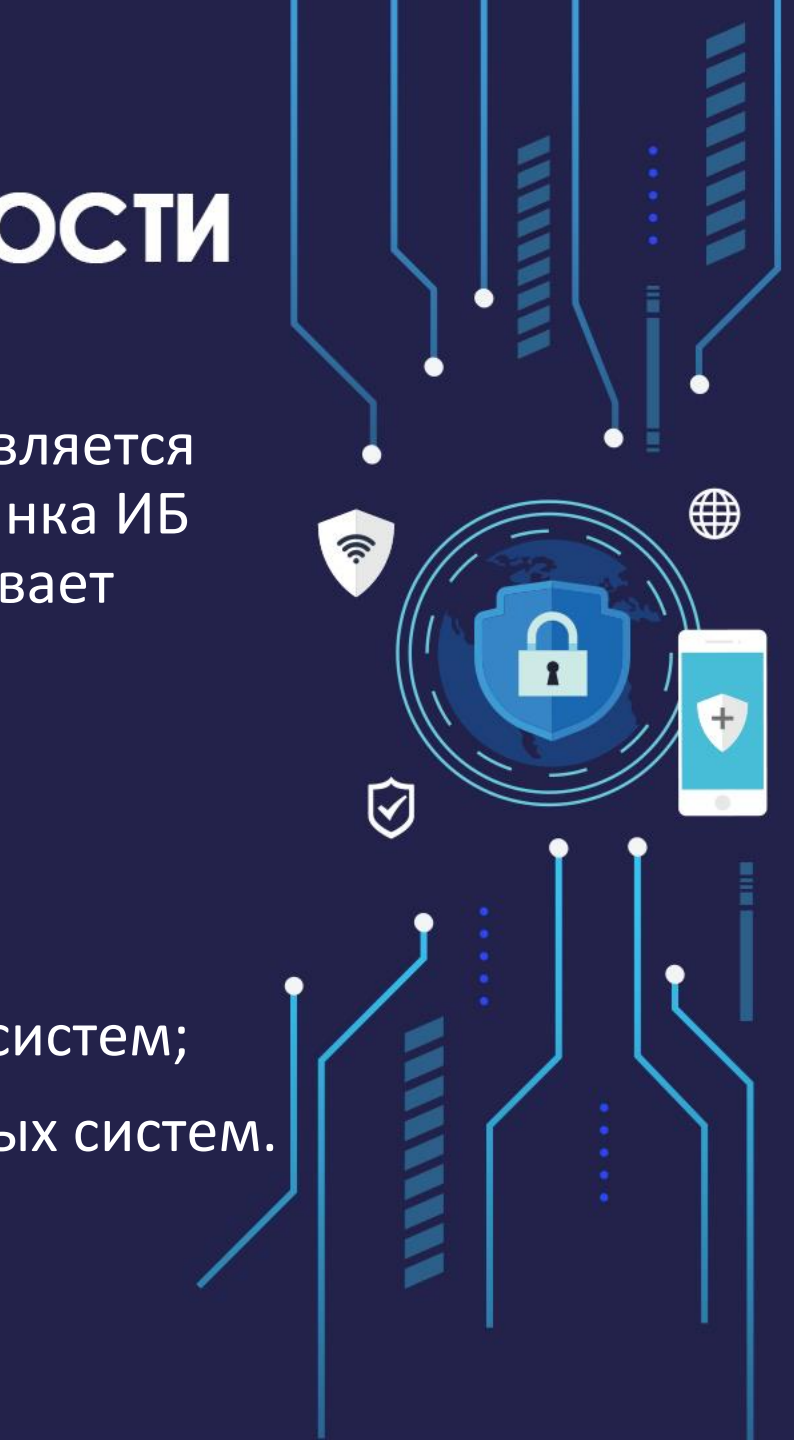
Теоретически можно свериться со списком Минюста, но никаких гарантий это не даст – он не всеохватывающий. Может быть назначена экспертиза на предмет наличия экстремистского контента в вашей публикации, и тут ваша судьба окажется в руках эксперта с его субъективным мнением.

Вот какие условия должны совпасть, чтобы информация попала в поле зрения генпрокуратуры и стала поводом для штрафа:

- Информация выражена в неприличной форме;
- Эта форма оскорбляет человеческое достоинство и общественную нравственность;
- При этом выражается явное неуважение к обществу, государству, государственным символам, конституции или органам государственной власти.

КАКОВО БУДУЩЕЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

На сегодняшний день информационная безопасность является одной из самых быстрорастущих ветвей сегодня рост рынка ИБ составляет 25-30% в год, в то время как IT-рынок показывает меньшие темпы. (около 5% ежегодно).



Специальности:

- Информационная безопасность;
- Информационная безопасность автоматизированных систем;
- Информационная безопасность телекоммуникационных систем.