Безопасность информации

Шеламова Марина Алексеевна

Информация - основной ресурс современного мира. Информационная эра диктует новые условия жизни, новый подход к работе и полностью меняет наше поведение. Теперь нам доступны мощнейшие ресурсы и колоссальный объем информации, который мы же и формируем. Но что это за среда? Чего мы не замечаем? Как она воздействует на нас и для чего это нужно? Давайте изучать то, частью чего мы уже давно являемся.

Информационная безопасность — состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере.

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

Безопасность информации определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные или на другие ресурсы автоматизированной информационной системы.

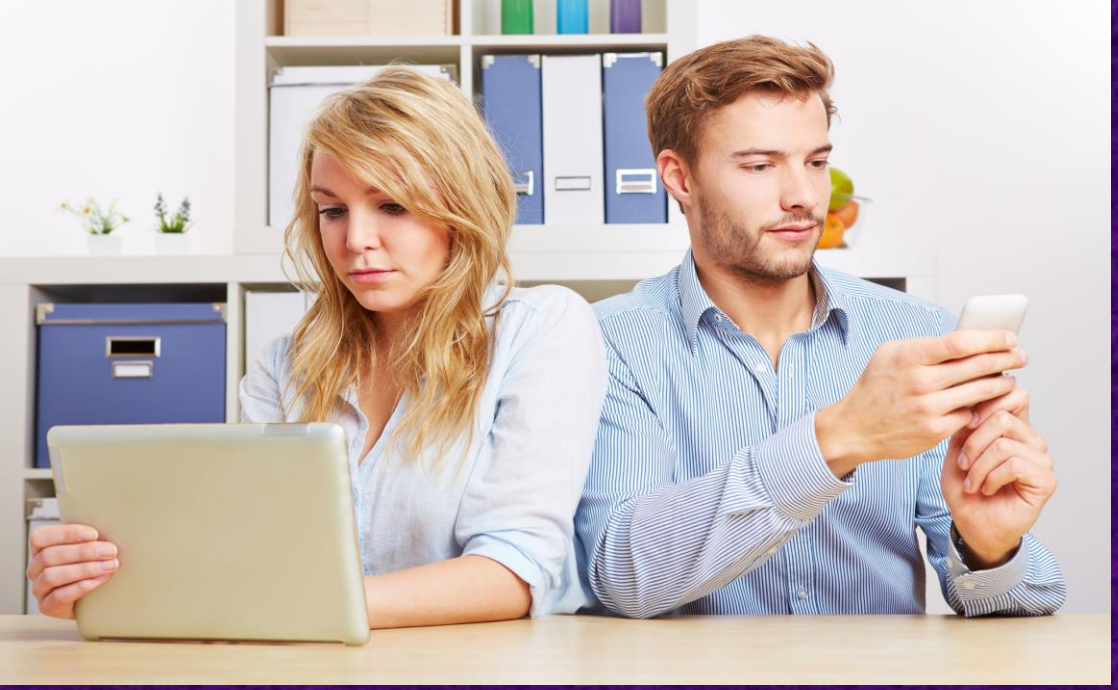
МЕТОДЫ КОНТРОЛЯ ДАННЫХ

Активно разрабатываемые медицинские информационные системы позволяют создавать электронные медицинские карты пациентов и истории болезни. Они удобнее и надежнее бумажных, в частности, появляется возможность легко и эффективно контролировать доступ к ним лишь конкретных лиц. В то же время потенциальная возможность передачи огромного количества конфиденциальной информации с колоссальной скоростью практически неограниченному числу адресатов порождает серьезные проблемы, относящиеся к сфере информационной безопасности.

СОБЛЮДЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ

Соблюдение конфиденциальности при использовании данной информации в медицинских организациях подразумевает не только применение технических средств защиты (специальные сертифицированные программные и технические средства защиты информации), но и проведение комплекса организационных мероприятий, направленных на предотвращение потери, искажения и несанкционированного доступа к персональным данным.

Для защиты конфиденциальной медицинской информации пользователь для входа в медицинскую информационную систему должен ввести свой логин и пароль для идентификации. Это позволяет обеспечить доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости.



КУЛЬТУРА ОБЩЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ

Интернет сегодня - это самый колоссальный источник информации, который знало человечество. Но его возможности, такие, как оперативность, быстрота и доступность связи между пользователями на дальних и близких расстояниях, позволяют использовать Интернет не только как инструмент для познания, но и как инструмент для общения. Поэтому даже находясь по ту сторону экрана, следует придерживаться правил поведения в социальных сетях.

ПРИ РЕГИСТРАЦИИ СВОЕГО АККАУНТА В СОЦИАЛЬНОЙ СЕТИ

Пользователь обязан:

- ✓ Сообщать о всех нарушениях администрации сайта;
- ✓ Не предоставлять логин и пароль от своего аккаунта другим лицам;
- ✓ При регистрации предоставлять достоверную информацию;
- ✓ Нести полную ответственность за информацию, размещенную на его странице;
- ✓ Соблюдать положения законодательства РБ.

Пользователь НЕ должен:

- × Создавать фальшивые аккаунты;
- × Оскорблять собеседников;
- × Распространять ложную и рекламную информацию, вредоносные программы, информацию содержащую: пропаганду преступной деятельности, угрозы, непристойные материалы, сцены насилия;
- × Незаконно размещать личные материалы третьих лиц, без их согласия.

НЕ СТОИТ публиковать в социальных сетях:

- тексты, изображения и видео на тему национальностей;
- контент, высмеивающий религии;
- информацию о фашизме и терроризме.

Перед тем как выложить любые фото и видеоматериалы в сеть, обязательно задумайтесь, что будет, если их увидит ваши родители, друзья, преподаватели, в общем, весь ваш круг общения. Помните — социальные сети место встреч абсолютно разных людей, всех возрастов, различных профессий, с самыми разными интересами и намерениями.

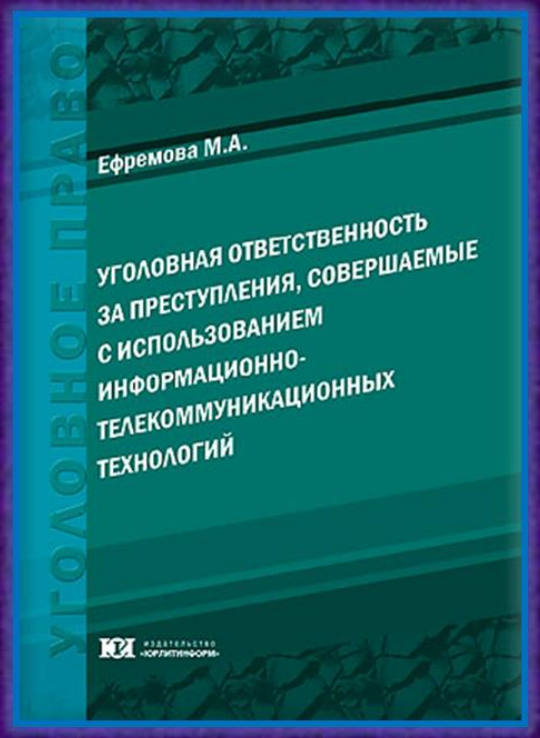
Включите самоцензуру. Не размещайте и не лайкайте посты, которые могут вас скомпрометировать!!!

Не полагайтесь на настройки конфиденциальности

Как бы прилежно вы ни пытались защитить свои личные данные в социальных сетях, лучше всего привыкнуть к мысли о том, что вся опубликованная вами информация может стать известной другим людям.

Полагайтесь на свое благоразумие.

- Никогда не оставляйте на незнакомых сайтах, а также по чьей-то просьбе логин и пароль ваших страничек.
- Ограничьте вашу персональную информацию. В социальной сети вовсе не обязательно выкладывать свой адрес и номер телефона. Размещенная в открытом доступе персональная информация о вас грозит неприятностями для вас со стороны других людей.
- Не поддавайтесь на предложения и не ходите на личные встречи с малознакомыми людьми.



ОТВЕТСТВЕННОСТЬ ЗА ПРАВОНАРУШЕНИЯ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Законом № 317-З в Кодекс Республики Беларусь об административных правонарушениях введена статья, устанавливающая административную ответственность за совершение правонарушений при использовании национального сегмента сети Интернет.

В законодательстве РБ предусмотрена ответственность, в том числе уголовная, за совершение противоправных деяний в сфере высоких технологий. Сейчас наблюдается резкий рост таких преступлений . Уголовные дела возбуждены за хищение имущества, путем введения в компьютерную систему ложной информации, сопряженное с несанкционированным доступом к компьютерной информации, а также за завладение имуществом путем обмана и злоупотребления доверием. Потерпевшими от данных преступлений являются лица в возрасте 20–25 лет, часто использующие для общения социальные сети.

Увлекаешься информатикой?
Используешь знания незаконно?
Нравится взламывать чужие сайты?

Отлично
Преступно
Наказуемо

ВНИМАНИЕ!!! Ответственность с 14 лет

Статья 212 Уголовного кодекса: хищение путем использования компьютерной техники либо введения в компьютерную систему ложной информации *(фишинг)* наказывается вплоть до лишения свободы на срок до 3 лет. Те же действия, совершенные повторно либо в группе – на срок до 5 лет.

Статья 349 Уголовного кодекса: несанкционированный доступ к компьютерной информации, совершенный из корыстной или иной личной заинтересованности, либо группой лиц наказывается на срок до 2 лет лишения свободы, а повлекший по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми или иные тяжкие последствия - на срок до 7 лет.

Всё тайное всегда когда-то становится явным

ФИШИНГ **– не только рыбалка!** ***Преступление*** **– не развлечение!**

Милиция общественной безопасности МВД Республики Беларусь

Чтобы различать компьютеры в Интернет, каждому из них присваивается адрес, представляющий собой уникальную цепочку цифр или соответствующее этой цепочке символьное имя компьютера.

Адрес компьютера позволяет однозначно идентифицировать компьютер, подключенный к Интернет

Фейк (англ. fake — подделка, фальшивка, обман, мошенничество) — что-либо ложное, недостоверное, сфальсифицированное, выдаваемое за действительное, реальное, достоверное с целью ввести в заблуждение.

Фейковые новости (англ. fake news) — намеренная дезинформация в социальных медиа и традиционных СМИ.

Фейком чаще всего является поддельный контент в сети

Способность отличать правдивую информацию от лжи зависит не только от интеллекта читателя. В частности, тут важно и его социальное окружение. Проведенные эксперименты доказали, что если люди вокруг поголовно кричат, что пингвины оранжевые, то даже закоренелые скептики в конце концов согласятся с данным утверждением.

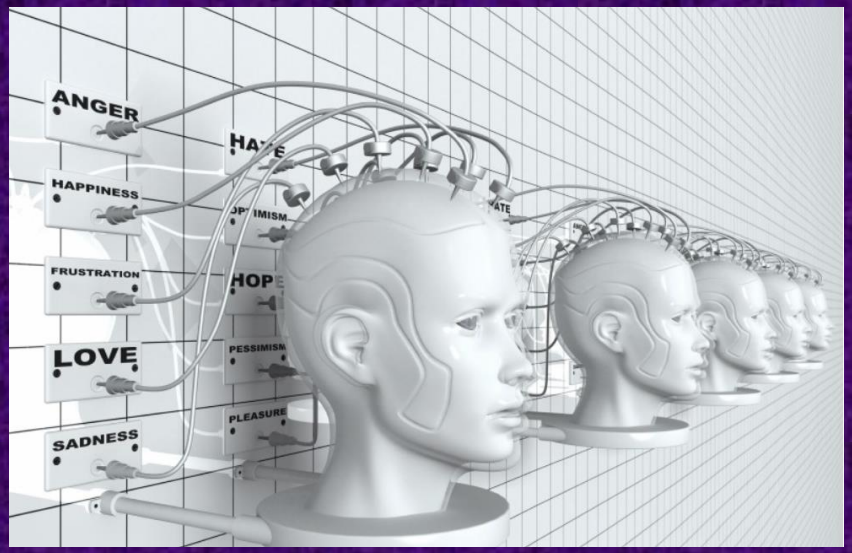
Количество фейков в Интернете в настоящее время достигло критической массы, их плодят все: шутники, лгуны, пиарщики, бойцы информационного фронта, охотники за лайками, прирожденные сплетники, больные фантазеры, а то и автоматические бредогенераторы.

Есть несколько целей, которые преследуют создатели фейкового контента. Самые распространенные из них:

- намеренная дезинформация пользователей о каких-либо фактах событиях для так называемого хайпа;
- формирование у потребителя информации определенного взгляда на вещи;
- проведение мошеннических и жульнических операций;
- открытое оскорбление определенных лиц;
- агитация;
- троллинг (чаще всего в таких случаях фейк создается для развлечения и самоутверждения путем участия в спорах, дискуссиях) и т.д.

В каждой из этих ситуаций фейк имеет негативный оттенок, поэтому его создание – недобросовестное и плохое действие.

Особое место в информационной сфере общества занимают индивидуальное, групповое и массовое сознание людей, которое все в большей степени подвергается агрессивным информационным воздействиям, что в ряде случаев наносит ущерб психическому и нравственному здоровью граждан, разрушает моральные нормы жизни общества, приводит к дестабилизации социально–политической обстановки.



Это связано с тем, что в сети Интернет отсутствует какой либо управляющий или контролирующий орган. Ответственность за помещаемую в Интернет информацию фактически не несет ни автор, часто анонимный, ни провайдер.

СПОСОБЫ СОВЕРШЕНИЯ КИБЕРПРЕСТУПЛЕНИЙ

- получение несанкционированного доступа к государственным и военным секретам, банковской и личной информации;
- кража или уничтожение информации, программ и технических ресурсов путем преодоления систем защиты, внедрения вирусов;
- воздействие на программное обеспечение и информацию;
- раскрытие и угроза публикации закрытой информации;
- захват каналов СМИ с целью распространения дезинформации, слухов, демонстрации мощи террористической организации и объявления своих требований;
- уничтожение или активное подавление линий связи;
- проведение информационно-психологических операций и т.д.

Сейчас почти все программы и «железо» имеют удаленное управление, которое привязано к поставщику. Управлять можно почти любым программным обеспечением или оборудованием. В большинстве случаев оно имеет встроенные модули, которые обращаются к поставщику за какой-то информацией. А это означает возможность удаленного влияния на систему.

Иностранное программное обеспечение открывает возможность слежки за пользователем.

- Массовая слежка. Социальные сети, смартфоны, фитнес-браслеты и все другие персональные гаджеты так или иначе собирают данные пользователей, анализируются и продаются третьим компаниям для предоставления адресной рекламы.
- Профессиональная, за конкретным лицом.

Фитнес-браслет следит за тобой! И это не паранойя

Использование любых социальных сетей или любых облачных хранилищ должно сопровождаться пониманием, что эта информация - публичная.

Кроме того, мы должны понимать, что как у производителей платформ, так и у разных приложений есть доступ к информации, которую мы храним в своих устройствах.

Как Google отслеживает вас?

Сервисы Google — это целостная система, доступ к которой получает любой владелец аккаунта Google. Большинство из них — веб-приложения, требующие от пользователя **только наличия браузера,** в котором они работают, и **интернет-подключения**.

Название службы	Описание
Google поиск	Крупнейшая поисковая система интернета. Основной продукт Google
YouTube	Популярнейший видеохостинг
Gmail	Электронная почта
Google Maps	Картографическая система
Google Drive	Облачное хранилище данных
Google Play	Магазин приложений
Google News	Портал новостей
Google Hangouts	Обмен мгновенными сообщениями (чат) видео- и голосовая связь
Google Translate	Перевод слов, текстов, фраз, веб-страниц
Google Photos	Редактирование, хранение и публикация фотографий. Фотографии хранятся на диске
Google Books	Поиск в книжной библиотеке
Google Docs	Сравнительно простые редакторы текстов, презентаций и электронных таблиц
Blogger	Платформа для ведения блогов
Google Earth	Геоинформационная система с фотографиями

Синдром танцующей свиньи

Если друг прислал вам ссылку на программку с танцующими свиньями, вы наверняка установите ее, даже если в лицензионном соглашении будет написано о возможности потери всех данных, чувства юмора, вины, совести, разума и среднего достатка.

Кибертерроризм

Может появиться злой гений, который придумает что-то такое, что все содрогнутся... Первая ласточка - компьютерный червь Stuxnet. Попав в системы лаборатории по обогащению урана в Иране, он физически разрушил центрифуги. Ровно то же самое может произойти с любой системой, которая вырабатывает электричество, запирает шлюзы, управляет подводной лодкой или ведет Международную космическую станцию. Если система имеет управляемые модули, связанные с интернетом, - это сразу означает резкое снижение уровня ее защищенности.

Некоторые инциденты нарушения безопасности в июне 2019 года

- В середине недели сотни тысяч пользователей Telegram по всему миру не смогли получить доступ к мессенджеру из-за DDoS-атаки на его серверы.
- Один из крупнейших мировых производителей запчастей для авиационной техники бельгийская компания ASCO была вынуждена приостановить работу заводов в четырех странах из-за атаки с использованием вымогательского ПО. Вредонос вывел из строя IT-системы ASCO, в результате компания отправила большую часть своих сотрудников в неоплачиваемый отпуск на неделю. Объем ущерба от атаки и использованное в ней вредоносное ПО, пока неизвестны.
- Житель китайской провинции Хэйлунцзян проложил электрокабель по дну рыбных прудов для кражи с нефтедобывающей установки электроэнергии для добычи криптовалюты биткойн. Убытки от его действий оцениваются в 48 560 юаней (порядка 453 тыс. рублей).

Есть ли какая-то система защиты от такого рода угроз?

В большинстве стран созданы специализированные центры, которые занимаются защитой от массовых угроз.

Например, в Китае есть так называемый великий китайский файрвол, он же «золотой щит», - фильтрация попадающей по интернету извне информации.

Рекомендации для личной безопасности

- Убедитесь, что ваш домашний Wi-Fi хорошо запаролен и никогда не пользуйтесь подозрительным интернет-соединением.
- Меняйте пароли чаще, делайте их длиннее.
- Установите антитрекинговые плагины в ваш браузер. Отключите историю в Google.
- Регулярно делайте резервные копии данных и храните их на разных облаках.

- И, самое главное, читайте пользовательские соглашения устанавливаемых программ.

Надеюсь, этот материал будет вам полезен