

ПЕРЕМЕНКА

СПЕЦИАЛЬНЫЙ ВЫПУСК

КИБЕРБЕЗОПАСНОСТЬ

Реализация мер эффективной кибербезопасности в настоящее время является достаточно сложной задачей, так как сегодня существует гораздо больше устройств, чем людей, а злоумышленники становятся все более изобретательными.

Кибербезопасность – это реализация мер по защите систем, сетей и программных приложений от цифровых атак. Такие атаки обычно направлены на получение доступа к конфиденциальной информации, ее изменение и уничтожение, на вымогательство у пользователей денег или на нарушение нормальной работы компаний.

30 ноября отмечается международный день информационной безопасности

День информационной безопасности существует с 1998 года, он учреждён Международной ассоциацией информационной безопасности (International Computer Security Association). Связан с именем Роберта Морриса (Robert Tappan Morris), студента, имевшего доступ к Arpanet и написавшего код первого червя – программы, самостоятельно распространяющейся по сети.

Червь Морриса» парализовал работу более чем шести тысяч компьютеров в университетах и государственных вычислительных центрах США. Вредоносный код создавался с исследовательской целью, но Моррис допустил ошибку в коде, из-за которой червь забирал все вычислительные ресурсы заражённого компьютера и тем самым выводил его из строя. Испугавшись содеянного, Моррис не сразу сообщил о том, что его код является причиной отказа компьютеров. Морриса осудили на три года условно. Ущерб составил, по разным оценкам, до 100 миллионов долларов.

Цель, с которой отмечается день информационной безопасности, состоит в пропаганде правил обеспечения безопасности личной информации, знания приёмов защиты от взлома компьютера и мобильного устройства.



ЧТО ТАКОЕ
КИБЕРБЕЗОПАСНОСТЬ?



КАК ГЛОБАЛЬНАЯ СЕТЬ
ВЛИЯЕТ НА ЧЕЛОВЕКА

В ЭТОМ ВЫПУСКЕ

Правовое обеспечение

Авторское право

Социальные сети

Фишинг

Кибербуллинг

Полезные ссылки



КИБЕРБЕЗОПАСНОСТЬ И ЕЁ ПРАВОВОЕ ОБЕСПЕЧЕНИЕ



Имея современный компьютер и выход в глобальную сеть, отдельные лица, организации, различные структуры, государства и их союзники осуществляют кибердеятельность, преследуя при этом свои, не известные другим субъектам информационного процесса, цели. Характер этих целей различен, начиная от информирования о просветительных, поступательных преобразований в различных областях науки и техники и заканчивая нанесением, с помощью этих же достижений, ущерба потенциальному противнику. Во-первых, в киберпространстве очень сложно определить сам источник воздействия на информационные ресурсы, и, во-вторых, – его местонахождение.

Поэтому на современном этапе развития и функционирования киберпространства особо актуальным становится принятие международным сообществом нормативно-правовых актов, регулирующих происходящие в нём процессы, что подразумевает создание на всех его уровнях достаточно совершенной системы безопасности, которую допустимо определить, как кибербезопасность.



[Федеральный закон от 13.03.2006 № 38–ФЗ \(ред. от 03.08.2018\)](#)

О рекламе»

[Федеральный закон от 27.07.2006 № 149–ФЗ \(ред. от 19.07.2018\)](#)

Об информации, информационных технологиях и о защите информации»

[Федеральный закон от 27.07.2006 № 152–ФЗ \(ред. от 31.12.2017\)](#)

О персональных данных»

[Федеральный закон от 29.12.2010 № 436–ФЗ \(ред. от 29.07.2018\)](#)

О защите детей от информации, причиняющей вред их здоровью и развитию»

[Письмо Минобрнауки России от 14.05.2018 № 08–1184](#)

О направлении информации «(вместе с «Методическими рекомендациями о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети «Интернет»)

[Федеральный закон от 21.07.2011 № 252–ФЗ](#)

О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»

[Приказ № 5 от «13» января 2012 года](#)

О проверочных мероприятиях по исключению доступа обучающихся образовательных учреждений к сайтам экстремистской направленности и иным ресурсам сети Интернет, несовместимым с образовательным процессом»

[Приказ № 279 от «26» марта 2012 года](#)

О проведении проверки эффективности контент-фильтрации, используемой подведомственными учреждениями профессионального образования при осуществлении доступа к ресурсам сети Интернет»



АВТОРСКОЕ ПРАВО

Современные школьники – активные пользователи цифрового пространства. Однако не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

- ✓ Термин **«интеллектуальная собственность»** относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.
- ✓ **Авторские права** - это права на интеллектуальную собственность, на произведения науки, литературы и искусства.



["Гражданский кодекс Российской Федерации \(часть четвертая\)" от \(ред. от 23.05.2018\)](#)

ГК РФ Глава 70.
АВТОРСКОЕ ПРАВО

- ✓ Авторские права выступают в качестве **гарантии** того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание.
- ✓ Никто **без разрешения автора** не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в интернете.
- ✓ Использование **«пиратского»** программного обеспечения может привести ко многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа.
- ✓ Не стоит также забывать, что существуют **легальные и бесплатные программы**, которые можно найти в сети.

Авторские права распространяются как на обнародованные, так и на необнародованные произведения, которые выражены в письменной форме, устной форме (в виде публичного произнесения, публичного исполнения и иной подобной форме), в форме изображения, в форме звуко- или видеозаписи, в объемно-пространственной форме и т.д.

Для возникновения, осуществления и защиты авторских прав не требуется регистрация произведения или соблюдение каких-либо иных формальностей.

В отношении программ для ЭВМ и баз данных возможна регистрация, осуществляемая по желанию правообладателя.

Авторские права не распространяются на идеи, концепции, принципы, методы, процессы, системы, способы, решения технических, организационных или иных задач, открытия, факты, языки программирования.



– это беспроводной способ передачи данных, использующий радиосигналы. Wi-Fi - аббревиатура от английского словосочетания Fidelity, что дословно переводится как беспроводная точность. Бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но общедоступные сети Wi-Fi не являются безопасными.

СОВЕТЫ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ WI-FI

- ✓ Не передавай свою личную информацию через общедоступные сети Wi-Fi. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера.
- ✓ Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закладки вируса на твоё устройство.
- ✓ При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе.
- ✓ Не используй публичный Wi-Fi для передачи личных данных, например для выхода в социальные сети или в электронную почту.
- ✓ Используй только защищенное соединение, то есть при наборе веб-адреса вводи именно «https://».
- ✓ В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Насколько безопасны открытые Wi-Fi сети?

Они опасны в крайней степени. Именно благодаря общедоступным бесплатным Wi-Fi сетям хакеры воруют огромное количество личной информации! Будьте аккуратны и старайтесь избегать передачи личных данных в сети. Максимум, можно ограничиться новостным серфингом, не более. Мобильный интернет сегодня доступен, скорости позволяют обрабатывать огромные объемы информации, поэтому если выбор встал между бесплатной **Wi-Fi** и мобильным интернетом – выбирайте последний.



КАК БЕЗОПАСНО ОБЩАТЬСЯ В СОЦИАЛЬНЫХ СЕТЯХ

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, в них уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

СОВЕТЫ ПО БЕЗОПАСНОМУ ОБЩЕНИЮ В СОЦИАЛЬНЫХ СЕТЯХ

Интернет, предоставляя возможность в любое мгновение получить ответ на любой вопрос, оказывает пагубное влияние на способность к концентрации и анализу, особенно у молодёжи. Понимание того, что информация всегда под рукой на компьютере, отбивает у людей желание что-либо запоминать.

Бернард Вербер

- ✓ 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 информацию: 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 ко всем сразу.

Мифы о социальных сетях

Миф №1. В социальных сетях все равны. В соц. сетях есть аккаунты известных артистов, политиков, бизнесменов. Технически они ничем не выделяются среди обычных. В социальных сетях эквивалент деньгам — это социальная поддержка (лайки, комментарии, просмотры, подписки). У кого пара лайков под фотографиями — социальный бедняк, у кого сотни тысяч — социальный олигарх.

Миф №2. Он(она) просто размещал(а) в соц сетях контент, людям понравилось и к нему(ней) пришли слава и деньги. Раскрученные аккаунты принадлежали либо детям богатых родителей, либо этих людей стала раскручивать какая-то фирма (в том числе сама соц сеть для создания её лица), либо человек вложил свои собственные деньги. И вот мальчики также пытаются кривляться перед камерой, как их кумир на ютубе, а девочки обозревать содержимое своих сумочек. Только проходит год-два, у кумира прибавляется очередной миллион подписчиков, а эти девочки и мальчики едва набрали несколько тысяч.

Миф №3. Главное, уникальный и качественный контент! На деле, если твой контент будет совершенно уникален, посетители социальных сетей, в которых воспитывается стадный инстинкт, просто не будут знать, как на это реагировать. Когда есть уже готовые оцененные шаблоны, пользователю сетей легко ориентироваться. Вот взять, к примеру, тревел-блогеров, которые снимают в путешествиях свое лицо посередине кадра и болтают, что в голову придёт (всегда думал, зачем им ехать куда-то за границу, так можно с камерой и в российской деревне ходить — всё равно кроме лица в кадре практически ничего не видно) — формат сформирован, много лайков и просмотров, значит, популярно и можно смотреть.

Миф №4. Социальные сети — это большие возможности для самореализации. Там ты работаешь на себя, делая проекты.

Миф №5. В социальных сетях я разбогатею на рекламе. Реклама акцентирует на себя внимание и раздражает, как вставка кричащих рекламных блоков во время трансляций передач и фильмов по телевизору. Как итог — негативные комментарии на тему.

Миф №6. Социальные сети помогут мне найти себе друзей, познакомиться с интересными людьми и т.п. Представьте деревню, где немного жителей, все друг друга знают, какой у кого характер, биография, у кого родственники в городе. Каждый человек тут яркая личность. Такая же ситуация в учебном классе. Но когда ты в огромном городе, где живут миллионы людей и толпы на улицах, то ценность человека просто теряется. Ты становишься каплей в океане.

Миф №7. Я сижу в социалках, чтобы общаться только со своими знакомыми и семьёй поделиться фотографиями из отпуска и т.п. На деле такие люди сами себя вводят в заблуждения. Да, у них может быть мало друзей-подписчиков, но при этом они также участвуют в виртуальной «жизни на показ», играя по правилам соц сети. Пытаясь поднять свой социальный статус, они из кожи вон лезут, чтобы показать себя харизматичными, позитивными, успешными. Остаётся только их сознание оцифровать и загрузить в тот же Инстаграм или ВК, в эту виртуальную выдуманную ими идеальную жизнь и виртуальные образы идеальных себя. Интернет-хвастуны проживают свою жизнь ради чужой зависти, это их еда психологическая. Крайне примитивный способ повысить самооценку.

Миф №8. Социальные сети — это свобода и независимость мнений.

Берегите своё психическое здоровье и держитесь подальше от социальных сетей, а если уж пользуетесь ими для нахождения какой-то информации или чтобы связаться с каким-то человеком, не позволяйте социальным сетям втягивать себя. Комментарии, пытающиеся навязать вам определённое мнение или вызвать злость, раздражение — просто игнорируйте. Представьте себе проплаченного агента, который их пишет и эмоции сразу отпустит. Детям и вовсе стоит запретить посещать социальные сети. Если на взрослых людей они действуют не лучшим образом, то на детскую несформировавшуюся психику воздействие может быть и вовсе разрушительным и катастрофическими.

СОВЕТЫ ПО БОРЬБЕ С ФИШИНГОМ



КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Обычной кражей денег и документов никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет и продолжают заниматься «любимым» делом. Так появилась новая угроза: интернет-мошенничества или фишинг (от английского слова - рыбная ловля), главная цель которого состоит в получении конфиденциальных данных пользователей - логинов и паролей.

- ✓ Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее.
- ✓ Используй безопасные веб-сайты, в том числе интернет-магазинов и поисковых систем.
- ✓ Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем.
- ✓ Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будут рассылаться спам и ссылки на фишинговые сайты.
- ✓ Установи надежный пароль (PIN) на мобильный телефон.
- ✓ Отключи сохранение пароля в браузере.
- ✓ Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

У всех фишеров одна единственная цель – сбор персональной и конфиденциальной информации и использование ее для получения материальной выгоды. Хотя фишеры стараются собирать различные типы информации в зависимости от способа атаки, реализуемой ими. К примеру, при простейшей форме фишинга злоумышленники в основном стремятся получить информацию о кредитной/дебетовой карт. В случае целевого фишинга (и охоте на высокопоставленных лиц) целью злоумышленников могут быть секретные правительственные документы, объекты интеллектуальной собственности фирмы, список клиентов или сотрудников; злоумышленник может быть членом конкурирующей компании или правительства или быть нанятым ими. Затем полученная информация может либо использоваться в злонамеренных целях, либо быть продана на черном рынке.

СОВЕТЫ ПО БОРЬБЕ С КИБЕРБУЛЛИНГОМ

На прошлой неделе я вышел пообедать. Какой-то парень остановил меня и попросил денег. Я не знал, что делать. Потом он сказал, что я должен побывать на его домашней странице, и дал мне свой URL (унифицированный указатель ресурса). Я не понял, правду он говорит или нет, но строка оказалась настолько хороша, что я дал ему пять долларов. Так что он, возможно, бездомный человек с домашней страницей в Интернете.»

Билл Гейтс

- ✓ Не бросайся в бой. Лучший способ: посоветоваться, как себя вести, и если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт.
- ✓ Управляй своей киберрепутацией.
- ✓ Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом.
- ✓ Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно. Соблюдай свою виртуальную честь смолоду.
- ✓ Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.
- ✓ Бань агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.
- ✓ Твои действия, если ты свидетель кибербуллинга: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.



КАК ЗАЩИТИТЬСЯ ОТ
КИБЕРБУЛЛИНГА

Кибербуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.



ПОЛЕЗНАЯ ИНФОРМАЦИЯ

На школьном сайте вы можете найти полезные ресурсы по безопасному использованию сети Интернет.



КАК ПОЛЬЗОВАТЬСЯ QR-КОДОМ НА ANDROID

Независимо от того, какое приложение вы установите на свой смартфон, алгоритм действий будет схожим:

- Установить и запустить приложение
- Навести объектив камеры на QR-код
- Дождаться, когда приложение распознает код
- Произвести действие, зашифрованное в коде