§ 5. Сетевой этикет и меры безопасности в сети Интернет

В Интернете часто используют специальные слова (сленг).

1. Для обозначения нарушений правил сетевого этикета:

Флейм (англ. *flame* — пламя) — неожиданно возникшее активное обсуждение, при развитии которого участники обычно забывают о первоначальной теме, переходят на личности и не могут остановиться.

Флуд (англ. *flood* — наводнение) — сообщения, не несущие никакой полезной информации. Флуд может распространяться с целью троллинга, т. е. из желания кому-либо досадить. Технический флуд представляет собой хакерскую атаку с большим количеством запросов, приводящую к отказу работы сервиса (DDoS-атака).

Спам (англ. *spam*) — сообщения, присылаемые от неизвестных людей или организаций без разрешения. Часто термин *спам* употребляется в значении *почтовый спам* — рассылка электронных писем, содержащих рекламу.

Оффтоп (англ. *off topic* — вне темы) — сетевое сообщение, не имеющее отношения к заранее установленной теме общения. Наиболее неодобряемой формой оффтопа являются рекламные сообщения.

Интернет — мир интересных и полезных возможностей, но в то же время это источник угроз, особенно для детей и молодежи. Агрессия, мошенничество, психологическое давление — опасности, которые могут поджидать в глобальной сети каждый день.

В 6-м классе вы познакомились с сетевым этикетом при работе с электронной почтой, узнали, какие меры безопасности необходимо соблюдать, пользуясь электронным почтовым ящиком. Работая с различными облачными сервисами или общаясь по сети, нужно соблюдать такие же правила, как и при работе с электронной почтой.

Обезличенность при общении в Интернете заставляет пользователей забывать, что они имеют дело не с машиной, а с реальными людьми. Правила сетевого этикета помогают достичь взаимопонимания и обеспечивают безопасность общения. Основные из них:

1. Будьте вежливы и не забывайте об обязательных формулах приветствия, обращения, благодарности.

2. Избегайте бессодержательных бесед, чтобы не тратить свое время и время собеседника.

3. Пишите грамотно. Используйте проверку орфографии. Перед отправкой сообщения перечитайте текст.

4. Без необходимости не пишите на транслите (т. е. не злоупотребляйте использованием букв алфавита другого языка). Не набирайте текст заглавными буквами. Не перегружайте сообщение смайликами.

5. Сохраняйте анонимность при общении с незнакомцами.

Неосмотрительность и халатный подход к обеспечению безопасности в Интернете могут дать возможность преступникам совершить противоправные действия. Сначала преступник получает несанкционированный доступ к учетным записям в социальных сетях, к электронному почтовому ящику, к аккаунтам и др. Получив реквизиты, злоумышленник заходит в учетную запись и осуществляет рассылку контактам владельца взломанной учетной записи сообщения мошеннического характера.

Рекомендации, которые помогут снизить вероятность совершения противоправных действий в Интернете:

1. Для выхода в сеть Интернет используйте устройства, на которых установлены и постоянно обновляются антивирусные программы.

2. При посещении известных сайтов обращайте внимание на их внешний вид: возможно, это поддельная копия.

3. Вводите личную информацию только на веб-сайтах, которые работают с использованием защищенных

Хотлинк (англ. *hotlink*) — включение в веб-страницу файлов-изображений или других ресурсов с чужого сервера. Этот прием используется недобросовестными веб-мастерами. При этом расходуются чужие ресурсы и трафик.

Оверквотинг (англ. *overquoting*) — избыточное цитирование.

2. Для обозначения противоправных действий в Интернете:

Фишинг (англ. *phishing* — *password* + + *fishing* — выуживание паролей) — вид мошенничества с целью получения доступа к логинам и паролям пользователей.

Кибersквоттинг (англ. *cybersquatting*) — регистрация доменных имен, содержащих торговую марку, принадлежащую другому лицу, с целью их дальнейшей перепродажи или недобросовестного использования.

Брутфорс (от англ. *brute force* — полный перебор) — метод атаки или взлома путем перебора всех возможных вариантов пароля.

Кардинг (от англ. *carding*) — вид мошенничества с использованием чужой платежной карты или ее реквизитов.

Кликджекинг (англ. *clickjacking*) — механизм обмана пользователей Интернета, позволяющий узнать контакты посетителей сайта еще до того, как они сами разместили их на сайте.

Руткит (англ. *rootkit*) — программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.

Фарминг (англ. *pharming*) — скрытое перенаправление на ложный IP-адрес.

Примеры мошенничества в Интернете:

1. Производится вирусная атака на компьютерные устройства, блокируется браузер или операционная система, а на экране монитора появляется требование оплатить крупный штраф.

2. На электронный почтовый ящик приходит письмо, которое обещает: после покупки обучающего курса можно уже завтра начинать зарабатывать огромные деньги. Помните, что никто не будет рассказывать совершенно незнакомым людям, как заработать огромные деньги, мошенники просто зарабатывают деньги на продаже этих обучающих курсов.

Пример 5.1. Статьи Уголовного кодекса Республики Беларусь, определяющие ответственность за преступления в сети Интернет (http://kodeksy.by).

Статья 212. Хищение путем использования компьютерной техники.

Статья 349. Несанкционированный доступ к компьютерной информации.

Статья 350. Модификация компьютерной информации.

Статья 351. Компьютерный саботаж.

Статья 352. Неправомерное завладение компьютерной информацией.

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети.

Статья 354. Разработка, использование либо распространение вредоносных программ.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети.

Анализ 3 млн созданных людьми восьмизначных паролей показал, что буква «e» была использована в паролях 1,5 млн раз, в то время как буква «f» — только 250 000 раз.

Ресурс для проверки уникальности пароля: https://exploit.in/passcheck

протоколов (в браузере рядом с адресом такого сайта отображается значок замка).

4. Не используйте одинаковые логины и пароли на различных сайтах.

5. Не используйте легкие пароли (даты рождения, номера телефонов и т. д.).

6. Остерегайтесь неожиданных или необычных электронных сообщений, даже если вам знаком отправитель; не открывайте вложения и не переходите по ссылкам в таких сообщениях.

7. При поступлении сообщений от знакомых, содержащих просьбы о финансовых операциях или о передаче финансовых реквизитов, обязательно проверяйте данную информацию по другим каналам связи (личная встреча, телефонный звонок, голосовая связь). Постарайтесь установить личность собеседника с помощью контрольных вопросов, ответы на которые могут быть известны только вам двоим.

Законодательством Республики Беларусь определена мера ответственности за следующие преступления в сети Интернет:

1. Несанкционированный доступ к данным.

2. Модификация (изменение) данных без разрешения владельца.

3. Умышленное уничтожение данных, приведение их в непригодное состояние.

4. Разработка, использование и распространение вредоносных программ.

5. Нарушение авторского права.

(Рассмотрите пример 5.1.)

1. Почему нужно соблюдать правила этикета при общении в сети Интернет?
2. Какие правила сетевого этикета не соблюдаются в приведенных ниже сообщениях?

Сегодня четверг. Это хуже, чем суббота, но гораздо лучше, чем понедельник... Но немного хуже, чем пятница. Зато четверг лучше, чем среда. Четверг даже лучше, чем воскресенье, потому что в воскресенье завтра понедельник, а в четверг завтра пятница...

Смайлы 😀😀😀 — это очень удобно 🤗🤗. Но в то же время у них есть обратная сторона 😟. Они берегут эту тайну 🤫🤐. И никто не должен знать о ней 🤐🤫. НИКТО! 🤫🤫🤫

нАриСуй Мне:
1) УвАжАеШь — рОзоВыЙ фОн;
2) ОбИдЕлся — КоричНевЫй фОн;
3) дружИшЬ — бЕлЫй фОн.
рАзошлИ Это Всем СвОим дРуЗьяМ, И тВоя СтЕнА бУдЕт СупеРКрАсИвая.

3. Какие меры необходимо предпринять, чтобы обезопасить свои учетные записи от действий мошенников?
4. Каким должен быть безопасный пароль?
5. Какие действия в сети Интернет определены законодательством Республики Беларусь как противоправные?

Упражнения

1 Приведите примеры, когда соблюдаются и не соблюдаются правила сетевого этикета. Сделайте вывод.

2 Выберите из таблицы небезопасные пароли.

sdfghjkl	password	qS8+njiPh	12345678	Yn2004

Создайте текстовый документ, содержащий пояснение вашего выбора для каждого пароля.

3 Подготовьте презентацию на тему «Сетевой этикет».

4 С помощью сервиса Google **Формы** создайте анкету на тему «Безопасность в сети Интернет».