РОСКОМНАДЗОР

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО ПРИМОРСКОМУ КРАЮ
(Управление Роскомнадзора по Приморскому краю)

юр .адрес: Беломорская ул., д.18, г. Владивосток, 690041
почтовый адрес: а/я 2210, г. Владивосток, 690022
приемная: (423) 239 08 11; факс: (423) 237 50 46
E-mail: rsockanc25@rkn.gov.ru

22.04.2020 № 5842-01/25

На

Об оказании содействия

Министерство образования Приморского края

Заместителю председателя Правительства Приморского края – министру образования Приморского края

Бондаренко Наталье Валерьевне

education2006@primorsky.ru

Уважаемая Наталья Валерьевна!

В соответствии с законодательством Российской Федерации Уполномоченным органом по защите прав субъектов персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

На территории Приморского края Уполномоченным органом является Управление Роскомнадзора по Приморскому краю.

В целях популяризации защиты прав субъектов персональных данных среди несовершеннолетних прошу рассмотреть возможность распространения методического материала Роскомнадзора о необходимости бережного отношения к своим персональным данным среди несовершеннолетних при проведении дистанционных уроков в образовательных учреждениях Приморского края и ссылки на портал «Персональные данные.дети» (персональныеданные.дети/zadaniya) на котором размещен тест направленный на изучение вопросов, связанных с защитой прав субъектов персональных данных, а также размещения методического материала на сайте Министерства образования Приморского края.

Методический материал для направления в образовательные учреждения общего и среднего образования, детские учреждения дополнительного образования для организации и проведения цикла дистанционных уроков по тематике защиты персональных данных содержит:

1. Учебно-методическое пособие, разработанное Федеральным институтом развития образования «Практическая психология безопасности: управление персональными данными в Интернете».

2. Презентации на темы «Персональные данные и Интернет», «Защита персональных данных несовершеннолетних» с сопровождающими текстовыми файлами.

3. Ссылки на скачивание социальных роликов посвященных защите персональных данных: **https://yadi.sk/i/C4CvJAXW3Vy7Er, https://yadi.sk/i/42FUFlvD3Vy7G7, https://yadi.sk/i/1NCx75Wv3YMn75.**

4. Буклеты «Правила общения в сети Интернет».

5. Тест для детей.

Информацию о принятом решении и сроках размещения методического материала прошу сообщить на электронный адрес: rsockanc25@rkn.gov.ru.

Приложение: Ссылки на информационный материал, в формате «.doc», 1 файл.

Руководитель

Документ подписан электронной подписью в системе электронного документооборота Роскомнадзора

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат	1d5cf3c33bb06a00000000329920003
Владелец	Шутов Эдуард Юрьевич
Действителен	с 20.01.2020 по 20.01.2021

Э. Ю. Шутов

Исполнитель: Пикула Т. А.
Тел.: (423) 2390822 доб. 140

Персональные данные и Интернет

Что такое «Персональные данные»?

ЧТО ТЫ ЗНАЕШЬ О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ?

ИНФОРМАЦИЯ

Общие персональные данные

- - ФИО,
- - адрес,
- - дата рождения,
- - место рождения,
- - номер телефона,
- - адрес электронной почты,
- - фотография,
- - возраст и т. д.

ОСТОРОЖНО БОТЫ!

- Мошенники;
- "Big Data«;
- Агрегаторы рекламы.

Как защитить свои данные от злоумышленников в сети

- Эффективное антивирусное программное обеспечение;
- Блокировщики скриптов для вашего браузера;
- Не отправлять друзьям, коллегам, даже членам семьи компрометирующую или частную информацию;
- Создайте электронные адреса, не привязанные ни к одной социальной сети или сайту и используйте только их для денежных операций и привязки к интернет-банкам .

- Не сообщайте критически важную информацию в интернете;
- Не "ведитесь" на предложения о «халяве и быстром заработке»;
- Вводите адрес сайта вручную (защита от фишинга);
- Вводите данные только на сайтах с протоколом **https:** (защищенный протокол);
- Проверяйте наличие сертификата и политику конфиденциальности веб-сайта.

Данные с вашего устройства

Как защитить информацию

- ✓ ИСПОЛЬЗУЙТЕ АНТИВИРУС
- ✓ НЕ ХРАНИТЕ ПАРОЛИ
- ✓ ДЕЛАЙТЕ РЕЗЕРВНЫЕ КОПИИ
- ✓ ИСПОЛЬЗУЙТЕ СЛОЖНЫЕ ПАРОЛИ
- ✓ НЕ ОТПРАВЛЯЙТЕ СВОИ ДАННЫЕ НЕЗНАКОМЦАМ

ПРОСТЫЕ ПРАВИЛА

Простые правила

- Установите пин-код или пароль;
- Включите шифрование данных на устройстве;
- Не устанавливайте сомнительные приложения;
- Не сообщайте ваши платежные данные по телефону или в переписке.

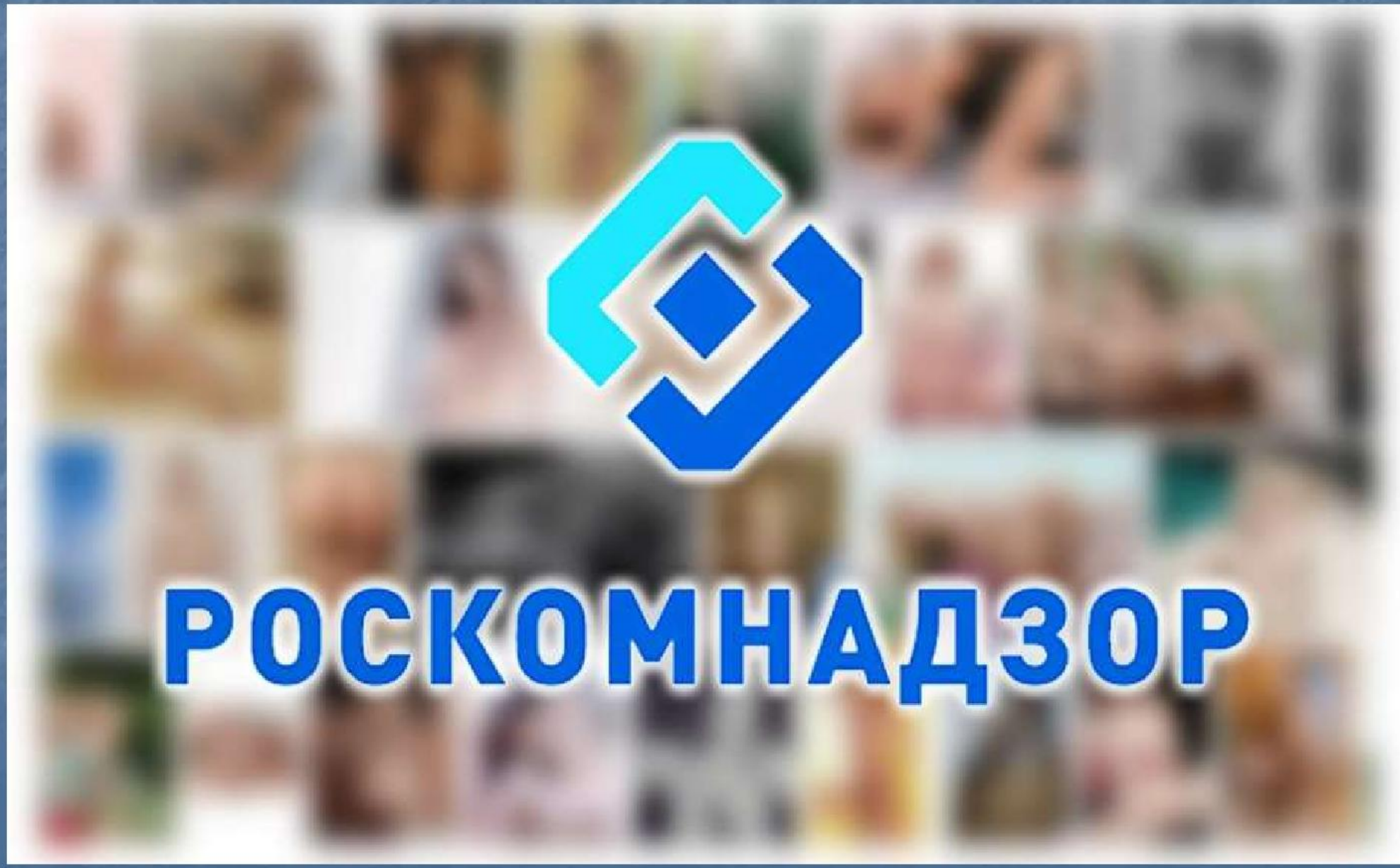
МИФЫ о безопасности в Интернете

Миф 1: Использование режима «инкогнито» в браузере может защитить меня.

Миф 2: Анонимности можно добиться при помощи продвинутых мер.

Миф 3: Письма, которые я отправляю и получаю, видны только мне и собеседнику.

Благодарим за внимание!



1. **Буклет для подростков**

https://yadi.sk/i/jsnpmpVsEoteEg

2. **Буклет детский**

https://yadi.sk/i/KwzObohYtVZCJw

3. **Презентация «Защита ПД несовершеннолетних»**

https://yadi.sk/i/BXx4seIYoZH74A

4. **Текст к презентации «Защита ПД несовершеннолетних»**

https://yadi.sk/i/HEU2FD9s2CxdBQ

5. **Презентация «Персональные данные и Интернет1»**

https://yadi.sk/i/XqwWt7ARjX6IIQ

6. **Текст к презентации «Персональные данные и Интернет1»**

https://yadi.sk/i/zSFNE83M2ORYFg

7. **Детский ролик о защите ПД**

https://yadi.sk/i/ps_WvvNCtecHaw

8. **Ролик «Персональные данные и дети»**

https://yadi.sk/i/cXJJPZuNOcc66A

9. **Социальный ролик**

https://yadi.sk/i/Gh-4324kN49LAQ

10. **Учебно-методическое пособие «Практическая психология безопасности»**

https://yadi.sk/i/3YU3cZVswr9LTw

Здравствуйте, дети!

Сегодня реальность во многом заменяется виртуальным миром. Мы знакомимся, общаемся и играем в Интернете; у нас есть друзья, с которыми в настоящей жизни мы никогда не встречались, но доверяемся таким людям больше, чем близким. Мы создаем своего виртуального (информационного) прототипа на страничках в социальных сетях, выкладывая информацию о себе.

Используя электронное пространство, мы полагаем, что это безопасно, потому что мы делимся всего лишь информацией о себе и к нашей обычной жизни вроде бы это не относится.

Но на самом деле границы между абстрактной категорией «информация» и реальным человеком носителем этой информации стираются.

Информация о человеке, его персональные данные сегодня превратились в дорогой товар, который используется по-разному:

- кто-то использует эти данные для того, чтобы при помощи рекламы продать вам какую-то вещь;
- кому-то вы просто не нравитесь, и в Интернете вас могут пытаться оскорбить, очернить, выставить вас в дурном свете, создать плохую репутацию и сделать изгоем в обществе;
- с помощью ваших персональных данных мошенники, воры, могут украсть ваши деньги, шантажировать вас и заставлять совершать какие-то действия;
- и многое другое.

Поэтому защита личной информации может приравниваться к защите реальной личности. И важно в первую очередь научиться правильно, безопасно обращаться со своими персональными данными.

Никому и никогда не разглашай свои пароли. Они – твой главный секрет. Придумай свой уникальный пароль, о котором никто не сможет догадаться. Не записывай пароли на бумажках, не храни их в открытом доступе. Не отправляй свои пароли по электронной почте.

При регистрации на сайтах и в социальных сетях старайся не указывать личную информацию (номер телефона, адрес места жительства, школы,

место работы родителей и другое) – она может быть доступна всем, даже тем, кого ты не знаешь!

Помни, что фотография, размещенная в Интернете доступна для просмотра всем. Старайся не размещать фото, на которых изображена твоя семья, школа, дом и другие личные данные.

Старайся не встречаться с теми, с кем ты знакомишься в Интернете.

Помни, что многие люди рассказывают о себе в Интернете неправду.

В Интернете и социальных сетях старайся общаться только с теми, с кем ты лично знаком. Подумай и посоветуйся с родителями, прежде чем добавить незнакомого человека к себе в список «друзей».

Не используй веб-камеру при общении с незнакомыми людьми, помни о необходимости сохранять дистанцию с незнакомыми людьми.

Уважай собеседников в Интернете. Никогда и ни при каких обстоятельствах не угрожай другим, не размещай агрессивный и провокационный материал. Будь дружелюбен. Не груби.

Помни, что даже в Интернете существует «сетевой этикет». Если ты пишешь сообщение заглавными буквами, то собеседник может подумать, что ты кричишь на него.

Не вступай в незнакомые сообщества и не распространяй по чей-либо просьбе информационные, провокационные и агрессивно-настроенные материалы и сообщения.

Не все, что ты можешь прочесть или увидеть в интернете - правда. Не ленись и перепроверяй информацию в других поисковиках или спроси у родителей.

Помни, что существуют сайты, непредназначенные для детей, не заходи на сайты «для тех, кто старше 18 лет», на неприличные и агрессивно настроенные сайты. Если ты попал на такой сайт по ссылке, закрой свой браузер, используя клавиши “ctrl+alt+delete”.

Расскажи все, что ты увидел, выучил или узнал нового взрослому.

Ни в коем случае не указывай свой номер телефона или электронный адрес, не отправляй с него смс на незнакомые номера в Интернете.

Если тебе пришло сообщение с незнакомого адреса, его лучше не открывать.

Если тебе показалось, что твои друзья отправляют тебе «странную» информацию или программы, переспроси у них, отправляли ли они тебе какие-либо файлы. Иногда мошенники могут действовать от имени чужих людей.

Если ты хочешь купить в Интернете какую-либо услугу или игру, обратись к взрослому. Он подскажет тебе, как избежать мошенничества.

Не загружай файлы, программы или музыку без согласия взрослых – они могут содержать вирусы и причинят вред компьютеру.

Попроси родителей установить на компьютер антивирус и специальное программное обеспечение, которое будет блокировать распространение вирусов.

Спасибо за внимание.

1 СЛАЙД

Сегодня мы проводим ознакомительное занятие, посвященное вопросам защиты персональных данных.

2 СЛАЙД

Прежде всего, хочу задать вопрос, знаете ли вы, что такое персональные данные? (ответы)

Персональные данные представляют собой информацию о конкретном человеке. Это те данные, которые позволяют нам узнать человека в толпе, идентифицировать его и определить, как конкретную личность.

3 СЛАЙД

Так если мы кому-то скажем, свои ФИО и адрес места жительства, то нас вполне можно опознать, как конкретное лицо. Но если мы исключим из этого набора данных Фамилию или адрес, то понять, о каком человеке идет речь будет практически невозможно.

4 СЛАЙД

Наша личная информация — лакомый кусок для рекламных компаний и злоумышленников, и они идут на множество уловок, чтобы их заполучить. Мы подробно разберём, как не стать жертвой злоумышленников или целью спам ботов всех мастей.

5 СЛАЙД

- На первом месте, конечно же, мошенники. Получив доступ к данным в вашем компьютере или смартфоне, они с лёгкостью смогут увести ваши деньги или продать вашу личную информацию.

- Они нужны банкам. Наверное, уже все слышали о таком понятии, как "Big Data". Упрощенно, это использование огромных объемов информации о каждом из нас, чтобы принять решение, например, о выдаче кредита или о добавлении вашего номера телефона в список для оповещения о новом продукте.

- Агрегаторы рекламы. Именно благодаря этим ребятам, поискав пылесос, вы натыкаетесь на пылесосы повсюду. Им очень хочется знать обо всех событиях в вашей жизни. Ведь на каждое у них есть для вас товар или услуга.

Какого типа данные имеются в виду?

Совешенно любые: от адреса проживания и номера телефона до цвета штор в вашей комнате.

Но самый лакомый кусок - это личные данные в ваших устройствах (смартфоне и компьютере), а так же ваших облачных хранилищах (dropbox, one drive, google drive и т. д.).

Защититься от банков и агрегаторов довольно просто. Достаточно не оставлять на всех подряд сайтах и не указывать в соцсетях личную информацию, которая может быть использована против вас, не комментировать и не лайкать сообщения, которые могут быть сочтены экстремистскими, делиться событиями из своей жизни с группой проверенных друзей, а не со всем миром).

6 СЛАЙД

Как защитить свои данные от злоумышленников в сети

Защищаемся от троянов

иногда по незнанию или невнимательности мы загружаем файлы (Трояны), которые открывают путь ко всем данным, хранящимся на устройстве. Классический случай - трояны, приходящие ссылками на электронную почту или в сообщениях в соцсетях.

Как защитится от троянов

-Эффективное антивирусное программное обеспечение.

-Блокировщики скриптов для вашего браузера. Например: Noscript для Firefox и ScriptSafe для Chrome. Блокировщики Popup всплывающих уведомлений.

Защищаемся от самого себя

Большую часть информации, присутствующей в открытом доступе, мы оставляем сами — в социальных сетях, мессенджерах и т.д., все это помогает киберпреступникам в достижении их целей.

Особенно злоумышленники любят сайты знакомств, где легче всего узнать о вас самую интересную информацию.

Ещё крайне важно не отправлять вашим друзьям, коллегам, даже членам семьи компрометирующую или частную информацию. Важно помнить, что ваши отношения могут поменяться и ваши интимные данные окажутся у всех на виду.

В это трудно поверить, так как от родных и друзей не принято ждать подвохов, но даже наделавшая немало шума история последних дней с известной в геймерских кругах стримершей Кариной случилась именно из-за такой доверчивости.

(Пользователь имиджборда «Двач» опубликовал в одном из тредов серию фотографий интимного характера, которые, как утверждается, принадлежат Карине Сычевой, более известной как стримерша Карина. Карина Сычева, или стримерша Карина, приобрела популярность в сети в конце 2015 года. Девушка играла в онлайн-игры и транслировала это в прямом эфире с помощью сервиса Twitch. Во время трансляций девушка представала в весьма откровенных нарядах и запомнилась юзерам эпатажным поведением в кадре.)

Как защититься:

Создайте электронные адреса, не привязанные ни к одной социальной сети или сайту и используйте только их для денежных операций и привязки к интернет-банкам.

Не сообщайте критически важную информацию в интернете. Не "ведитесь" на предложения о "халяве и быстром заработке" или увеличении чего-либо, присланные на вашу почту, особенно попавшие в папку спам.

7,8 СЛАЙД

Фишинг

Нас ловят на точные копии любимых нами сайтов и сервисов, чаще всего таких, где требуется ввод конфиденциальных данных, например номера и CSV-коды кредитных карт.

Как защитится:

Внимательно смотрите на строку адреса сайта, на котором вы решили вводить свои данные. Злоумышленники часто используют похожие до степени смешения названия или меняют схожие по написанию буквы в адресах.

Самое надежное решение для защиты от фишинга - ввести адрес сайта вручную.

Вводите данные только на сайтах с протоколом https: (защищенный протокол). Его наличие гарантирует, что любые введенные данные шифруются и их почти невозможно перехватить.

До передачи личной или финансовой информации проверьте наличие сертификата и политику конфиденциальности веб-сайта.

9 СЛАЙД

Данные с вашего устройства

Вы часто оставляете без присмотра ваш ноутбук или телефон. Или ещё хуже вы его теряете. Злоумышленники не преминут заглянуть в оставленное без присмотра устройство и, если на нем нет пароля, смогут без труда получить все интересующие их данные.

Как защититься:

Установите пин-код или лучше пароль на ваше устройство. Также можно разблокировать устройство по отпечатку пальца или лицу.

В пин-коде используются только цифры, обычно их 4. В пароле любые символы в любом количестве. Подобрать пин-код реально. Пароль же практически не подбирается.

Включите шифрование данных на вашем устройстве на Android (на смартфонах от компании Apple она включена по умолчанию).

Не устанавливайте сомнительные приложения не из официального магазина приложений. Многие устройства автоматически синхронизируют все фото в облачные хранилища и, если вы не хотите, чтобы эти фото увидел весь мир, позаботьтесь о сложном пароле или внимательно проверьте, что автосинхронизация отключена.

10 СЛАЙД

Социальная инженерия

Это самый сложный и одновременно эффективный способ получить ваши данные.

При этом "взламывают" вас, а не ваше устройство. С её помощью особо изощренные преступники могут выманить ваши данные, притворившись, например сотрудником вашего банка или покупателем вашего товара.

Самое опасное, что, делясь своими данными в соцсетях, мы сами помогаем преступникам подобрать к нам ключи.

Как защититься:

Самый простой способ - это не сообщать ваши платежные данные по телефону или в переписке. Ни вашему банку, ни офицеру ФСБ не нужны ваши данные для их работы.

11 СЛАЙД

5 мифов о безопасности в интернете, с которыми давно пора расстаться

Миф 1: использование режима инкогнито в браузере может защитить меня.

12 СЛАЙД

Независимо от того, какой браузер вы используете, он не скроет ваши действия от интернет-провайдера, сайтов и правоохранительных органов, которые следят за вашей деятельностью.

Миф 2: Анонимности можно добиться при помощи продвинутых мер.

13 СЛАЙД

Даже использование Tor или VPN не дает вам полной анонимности, поскольку каждая служба использует какой-либо идентификатор, чтобы отличать вас от других пользователей. Даже VPN-провайдеры, которые рекламируют анонимные службы, могут регистрировать ваше имя, IP-адрес и другие сведения о вас. Идентификатор может не раскрывать вашего реального имени, но он все равно является частью информации, которая в связи с другими данными поможет при необходимости идентифицировать вас.

14 СЛАЙД

Миф 3: письма, которые я отправляю и получаю, видны только мне и собеседнику.

В большинстве случаев, когда вы отправляете сообщение по электронной почте или в социальной сети, оно не видно никому, кроме отправителя и получателя. Но иногда нарушения в системе безопасности могут сделать конфиденциальную переписку общедоступной. Кроме того, правительственные агентства могут без особого труда получить доступ к вашей электронной почте. Закон гласит, что при наличии ордера или распоряжения суда спецслужбы могут получить доступ к электронным письмам, хранящимся на сервере интернет-провайдера или почтового клиента.

15 СЛАЙД

Также в целях просвещения населения Роскомнадзор создал 2 социальных ролика о персональных данных.

Подытоживая свое выступление, отмечу, что всегда нужно помнить, о злоумышленниках, которые имея свободный доступ к информации о социальном статусе, семейном положении, могут воспользоваться ситуацией и совершить неправомерные посягательства на частную жизнь семьи, здоровье и половую неприкосновенность Вашу, а так же Ваших несовершеннолетних родственников.

Мы видим свою задачу помочь, научиться понимать последствия своих действий в Интернете, научить правилам безопасности, которые им следует соблюдать и сейчас, и на протяжении всей жизни.

Для этого Роскомнадзор ведет информационно-развлекательный сайт для детей и подростков Персональныйданные.дети., направленный на изучение вопросов, связанных с защитой прав субъектов персональных данных. Если у Вас есть несовершеннолетние родственники, братья, сестры, племянники, да и просто знакомые, Вы можете смело ознакомить их с этим сайтом.

ТЕСТ

«Что ты знаешь о персональных данных?»

1. Персональные данные состоят из

- ФИО, возраст, домашний адрес и номер телефона
- Группа крови, отпечатки пальцев, медицинские диагнозы
- Сведения об образовании, фотографии
- Все вышеперечисленное. Персональные данные - это информация, по которой тебя можно идентифицировать.

Правильный ответ: Все вышеперечисленное.

Перечень данных, который можно отнести к персональным, четко не определен в законах. Поэтому набор данных, позволяющий определить или идентифицировать тебя среди множества других людей, является персональными.

2. Можешь ли ты контролировать размещение своих фотографий в сети Интернет, если выкладываешь их в социальные сети?

- Да
- Нет

Правильный ответ: Нет, не правильно.

Доступ неограниченного круга лиц к такой информации может повлиять на Вашу личную безопасность и безопасность Ваших друзей, родных и знакомых. Вы не можете быть уверены в том, что эти сведения не будут использованы против Вас.

3. Друг устраивает вечеринку в выходные, и все ваши друзья приглашены. Правильно ли будет разместить дату, время и место на сайте, потому что тогда у каждого будут детали этой встречи.

- Да
- Нет

Правильный ответ: Сначала подумаете, будете ли Вы чувствовать себя комфортно, если другие увидят Вашу публикацию.

Информация о Вас в Интернете помогает людям составить о Вас свое впечатление, о Вашей личности и о том, как Вы ведете себя в реальной жизни, влияет на Вашу репутацию. Эта информация доступна для Ваших учителей, родителей, друзей. Поэтому нужно задуматься, готовы ли Вы открыть для всех информацию о своей частной жизни/. Ты никогда не можешь знать точно, кто имеет доступ к информации, которую публикуешь на сайте. То, что ты разместишь на сайте, может повлиять на твою личную безопасность - особенно, если говоришь людям, где собираешься быть в определенное время.

4. Какие файлы ты разместишь в социальных сетях?

- Все, что захочу, это смешно и интересно – моим друзьям понравится!
- Сначала подумаю. Буду ли я чувствовать себя комфортно, если родители, учителя увидят то, что я публикую?
- Фотографии, ФИО, адрес

Правильный ответ: Сначала подумаете, будете ли Вы чувствовать себя комфортно, если другие увидят Вашу публикацию.

Информация о Вас в Интернете помогает людям составить о Вас свое впечатление, о Вашей личности и о том, как Вы ведете себя в реальной жизни, влияет на Вашу репутацию. Эта информация доступна для Ваших учителей, родителей, друзей. Поэтому нужно задуматься, готовы ли Вы открыть для всех информацию о своей частной жизни.

5. Может ли твой друг заходить в твой аккаунт и отправлять от твоего имени сообщения?

- Да, потому что он мой друг, и я ему доверяю
- Нет. Имея доступ к твоему аккаунту, друг может иметь доступ не только к тем файлам, которые ты разрешил смотреть, но и ко всем остальным данным.

Правильный ответ: Нет, не может.

Данные, которые содержатся в Вашем аккаунте – это Ваше личное пространство, которое содержит огромное количество не только данных о Вас, но и тех людей, с которыми Вы общаетесь. Предоставив кому-то доступ к своему аккаунту, Вы даете возможность другу не только посмотреть какой-то конкретный файл, но также доступ ко всей информации из Вашего аккаунта.

6. При заполнении онлайн-формы для ввода данных, которые будут опубликованы, какие данные не стоит указывать?

- ☐ Никнэйм или псевдоним
- ☐ ФИО
- ☐ Адрес, где ты живешь
- ☐ Адрес, где ты учишься

* - Допускается несколько вариантов ответа

Правильный ответ: ФИО; адрес, где Вы живете.

Эти данные позволяют установить Вашу личность в реальной жизни и дают возможность для вторжения в Ваше личное пространство, а также для использования Вас как объекта навязчивой рекламы или противоправных действий

7. Какие последствия могут наступить, если ты отметишь друга на фото

- ○ Массовое распространение фотографии в сети, если не настроена приватность учетной записи
- ○ Никаких последствий не будет
- ○ Ничего не случится, мой друг просто станет популярнее

Правильный ответ: Массовое распространение фотографии в сети, если не настроена приватность учетной записи.

Вы никогда не узнаете точно, кто имеет доступ к такой информации. Более того, вполне возможно, что Ваш друг не хочет, чтобы фотография, на которой Вы его отметили, увидели другие люди.

8. Если у тебя есть сомнения, дать ли людям, с которыми общаешься в сети больше личной информации о себе, что ты сделаешь

- ☐ Расскажешь взрослому и попросишь совет
- ☐ Расскажешь другу (подруге) и попросишь совет
- ☐ Отправишь личные данные и посмотришь, что будет
- ☐ Не отправишь личные данные

* - Допускается несколько вариантов ответа

Правильный ответ: Расскажешь взрослому и попросишь совет; Не отдашь личные данные.

Не стоит сообщать незнакомым людям в сети много информации о себе. Вы не можете точно знать, что за человек с Вами общается в Интернете и как он будет использовать Ваши персональные данные. Старайтесь советоваться со взрослыми, как Вам лучше поступить в таком случае.»

Типовая программа проведения внеклассных уроков

1) Проведение урока на основе презентаций;
2) Проведение тестирования для закрепления озвученных уроков;
3) Трансляция роликов на тему защиты персональных данных несовершеннолетних,
4) Ознакомление с Интернет-порталом «Персональныеданные.дети».

ФЕДЕРАЛЬНЫЙ ИНСТИТУТ РАЗВИТИЯ ОБРАЗОВАНИЯ

ФОНД РАЗВИТИЯ ИНТЕРНЕТ

КООРДИНАЦИОННЫЙ ЦЕНТР
НАЦИОНАЛЬНОГО ДОМЕНА СЕТИ ИНТЕРНЕТ

Солдатова Г.У., Приезжева А.А.,
Олькина О.И., Шляпников В.Н.

ПРАКТИЧЕСКАЯ ПСИХОЛОГИЯ БЕЗОПАСНОСТИ: УПРАВЛЕНИЕ ПЕРСОНАЛЬНЫМИ ДАННЫМИ В ИНТЕРНЕТЕ

Учебно-методическое пособие
для работников системы общего образования

2-е издание,
исправленное и дополненное

Одобрено экспертным советом Федерального государственного
автономного учреждения «Федеральный институт развития образования»
по образованию и социализации детей
(регистрационный номер рецензии № 499 от 14.12.2015 г.)

генезис

МОСКВА
2017

УДК 004.056
ББК 88.5
П 692

Автор вступительной статьи: *А.А. Воробьев*

Рецензенты:

Карабанова О.А., доктор психологических наук, профессор, зав. кафедрой возрастной психологии факультета психологии МГУ имени М.В. Ломоносова;

Марчак И.С., руководитель проектного офиса «Школа новых технологий» Департамента информационных технологий г. Москвы

П 692 Практическая психология безопасности. Управление персональными данными в интернете: учеб.-метод. пособие для работников системы общего образования / Г.У. Солдатова, А.А. Приезжева, О.И. Олькина, В.Н. Шляпников. — М.: Генезис, 2017. — 224 с.

ISBN 978-5-98563-464-8

Пособие посвящено решению актуальной задачи: повышению цифровой компетентности школьников и учителей в сфере управления персональными данными в интернете. Проанализированы теоретические и методические аспекты проблемы приватности и персональных данных. Практикум разработан для учащихся 6–10-х классов общеобразовательных школ в соответствии с принципами культурно-деятельностного подхода в психологии и педагогике. Материалы к урокам подготовлены с учетом действующего законодательства РФ, а также мирового опыта управления персональными данными в интернете.

Пособие адресовано учителям, классным руководителям, педагогам-психологам, библиотекарям, специалистам по информатизации учебного процесса, руководителям образовательных учреждений, а также руководителям и экспертам органов управления образованием, специалистам в области медиаобразования, работникам системы дополнительного профессионального образования учителей, студентам и аспирантам педагогических вузов.

УДК 004.056
ББК 88.5

ISBN 978-5-98563-464-8

СОДЕРЖАНИЕ

ДЕТИ В ИНТЕРНЕТЕ

Предупрежден — значит вооружен

Одно из неотъемлемых прав каждого интернет-пользователя — право на защиту персональных данных. Сбор, использование и хранение личной информации должны производиться на основе прозрачной политики конфиденциальности: оператор персональных данных (например, любой государственный орган) обязан запрашивать согласие пользователя на их обработку, то есть сообщать о содержании и целях поиска и изменения таких данных, а также о местах их хранения и механизмах доступа. Так интернет-пользователь получает право удалить свою личную информацию, а также контролировать порядок использования и степень доступа к ней.

По данным ряда опросов, больше половины россиян не знают о своих правах в интернете. И в целом по стране индекс цифровой грамотности в области безопасного использования информационных технологий остается довольно низким — 4,86 (из 10 возможных). Результаты исследования Регионального общественного Центра интернет-технологий (РОЦИТ) и Всероссийского центра изучения общественного мнения (ВЦИОМ), проведенного в 2015 году (www.mindex.rocit.ru), свидетельствуют о том, что лишь четверть пользователей Рунета ощущают себя полностью уверенными в вопросах защиты собственных персональных данных, то есть знают об основных способах сохранения конфиденциальности и применяют их на практике.

Нет среди россиян и точного понимания того, что такое «персональные данные». Большинство считает, что это рек-

визиты паспорта и банковского счета — такие ответы дают 80% опрошенных. Очевидно, что пользователи Рунета нуждаются в ликбезе: в разъяснении понятия «персональные данные», основ их защиты в сети и необходимости соблюдения конфиденциальности при использовании информационных технологий. Процесс просвещения, несомненно, покажет наибольшую эффективность, если проводить его комплексно, охватив основные группы пользователей: детей, их родителей и, конечно, педагогов.

Информация о частной жизни появляется в интернете разными путями: ее выкладывают сами пользователи, их друзья, родители. Немалая часть персональных данных школьников оказывается в сети в результате неправильного обращения с ними в образовательных учреждениях. Педагоги, активно используя возможности информационных технологий в процессе обучения (например, электронные дневники и журналы, персональные методические блоги и школьные сайты, электронную почту и социальные сети), работают с огромным количеством персональных данных детей, однако не всегда способны организовать их обработку и хранение должным образом.

Таким образом, стремительное развитие интернета и IT-сервисов, работающих с использованием персональных данных, привело к появлению одного из главных рисков современного информационного общества — потере приватности. Среди экспертов в области информационных технологий бытует мнение, что, при сохранении тенденций и темпов развития интернета, уже в недалеком будущем частная жизнь станет прозрачной и публичной «по умолчанию» — персональную информацию будет невозможно не открыть государству или корпорациям, а справляться с вопросами ее безопасности будет все сложнее.

Именно поэтому важно привлечь внимание общественности к проблемам и последствиям ненадлежащей обработки персональ-

ных данных и широкого распространения личной информации в сети, а также продолжить активную информационно-просветительскую работу в области интернет-безопасности и защиты персональных данных. Продолжить, потому что отдельные попытки обратить внимание детей и взрослых, педагогов, СМИ и IT-специалистов на вопросы безопасности в интернете уже были. Так, в 2009 г. при поддержке Координационного центра доменов .RU и .РФ впервые был проведен **Всероссийский конкурс сайтов «Позитивный контент»** *(www.positivecontent.ru)*[*].

Учебно-методическое пособие «Практическая психология безопасности. Управление персональными данными в интернете» продолжает миссию этого проекта, уделяя особое внимание несовершеннолетним пользователям интернета как одной из наиболее уязвимых категорий пользователей. Цель пособия — донести до российских учителей и их учеников необходимость защиты личной информации и доступно объяснить правила безопасного управления персональными данными в интернете.

Директор Координационного центра
национального домена сети интернет
А.А. Воробьев

[*] Подробнее о конкурсе — на с. 222.

ВСТУПИТЕЛЬНОЕ СЛОВО

Методическое пособие «Практическая психология безопасности: управление персональными данными в интернете» — часть информационно-просветительской работы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор РФ) в области защиты персональных данных несовершеннолетних пользователей интернета.

В основе пособия — уникальный опыт работы Уполномоченного органа по защите прав субъектов персональных данных РФ, а также передовые научно-исследовательские и учебно-методические разработки Федерального института развития образования, факультета психологии МГУ имени М.В. Ломоносова и Фонда Развития Интернет.

Уровень развития информационных технологий, в частности, возросшие технические возможности по сбору, копированию и распространению информации, достигли того предела, когда прежние подходы к регуляции обращения персональных данных требуют пересмотра и серьезной модернизации. Существующие угрозы и вызовы безопасному обороту персональных данных принимают все более сложный и системный характер и требуют выработки новых эффективных решений и действенных мер. Большое значение в сложившейся ситуации приобретает стратегическое прогнозирование и планирование, мониторинг угроз и стратегическая оценка защищенности персональных данных граждан.

Одним из ключевых направлений работы по защите прав субъектов персональных данных становится информационно-

просветительская деятельность, в рамках которой особое внимание уделяется несовершеннолетним пользователям интернета как одной из наиболее уязвимых категорий пользователей. В связи с этим создание данного пособия — один из значимых шагов на пути реализации информационно-просветительской стратегии деятельности Уполномоченного органа, о которой было заявлено в 2015 г. Его главная задача — донести до российских учителей и их учеников необходимость защиты личной информации и объяснить правила безопасного управления персональными данными в интернете.

Согласно Федеральному закону «О персональных данных», статус субъекта персональных данных не зависит от дееспособности лица, а это значит, что любой ребенок является носителем личной информации и, соответственно, субъектом персональных данных. Ответственность за незаконную обработку данных и последствия такой обработки лежит на операторе, но это юридический аспект. В то же время, говоря о специфике работы с данными такой незащищенной категории граждан, как несовершеннолетние, мы должны понимать, что на взрослых лежит большая социальная ответственность. Ведь беспечное отношение к информации со стороны людей, которые непосредственно вовлечены в процесс воспитания, а также операторов персональных данных детей, существенно облегчает злоумышленникам путь к частной жизни детей и может привести к плачевным последствиям.

В наше время личная информация о детях появляется в сети разными путями: ее выкладывают сами юные пользователи, их родители и друзья. Но это всего лишь полбеды: как показывает практика, значительная часть информации о несовершеннолетних пользователях оказывается в интернете в результате неправильного обращения с персональными данными в образовательных учреждениях.

Сегодня информационные технологии стали неотъемлемой частью образовательного процесса. Педагоги активно обогащают образовательную среду, используя уникальные возможности новых технологий, и не всегда задумываются о безопасности школьников как в интернете, так и в реальной жизни. В частности, это относится к хранению и обработке персональных данных детей и подростков. Ведение электронных дневников и журналов, школьных сайтов и других сетевых проектов стало неотъемлемой частью деятельности современного образовательного учреждения. В результате огромные массивы персональных данных учеников и их родителей стекаются в школы, а хранение и обработка этих данных далеко не всегда осуществляются надлежащим образом.

В ходе мониторинга, проведенного в 2014 г. Управлением по защите прав субъектов персональных данных Роскомнадзора РФ, было выявлено более 2000 сайтов, которые распространяли данные о несовершеннолетних пользователях, не имея на то законных оснований. В большинстве случаев эти нарушения сводились к размещению в интернете различных списков, содержащих персональные данные детей и родителей. Как показывает практика, причиной таких нарушений чаще всего становятся подзаконные нормативные правовые акты, обязывающие организации выкладывать в публичный доступ информацию о детях.

Вопросы защиты персональных данных несовершеннолетних пользователей, в том числе в интернете, требуют комплексного подхода, который должен включать не только принятие мер, направленных на устранение нарушений законодательства, но и создание механизмов, обеспечивающих безопасность детей и подростков в информационном пространстве.

Для привлечения внимания общественности к проблемам и последствиям незаконной обработки персональных данных,

повсеместного распространения личной информации в сети интернет, а также повышения уровня информированности российских пользователей в 2015 г. Управлением по защите прав субъектов персональных данных Роскомнадзора РФ был реализован целый ряд информационно-просветительских проектов:

1. Началом этой работы стало создание *научно-практического комментария к Федеральному закону «О персональных данных».* Комментарий получил высокую оценку со стороны отраслевого сообщества и экспертов и стал настольной книгой у большинства операторов персональных данных (Федеральный закон «О персональных данных»: научно-практический комментарий, 2015).

2. Параллельно с этим для несовершеннолетних пользователей интернета был запущен информационно-образовательный портал *ПЕРСОНАЛЬНЫЕ ДАННЫЕ. ДЕТИ*, цель которого — в игровой форме объяснить детям и подросткам правила безопасного обращения с персональными данными в сети. Яркие и запоминающиеся герои в живой и понятной форме делятся с посетителями сайта своими историями, рассказывают о последствиях неосторожного обращения с личной информацией и объясняют правила безопасного использования персональных данных, а интерактивные игры и задания помогают школьникам закрепить новый материал. Информация, размещенная на сайте, рекомендована в школах для изучения в рамках уроков безопасного интернета.

3. *«Защити свои персональные данные»* — еще один проект для школьников, реализованный по инициативе Роскомнадзора РФ. Цель проекта — информирование детей по вопросам безопасного обращения с персональными данными в сети интернет. В рамках этой инициативы в сентябре 2015 г. среди школьников Москвы был проведен конкурс на лучший плакат «Защити свои персональные данные», а также на лучшие видео-

ролики: «Последствия утечки персональных данных» и «Как мне защитить свои персональные данные?». С работами победителей можно ознакомиться на портале *ПЕРСОНАЛЬНЫЕ ДАННЫЕ. ДЕТИ*. Такой конкурс планируется проводить в различных регионах Российской Федерации ежегодно.

4. В 2015 г. по инициативе Роскомнадзора стартовала кампания по пропаганде безопасной работы с персональными данными в сети интернет. На VI Международной конференции по защите персональных данных, которая проводилась в ноябре 2015 г. в Москве, был представлен ролик социальной рекламы, подготовленный Управлением по защите прав субъектов персональных данных Роскомнадзора РФ для трансляции в интернете, а также по федеральным каналам телевидения.

Методическое пособие *«Практическая психология безопасности: управление персональными данными в интернете»* — продолжение этой линии работы, позволяющее донести ее результаты в простой и доступной форме до российских школьников и учителей. Внедрение изложенной в пособии программы в учебно-воспитательную работу образовательных учреждений станет важным этапом на пути воспитания нового поколения компетентных пользователей интернета, способных эффективно и безопасно управлять своими персональными данными в мире цифровых технологий.

Заместитель руководителя Роскомнадзора
А.А. Приезжева

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Защита и управление

Персональные или личные данные — это основное содержание широко исследуемого феномена приватности, связанного с частной жизнью и правом личности на неприкосновенность. Понятие «приватность» пришло к нам из англо-американской правовой системы, где начало употребляться в законодательной практике с конца XIX в. Там оно прошло путь от понятия, обозначающего право на частную собственность, до довольно сложного феномена, объединяющего личную и социальную жизнь человека. На Западе приватность входит в число фундаментальных прав человека, а на Востоке эта тема не из числа приоритетных.

Если для американца частная жизнь и личное пространство — святыня, то для россиянина их границы условны и размыты. В российской культуре все эти моменты до недавнего времени не акцентировались как значимая часть ментальности народа, приватность была «неродным» словом. Появившись в конце 90-х гг. в бытовом лексиконе, она долгое время шла калькой с английского «прайвеси» (privacy). В таком виде даже появилась в орфографических словарях. В результате приватность — за рубежом достаточно разработанная в науке тема (*Westin*, 1967; *Pastalan*, 1970; *Altman*, 1975; *Wolfe*, 1978 и др.) — в российской психологии, за некоторым исключением (*Нартова-Бочавер*, 2006; *Ктениду*, 2010; *Емелин*, 2014), практически не исследовалась.

Проблемы приватности и персональных данных в интернете сегодня активно обсуждаются профессионалами в области информационных технологий, журналистами, политиками, педа-

гогами. Но для среднестатистического российского пользователя сети вопросы защиты персональных данных пока еще не вошли в число приоритетных. Исследования показывают, что, по сравнению с жителями других стран Европы и Северной Америки, россияне меньше заботятся о приватности и готовы легче с ней расстаться (The EMC Privacy Index.., 2014).

Направленность зарубежных исследований приватности определялась главным образом интересом и уважением к частной собственности и личной жизни. Приватность очерчивает сферу важных жизненных интересов человека, в которой он не изолирован от окружающего мира, но тем не менее автономен в границах своей материальной и личной собственности. Хотя понятие приватности возникло гораздо раньше распространения инфокоммуникационных технологий, одно из его первых научных определений было связано с информацией — как процесс ее ввода и вывода. Другими словами, это право индивида решать, насколько быть открытым или закрытым по отношению к внешнему миру — какая информация и при каких условиях может быть сохранена как тайна или, наоборот, передана другим людям (*Westin*, 1967).

Наиболее фундаментальный подход к пониманию приватности представлен в широко известной концепции И. Альтмана. Он, в свою очередь, развивает идеи А. Уэстина, определяя приватность как «важный регуляторный динамический процесс, детерминирующий и непрерывно корректирующий границы личности с точки зрения ее взаимоотношений с окружающим миром». Таким образом, удовлетворяющая человека приватность — это «установление желаемого баланса между “открытостью и закрытостью”, “я и другими”, “прошлым и будущим”». Изучая приватность в контексте объективного человеческого поведения, преобразующего окружающую среду, Альтман выделил

несколько форм такого преобразования: дистанцию, личное пространство, территориальность, персонализацию (*Altman*, 1975).

Профессор Р. Кларк, главный редактор руководства PIA по оценке ущерба, вызванного нарушением приватности (разработанного британским информационным комиссариатом), определяет ее как право человека на личное пространство, свободное от вмешательства других людей и организаций (*Clarke*, 1997). Цель создания данного руководства — определение рисков в сфере приватности и поиск наилучших способов для обеспечения неприкосновенности частной жизни. В нем приватность рассматривается шире, чем неприкосновенность информации: акцент делается на возможности контролировать личную информацию, а не на желании скрыть ее или утаить. Выделяют четыре типа приватности.

- *Приватность самой личности (физическая)* — защита организма человека от нежелательных воздействий на него, например, свобода от пыток, право на отказ от вакцинации, лоботомии, стерилизации, переливания крови, пересадки органов, предоставления биометрических данных и др.
- *Приватность поведения личности (поведенческая)* — защита предпочтений и привычек, политических и религиозных взглядов, личного пространства и приватных мест от несанкционированных наблюдений и вторжений.
- *Приватность персональных коммуникаций (коммуникационная)* — право на свободу коммуникаций, тайну переписки (в том числе электронной) и телефонных переговоров, защиту от слежки.
- *Приватность персональной информации (информационная)* — обеспечение прав граждан в области персональных данных, включая их циркуляцию, защиту и контроль (ICO PIA Handbook, December, 2007).

Стремительное развитие интернета и его сервисов, работающих на основе персональных данных, привело к тому, что в современной культуре угроза потери приватности стала определяться как один из главных рисков информационного общества. Так, в нашей стране в течение 2015 г. Роскомнадзором зарегистрировано приблизительно 33 тыс. обращений от граждан с жалобами на нарушения, связанные с публикацией их личных данных в интернете. Среди основных источников киберугроз, подстерегающих субъектов персональных данных в интернете, выделяются: практика принятия пользовательских решений по умолчанию, хищение персональных данных, их распространение в открытых источниках и передача личной информации по незащищенным каналам связи, использование поддельных (выдающих себя за фирменные) мобильных приложений, видеонаблюдения и геолокационных сервисов, фишинг.

Эксперты (2,5 тыс. чел.), формирующие облик современного интернета, в 2014 г. были опрошены специалистами аналитического центра Pew Research и дали прогнозы по поводу будущего приватности. Если их суммировать, то выводы следующие. Во-первых, жизнь станет публичной, так как в современном мире невозможно будет жить, не открывая свою персональную информацию государству и корпорациям, мотивированным на использование персональных данных населения. Во-вторых, приватность станет роскошью, и только отдельные люди или сообщества будут иметь ресурсы для защиты от «электронной слежки». В-третьих, справляться с вопросами безопасности персональных данных будет все сложнее. Ситуация усугубится с возникновением такого явления, как «интернет вещей»* — дома, рабочие места и все окружающие объекты будут, мягко выража-

* Подробнее см. журнал «Дети в информационном обществе» (№ 18). URL: http://detionline.com/assets/files/journal/18/inf-obshestvo.pdf.

ясь, «сплетничать» за спиной человека. В-четвертых, культурам, проповедующим различные взгляды на приватность, невозможно будет прийти к согласию о том, как реализовывать гражданские свободы в интернете (*Rainie, Anderson*, 2014).

Проникновение интернета во все сферы жизни и ускоряющийся темп конвергенции реального и виртуального миров требуют пересмотра устоявшегося баланса между частным и публичным в жизни общества. В контексте измерений, характеризующих социальные аспекты приватности — «открытость и закрытость», «прошлое и будущее», «я и другие» — ключевое значение приобретают такие особенности онлайн-среды, как ее трансграничность, вневременность, а также феномен размывания идентичности.

Интернет характеризуется трансграничностью, поэтому баланс «открытости — закрытости» все более смещается в сторону открытости. Одно из главных условий приватности — соблюдение различных границ. Вне зависимости от их типа (социальные, личностные или физические), они имеют пространственные маркеры, предполагающие реальную или воображаемую разделительную черту. В виртуальном мире привычное понимание границ трансформируется и постепенно теряет свое значение. Другой смысл начинают приобретать понятия «дистанция», «территориальность», «личное пространство». Настройки конфиденциальности дают всего лишь иллюзию закрытости и «только моего» пространства профиля. Это как раскладные картонные стенки, которые можно возить с собой и, например, отгородиться ими от соседей в метро. К тому же далеко не все хотят закрыться от всего мира и мечтают, чтобы их оставили в покое. Большинство людей стремится быть частью виртуального общества и пользоваться его возможностями, например, применять разные полезные приложения и программы,

которых с каждым днем становится все больше. На самом деле мы добровольно предоставляем персональную информацию и, подписывая соглашения, разрешаем всячески использовать свои персональные данные: записывать, хранить, архивировать, перепродавать и т.д. Таким образом, мы с помощью своего собственного компьютера ежедневно сами себя оцифровываем и ограничиваем свое право на приватность.

Интернет изменяет не только пространство, но и время. Для понимания того, что происходит со временем в информационном обществе, Мануэль Кастельс придумал термин «вневременность». Это то время, которое одновременно и разрывается, и спрессовывается — прошлое, настоящее и будущее не связаны последовательностью, они практически соединены вместе (*Кастельс*, 2000). В контексте темы приватности и защиты персональных данных вопрос уникального цифрового отпечатка, соединяющего прошлое, настоящее и будущее, приобретает особую актуальность. Раньше собранное титаническими и многолетними усилиями персональное досье могло сгореть в одночасье и исчезнуть навсегда. Сегодня наш цифровой отпечаток, например, браузер со всеми плагинами, действиями, cookie, геометками, регулярностью посещений определенных ресурсов, дополненный друзьями, организациями и посторонними людьми, — лучшее досье, созданное нами самими. Причем это не только наше прошлое и настоящее — это цифровой след, наш идентификатор, который всегда будет с нами, формирует нашу нынешнюю жизнь, а следовательно, и часть нашего будущего.

Все труднее находить точку оптимального баланса между «я» и «другими», которая отражала бы нашу истинную идентичность и то, что мы хотели бы, чтобы о нас знали окружающие. Разнообразие «других» в онлайн-пространстве существенно увеличивается: это не только друзья, знакомые, но и представители

различных групп, а также просто посторонние люди, среди которых могут быть и враждебные «чужие». Персонализируя себя в онлайн-среде через раскрытие своих связей и контактов, политических, философских, духовных, культурных, эстетических и других ценностей и интересов, значимых событий, потребностей и склонностей, мы все меньше можем контролировать свою открытость и знать, где и кому достается наша персональная информация, а также как она воспринимается. Ведь нередко образы, которые мы создаем в разных группах или сообществах, могут мало совпадать с реальностью. Расширяющийся диапазон связей и контактов в сети, ее ролевые возможности способствуют размыванию нашей идентичности, а соответственно, и границ приватности, что также ведет к нежелательному распространению и искажению персональных данных.

Как определяются персональные данные в законодательных актах в разных регионах мира и как формулируется правовая позиция по их защите? В Директиве Европейского парламента и Совета Европейского Союза от 24.10.1995 № 95/46/ЕС «О защите данных» персональные данные определяются как «любая информация, которая относится к уже идентифицированному лицу, либо с помощью которой можно идентифицировать физическое лицо (субъект данных)». В соответствии с Директивой идентифицируемое лицо — это «лицо, которое может быть определено прямо или косвенно, в частности, посредством ссылки на идентификационный номер или на один или несколько факторов, специфичных для его физической, психологической, ментальной, экономической, культурной или социальной идентичности».

В США существует около 20 локальных (секторальных) и национальных нормативных актов, касающихся приватности и защиты данных. Подобные законы есть практически в каж-

дом штате. Например, только в Калифорнии действует более 25 законов о защите персональных данных и приватности. Большое количество компаний, регулируемых Федеральной Комиссией по Торговле (Federal Trade Commission — FTC), подвергается санкциям в случае, если они совершают незаконные или обманные торговые операции, не принимают минимальных мер по защите данных своих потребителей либо не выполняют свои обещания относительно обеспечения приватности.

Международно признанные права и свободы человека нашли свое отражение в главе второй действующей Конституции Российской Федерации. В их число вошли и такие важнейшие права человека: на неприкосновенность частной жизни, личную и семейную тайну, тайну почтовых, телефонных, телеграфных и иных сообщений (все эти права можно рассматривать как право на приватность). В Федеральном законе от 25.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» персональные данные (информация о гражданах) определяются как «сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность». В соответствии со ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», они понимаются еще шире — как «любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)»*.

Сегодня в нашей культуре приватность стала пониматься в более широком контексте именно в связи с развитием интернета, в результате вопросы защиты персональных данных попали в число самых актуальных вопросов безопасности не только взрослых, но и детей. Об этом говорит, в частности, тот факт,

---

* С перечнем основных законодательных актов по проблеме персональных данных можно ознакомиться на с. 54.

что Роскомнадзор в 2014 г. провел первый Всероссийский День защиты персональных данных детей.

Психологи рассматривают приватность и как результат развития личности, и как необходимое условие для ее развития. В западной психологии приватность рассматривается как ключевой фактор становления автономии ребенка, которая начинает складываться в раннем детстве. В процессе социализации ребенка личное пространство и приватность формируются через развитие самостоятельности и независимости в отношениях между ребенком и членами его семьи, в его отношениях с друзьями, учителями и обществом в целом.

В 1998 г. в США появился первый законодательный «Акт о защите приватности детей онлайн» (Children's Online Privacy Protection Act of 1998, COPPA — 15 U.S.C. 6501, et seq.), принятый Конгрессом и Федеральной Торговой Комиссией США. Он лег в основу действующих в США на настоящий момент «Правил защиты приватности детей онлайн». Они регламентируют порядок сбора персональных данных детей в возрасте до 13 лет физическими или юридическими лицами, действующими в интернете на коммерческой основе. Также в них определяется, какие пункты операторы персональных данных обязаны включать в политику приватности, каким образом должно быть составлено согласие на обработку данных, какова ответственность операторов в области защиты личных данных детей. В этом документе дается определение персональной информации, собираемой онлайн, и выделяются следующие категории: 1) фамилия и имя; 2) адрес проживания или другой физический адрес, включая название улицы, города или населенного пункта; 3) контактные данные онлайн; 4) имя, отображаемое на экране, или имя пользователя, и его контактная информация; 5) номер телефона; 6) социальный страховой номер; 7) постоянный идентификатор, который может

использоваться для опознавания пользователя в течение времени на различных веб-сайтах или онлайн-сервисах. Такой постоянный идентификатор может включать IP-адрес, серийный номер устройства или процессора, иной уникальный идентификатор; 8) фотография, видео- или аудиофайл, где содержится такая информация, как голос или изображение ребенка; 9) геолокационная информация, достаточная для того, чтобы идентифицировать улицу и населенный пункт; 10) информация, касающаяся ребенка или его родителей, которую онлайн-оператор данных получает от ребенка и совмещает с идентификатором, описанным в п. 7 (Children's Online Privacy Protection Rule, 1998).

По мнению аналитиков, приватность сегодня теряет связь с секретностью, тайной, анонимностью и уединенностью — а ведь именно в этом заключался ее главный смысл для старших поколений. В наши дни вопрос обеспечения приватности становится больше связан с проблемой безопасности и защиты персональных данных, а значит — с вопросами их контроля со стороны пользователя.

РОССИЙСКИЕ ШКОЛЬНИКИ

Приватность и безопасность в сети

Сегодня все пользователи сети в той или иной степени понимают, что свою частную жизнь и ее важнейшую составляющую — персональные данные — необходимо защищать. Для этого специально созданы различные механизмы: от паролей до сложных ключей, идентификаторов, электронных цифровых подписей. И тем не менее, поскольку многие из нас — недавние и не вполне опытные пользователи интернета, риски распространения и ненадлежащего использования приватных сведений очень высоки.

Разумеется, это касается и российских школьников, активно общающихся в соцсетях, где личной информацией делятся много и часто. Попытаемся представить реальную картину того, что происходит с персональными данными наших детей и подростков. Какое количество российских школьников сталкивается с проблемами, возникающими в результате ненадлежащего использования персональных данных, существует ли какая-нибудь динамика в этом вопросе, что знают об этих проблемах родители и способны ли они помочь детям с ними справиться?

В поиске ответов на эти вопросы был проведен сравнительный анализ результатов нескольких исследований Фонда Развития Интернет, проводившихся в разное время.

1. Исследование, проведенное в 2010 г. в рамках проекта Еврокомиссии EU Kids Online II. Цель — изучение детского и родительского опыта столкновения с интернет-угрозами и безопасного использования интернета и новых онлайн-технологий в 25 странах Европы, в России и других странах мира. Выборка составила

1025 пар «родитель — ребенок». В данном исследовании, проведенном в 11 регионах Российской Федерации, приняли участие дети в возрасте 9–16 лет (*Солдатова, Рассказова и др.*, 2012).

2. Исследование цифровой компетентности российских подростков и их родителей, которое проводилось в 2013 г. Фондом Развития интернет и факультетом психологии МГУ имени М.В. Ломоносова. В ходе исследования были опрошены 1203 подростка 12–17 лет и 1209 родителей детей этого возраста из 58 городов с населением от 100 тысяч человек во всех 8 федеральных округах России. Опрос проводился Аналитическим центром Юрия Левады по специально разработанной методике Фонда Развития Интернет (*Солдатова, Нестик и др.*, 2013).

3. Исследование информации, которую сообщает о себе подростковая аудитория, на основе данных, полученных в результате поиска в социальной сети ВКонтакте (март 2015 г.). Для проверки и уточнения данных, предоставляемых поиском, также было проведено исследование 100 профилей московских подростков 14–17 лет (54 мальчика и 46 девочек). Отмечалось наличие либо отсутствие различных видов персональной информации на странице. Дополнительно был проведен анализ содержимого записей на стенах этих подростков в социальной сети (по 10 последних в каждом профиле записей, итого 1000) (*Солдатова*, *Олькина*, 2015).

4. Исследование отношения российских подростков к приватности и персональным данным, которое проводилось в 2016 г. Общая выборка составила 320 подростков в возрасте 11–17 лет (130 мальчиков — 40,6%, 190 девочек — 59,4%), обучающихся в образовательных учреждениях Москвы и Московской области. Исследовались: уровень подверженности школьников рискам, возникающим вследствие неосторожного обращения с персональными данными; представления школьников об уровне конфиденциальности и публичности различных категорий

информации; фактический уровень доступа к тем или иным видам данных подростков в социальных сетях; готовность ребят делиться личной информацией с другими пользователями, а также круг лиц, к которым подростки обращаются за помощью с настройками приватности в сети (*Солдатова, Олькина*, 2015).

Распространенность случаев столкновения детей и подростков с рисками ненадлежащего использования персональных данных в сети анализировалась на основе ответов на соответствующие вопросы, вошедшие в анкеты наших исследований за 2010, 2013 и 2016 гг. (рис. 1).

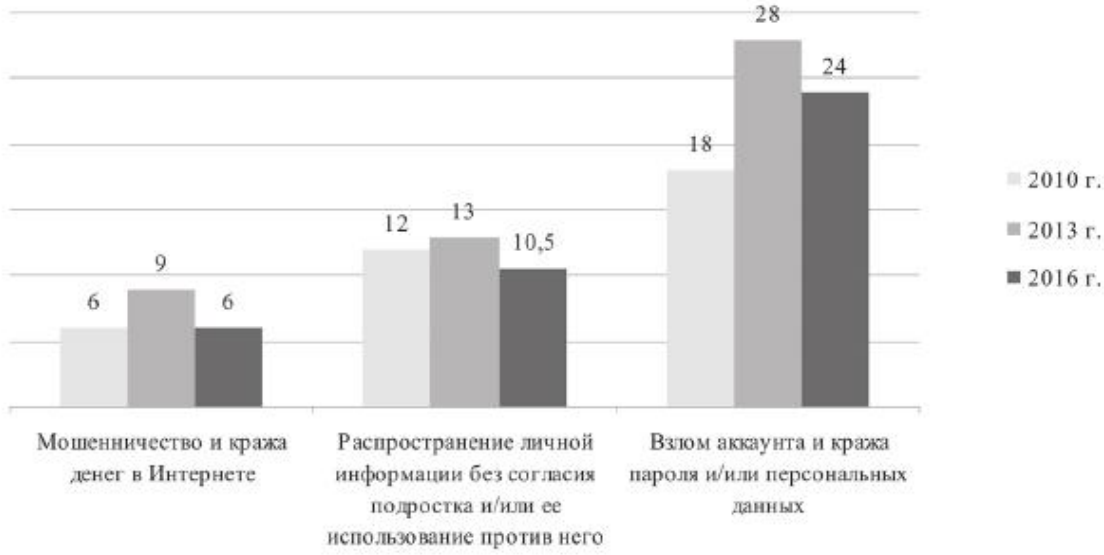


Рис. 1. Ответы подростков на вопрос:
«Случалось ли что-либо из перечисленного с тобой в интернете в течение последних 12 месяцев?», %

В 2010 г. в среднем каждый третий ребенок 11–16 лет сталкивался в сети с негативными последствиями ненадлежащего обращения со своими персональными данными или использованием его личной информации злоумышленниками. Дети 13–14 лет чаще попадали в ситуацию, когда кто-то использовал личную информацию, предоставленную ребенком в интернете, для розыгрыша или оскорбления, в то же время жертвой кражи

пароля для тех же целей чаще становились дети 15–16 лет. Дети 11–13 лет, как мальчики, так и девочки, одинаково часто попадали в ситуации, связанные с обманом и мошенничеством. Среди детей старшего возраста девочки несколько чаще становились жертвами мошенничества и неправомерного использования личной информации (*Солдатова, Рассказова и др.*, 2012).

В 2013 г. число детей, столкнувшихся с проблемами, которые связаны с персональными данными и мошенничеством в сети, существенно увеличилось — с 36 до 50%. Иными словами, если в 2010 г. с негативными последствиями ненадлежащего обращения с персональными данными в интернете сталкивался каждый третий ребенок, то в 2013 г. — уже каждый второй. Особенно увеличился показатель количества взломов аккаунтов и краж персональных данных: каждый четвертый ребенок сталкивался с этой проблемой. Известно, что в интернете существуют сайты, на которых можно сделать заказ на взлом профиля. Представители подобного «бизнеса» могут выполнять такие заказы в самых разных целях: шантажа, доступа к переписке пользователя, рассылки спама, получения данных о кредитной карте, промышленного шпионажа и т.д.

В 2016 г. число столкновений детей с представленными категориями рисков незначительно снизилось. Тем не менее процент детей, столкнувшихся с отрицательными последствиями ненадлежащего использования ими своих персональных данных или использованием их персональных данных злоумышленниками, по-прежнему достаточно высок и составляет 40,5%. Столь высокая подверженность рискам в первую очередь обусловлена тем, что, с одной стороны, дети интенсивно осваивают коммуникацию в социальных сетях, с другой — недостаточно осведомлены об элементарных правилах безопасного поведения и общения в интернете.

Различные социальные сети пользуются большой популярностью у школьников, поскольку позволяют осуществлять коммуникацию в сети. Они же — хранилище личной информации и площадка ее презентации интернет-пользователями. По данным исследований Фонда Развития Интернет, уже в 2013 г. 9 из 10 подростков — пользователей интернета — отметили, что у них есть своя страница ВКонтакте (*Солдатова, Нестик и др.*, 2013).

При этом важно понимать, что одно только наличие у подростка профиля в данной социальной сети не является непосредственной угрозой его приватности. Вероятность столкновения с рисками, связанными с персональными данными, зависит от навыков безопасного использования сетей. В этом случае особенно важны следующие моменты:

- соблюдает ли подросток правила конфиденциальности в отношении пароля;
- какой доступ установлен к его профилю в целом и к отдельным категориям личной информации в социальной сети;
- какую информацию о себе подросток сообщает незнакомым людям;
- осведомлены ли родители о проблемах своего ребенка, связанных с последствиями неосторожного отношения к персональным данным.

Соблюдение правил конфиденциальности в отношении пароля. Ключом к личной информации, особенно той, которая предназначена не для всех, является пароль. Именно с утерей конфиденциальности в отношении пароля нередко связаны неблагоприятные последствия в виде взломов профилей, кражи персональных данных, мошенничества и обмана в сети. Внимание к своему паролю входит в число элементарных правил

онлайн-безопасности. Соблюдают ли их подростки, и с кем они готовы поделиться ключом к своей информации?

Данные исследования 2013 г. показывают, что только половина опрошенных подростков никому не давали пароль от своего аккаунта в социальной сети или электронной почты. Остальные же легко делятся паролем не только с родителями: каждый пятый подросток сообщал пароль близкому другу и практически каждый десятый — друзьям, братьям или сестрам. В 2016 г. картина не изменилась: по-прежнему каждый второй подросток (55%) не соблюдает принцип конфиденциальности в отношении своих паролей и сообщает их своему ближайшему окружению. Кроме того, даже несколько увеличилась доля детей, готовых сообщить свой пароль незнакомому человеку (рис. 2).

Рис. 2. Ответы подростков на вопрос:
«Давал ли ты когда-нибудь пароль от своего аккаунта
в социальной сети или электронной почты?», %
(выборка — подростки, пользующиеся интернетом)

Доступ к профилю и отдельным категориям персональной информации. В исследовании 2010 г. подросткам был задан вопрос о том, какой доступ установлен к их профилю в социальной сети. Результаты свидетельствовали о том, что почти у третьей части опрошенных детей профили были открыты всему

миру. При этом наибольший процент открытых профилей наблюдался у детей 9–12 лет, зарегистрировавшихся в социальной сети несмотря на возрастные ограничения. Дети старшего возраста реже оставляли свой профиль открытым.

В настоящий момент зарегистрироваться ВКонтакте, имея мобильный телефон, может любой пользователь. Следовательно, в тех случаях, когда подросток оставляет свой профиль полностью открытым (выставлена настройка «страница видна всем пользователям социальной сети»), это автоматически означает открытый доступ к его персональной странице. Результаты исследования 2016 г. свидетельствуют о том, что число страниц с открытым доступом в среднем составляет более 60%, что более чем в два раза превышает показатель 2010 г. При этом если пять лет назад прослеживалась четкая возрастная динамика — с возрастом количество детей, открывавших свой профиль, уменьшалось, то в настоящий момент такая тенденция отсутствует (рис. 3).

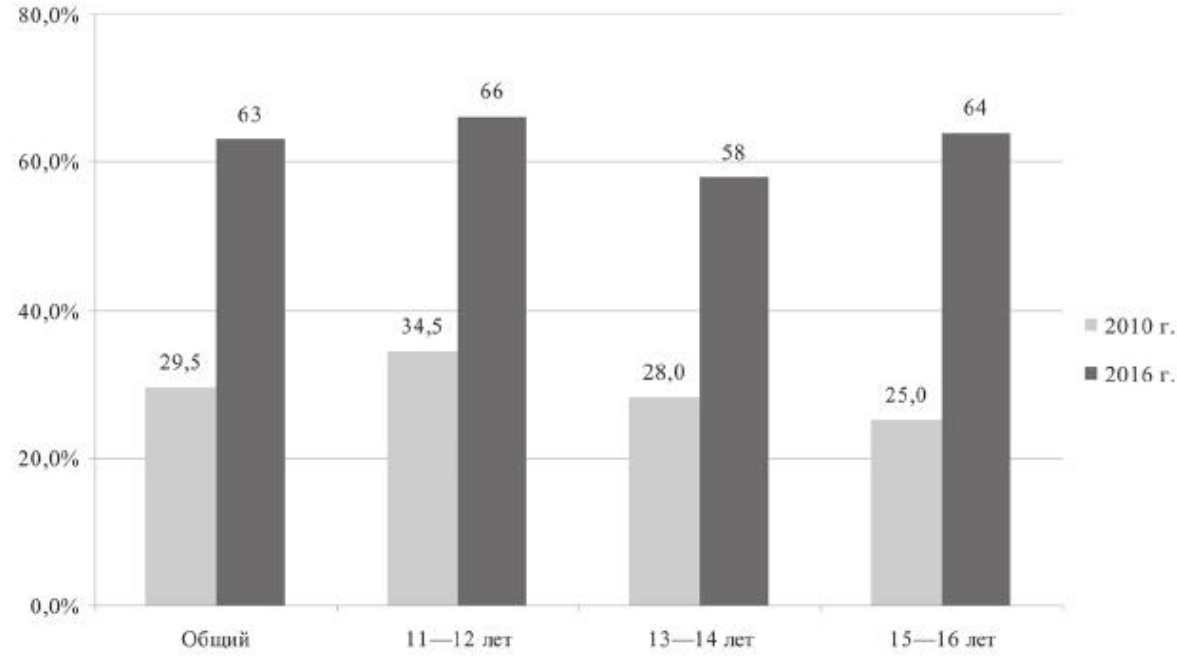


Рис. 3. Число подростков, у которых установлен общий доступ к профилю в социальной сети, %

Остановимся подробнее на анализе той информации, которую подростки публикуют в сети. В 2010 г. каждый третий ребенок в социальной сети выкладывал информацию о себе в максимально полном объеме. Большинство российских школьников (от 60 до 80%) сообщали в сети фамилию, точный возраст, номер школы, а также размещали фотографии, на которых отчетливо видны их лица. Еще треть детей указывали на странице в сети номер телефона или свой домашний адрес (*Солдатова, Рассказова и др.*, 2012). Этой информацией мог воспользоваться любой человек с любыми целями. В 2016 г. школьники стали осторожнее. Они по-прежнему включают в свой профиль фамилию; чуть реже, чем пять лет назад, но все же достаточно часто — фотографию, на которой видно лицо. Число детей, которые размещают у себя на странице точный возраст, информацию о своей школе, а также указывают номер телефона и домашний адрес, значительно сократилось (рис. 4).

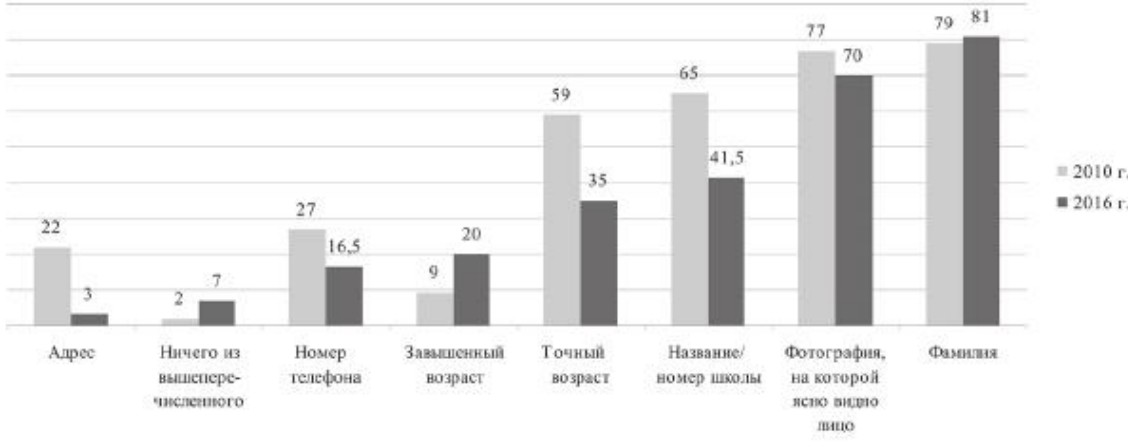


Рис. 4. Ответы подростков на вопрос:
«Какую информацию о тебе включает твой профиль?», %
(выборка — дети, у которых есть профиль в социальной сети)

При этом в два раза увеличилось число школьников, указывающих завышенный возраст, — в отличие от 2010 г., в 2016 г. это делает каждый пятый ребенок. Это свидетельствует о том, что в настоящий момент все больше аккаунтов создается детьми в

возрасте до 14 лет, которые вынуждены указывать завышенный возраст, чтобы использовать социальную сеть.

Современные настройки приватности стали гибче, они позволяют пользователю регулировать уровень доступа к каждому виду его данных. Таким образом, само по себе наличие информации в профиле еще не означает ее доступности для всех пользователей, поскольку владелец мог ограничить к ней доступ. В 2016 г. детям и подросткам был задан вопрос о том, какие из категорий персональной информации видны тем или иным группам пользователей социальной сети на их странице. Результаты опроса показывают, что примерно у трети детей установлен свободный доступ к общей информации (она может включать в себя такие сведения, как возраст ребенка, школа, интересы, хобби и т.д.), каждый шестой ребенок открывает косвенную контактную информацию (ссылку на свой сайт, скайп, аккаунты в других социальных сетях и т.д.). При этом 12% школьников готовы делиться непосредственно контактной информацией — оставляют доступными для всех номера мобильного и/или домашнего телефонов (рис. 5).

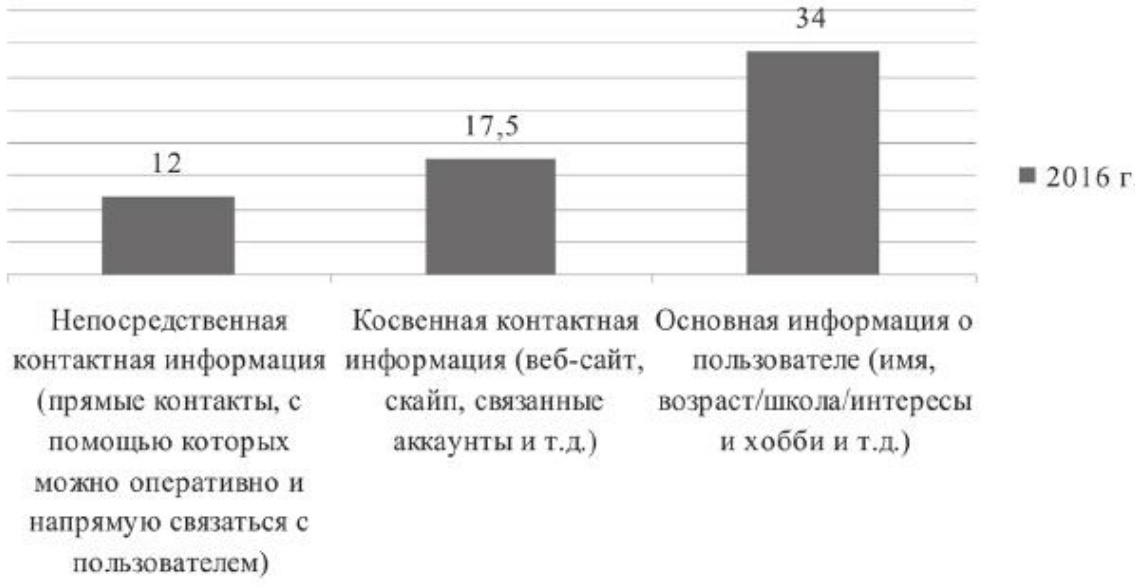


Рис. 5. Число подростков, указавших, что данные виды персональной информации видят все пользователи социальной сети, %

Сравнение результатов опросов по предоставлению персональных данных в сети с данными поискового запроса ВКонтакте отражает четкую тенденцию — исчезновение анонимности в социальных медиа и доступность паспортных данных пользователей. Экспресс-исследование детских аккаунтов ВКонтакте в целом подтвердило полученные в ходе анкетирования данные и показало, что любой зарегистрированный пользователь ВКонтакте может узнать дату рождения и реальные фамилию и имя 9 из 10 московских подростков; узнать, где родился каждый шестой юный москвич, и сходить в гости к четырем детям из ста, указавшим сведения о своем адресе (улица и номер дома). Помимо этого, каждому зарегистрированному пользователю видны фотографии 75% московских подростков. Также поисковый анализ ВКонтакте показал, что у каждого третьего ребенка, помимо основного фото, видны фотографии, на которых его отметили другие пользователи. Пройдя по ссылке «фотографии с пользователем», заинтересованное лицо с большой вероятностью сможет получить реальные изображения подростка, а также иные виды информации. Это может быть информация об учебном заведении, посещенных местах и мероприятиях, интересах и т.д. Следует также отметить, что иногда вместо реального фото дети используют различные картинки (героев мультиков, персонажей из комиксов), абстракции, фотографии знаменитостей, карикатуры, изображения домашних животных, лозунги. Также можно встретить фотографии подростка вместе со сверстниками и романтические снимки. По данным экспресс-исследования, примерно каждый пятый ребенок использует ненастоящую фотографию.

Нельзя не вспомнить также о геотегах. Это географические координаты местоположения или изображенного на снимке объекта. Геотеги устанавливают для возможности поделиться

с родными или друзьями тем, что происходит в режиме реального времени. Ни одна из проанализированных нами стен не содержала записей с геометками, но при этом каждый десятый подросток-москвич 14–17 лет открывает свою карту с указанием посещенных мест. Однако в социальных сетях, где основное содержание составляют именно фото или видеоизображения, с геометками другая ситуация. Группа американских исследователей изучила объемный фотоархив Flickr. Они пришли к выводу, что большинство снимков, на которых изображены дети, имеют геометки, причем последние модели смартфонов ставят их автоматически в момент съемки фотографии или записи видео. Получить адреса мест проживания большинства детей не составило труда, как и установить, что многие из ребят проживают в обеспеченных и респектабельных районах, что может быть стимулом для преступных действий злоумышленников (*Kuzma*, 2012).

По данным анализа профилей также можно составить представление о том, насколько доступна информация об интересах и навыках подростков. У 9 из 10 московских подростков 14–17 лет в профиле видны видео и принадлежность к сообществам ВКонтакте. Каждый третий открывает зарегистрированным пользователям свои аудиозаписи. Однако в текстовом виде интересы (музыку, фильмы, любимые шоу, телепередачи и игры) и самого себя описывает только каждый десятый подросток. Примерно каждый пятый школьник указывает свои политические и мировоззренческие взгляды, делится представлениями о «главных ценностях в жизни».

Заметим, что несмотря на большие объемы циркулирующих в социальной сети персональных данных, их доступность далеко не всегда означает достоверность. В том числе это связано с ролевым экспериментированием в сети и подростковой модой на

«экстравагантные данные» с целью самопрезентации и создания определенного имиджа. На примере сопоставления семейного статуса, который подростки публикуют ВКонтакте, с реальной статистикой эта «мода» особенно наглядна: число «замужних» и «женатых» подростков 14–17 лет в этой сети практически в 5 раз превышает реальное число зарегистрированных на территории РФ браков в этой возрастной категории (рис. 6) (Сайт Федеральной службы государственной статистики, 2016).

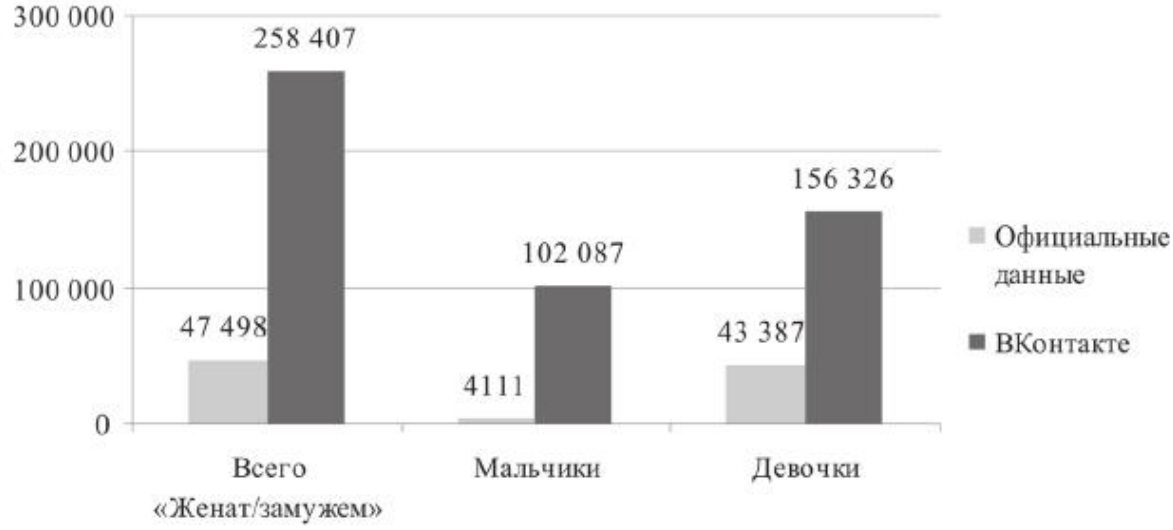


Рис. 6. Статусы подростков до 18 лет ВКонтакте по сравнению с официальной статистикой регистрации браков РФ от 14 до 18 лет (по возрасту жениха и невесты) за 2010–2014 гг., чел.*

Стоит отметить также, что даже максимально закрытый профиль или полное отсутствие данных в личном профиле пользователя не гарантируют в ВКонтакте полную приватность. Ведь даже если сам подросток не публикует фотографии и записи на своей стене, зарегистрированный пользователь может зайти на страницы его друзей и получить большое количество информации: возраст, место учебы, информацию о месте проживания, учебном заведении, посещенных мероприятиях и т.д. Кроме того, поиск

* С Крымским федеральным округом.

ВКонтакте работает «против пользователя». Например, если пользователь в настройках приватности предпочел скрыть дату своего рождения, город и место проживания, в случае соответствия страницы выбранным критериям она все равно появится в поиске.

Информация, которой подростки делятся с незнакомыми людьми. Помимо того, что дети предоставляют открытый доступ к тем или иным видам персональных данных, они нередко общаются в интернете с малознакомыми людьми и высылают им информацию о себе. В 2010 г. доля детей, которые заводили новые знакомства в интернете и добавляли в список друзей тех, кого не знают лично, составляла 68%. Более 40% из них свободно делились персональными данными с незнакомыми людьми. Еще около трети отправляли фото или видео со своим изображением кому-либо, с кем не было предварительной личной встречи или знакомства.

В 2016 г. доля детей, совершающих «рискованные действия», потенциально ведущие к утере персональных данных либо их использованию против подростка, уменьшилась. Тем не менее

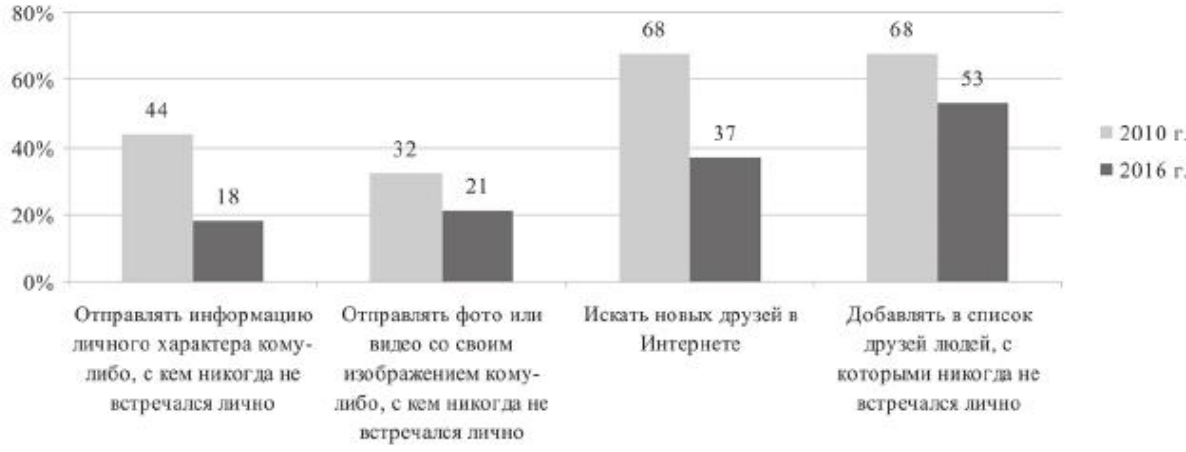


Рис. 7. Число подростков, утвердительно ответивших на вопрос: «Приходилось ли тебе делать что-либо из представленных вариантов хотя бы однажды в течение последних 12 месяцев?», %

по-прежнему половина детей добавляет в свой френд-лист незнакомцев, причем более трети специально ищут их сами. И практически каждый пятый ребенок отметил, что он регулярно отправляет незнакомым пользователям свои фото- и видеоматериалы, а также иную информацию личного характера (рис. 7).

В 2013 и 2016 гг. детям был задан вопрос о том, какие именно виды персональных данных они готовы предоставить незнакомым людям. В 2016 г. доля тех, кто предоставит незнакомцу информацию о своих интересах, городе проживания и возрасте увеличилась. Свои имя и фамилию по-прежнему сообщают почти 40% детей. С трети до четверти уменьшилось число школьников, которые отправят свое фото, более чем вдвое сократилось число сообщающих номер школы и телефона. Тем не менее каждый четвертый готов отправить незнакомому человеку в сети свою фотографию, каждый двенадцатый — номер школы и номер телефона (рис. 8).

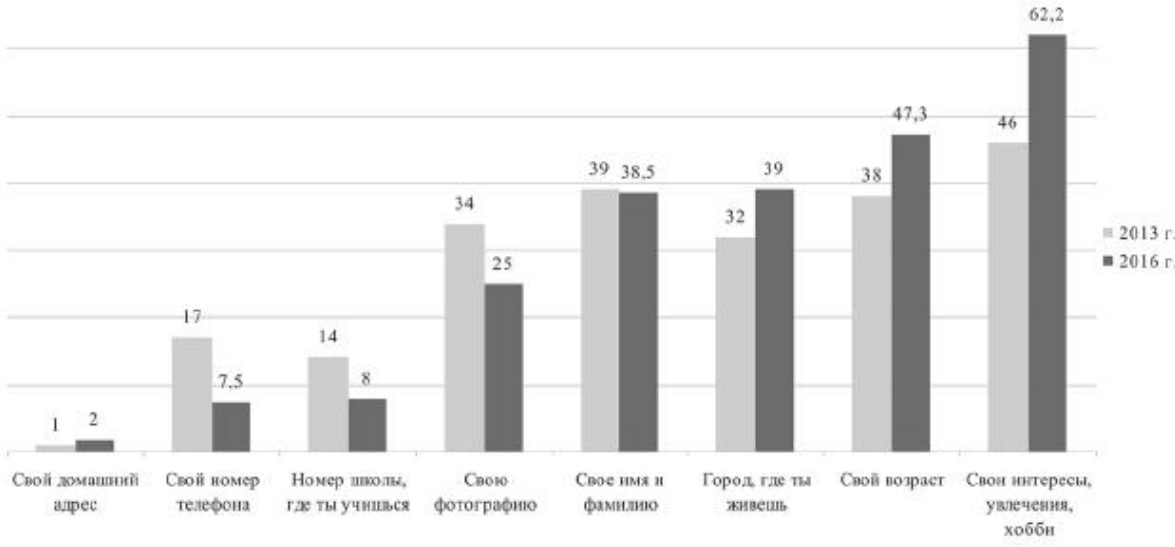


Рис. 8. Ответы подростков на вопрос: «Если ты познакомился (-ась) в интернете с новым другом, и он хочет узнать о тебе больше информации, какую информацию о себе ты ему, скорее всего, дашь?», %

На родителей не стоит рассчитывать. Что знают родители о рисках, связанных с персональными данными их детей? Сравнение данных за 2010 и 2013 гг. показало, в частности, что возросло количество родителей, которые не осведомлены о проблемах, возникающих в результате неосторожного использования детьми персональных данных в социальных сетях (рис. 9). Если число детей, столкнувшихся с проблемой взлома профиля в социальной сети и электронной почте, за три года увеличилось на 10% (с 18 до 28%), то число знающих об этом родителей увеличилось всего на 3% (с 13 до 16%). По всем другим аспектам уровень осведомленности родителей о последствиях неосторожного обращения с персональными данными также невысокий. В том числе это касается мошенничества и кражи денег в сети — рисков, которые могут нанести существенный урон семейному кошельку. В 2010 г. родители даже несколько преувеличивали опасность по сравнению с ответами подростков, но в 2013 г., несмотря на то, что дети стали встречаться с мошенничеством еще чаще, уровень осведомленности родителей об этих рисках снизился.

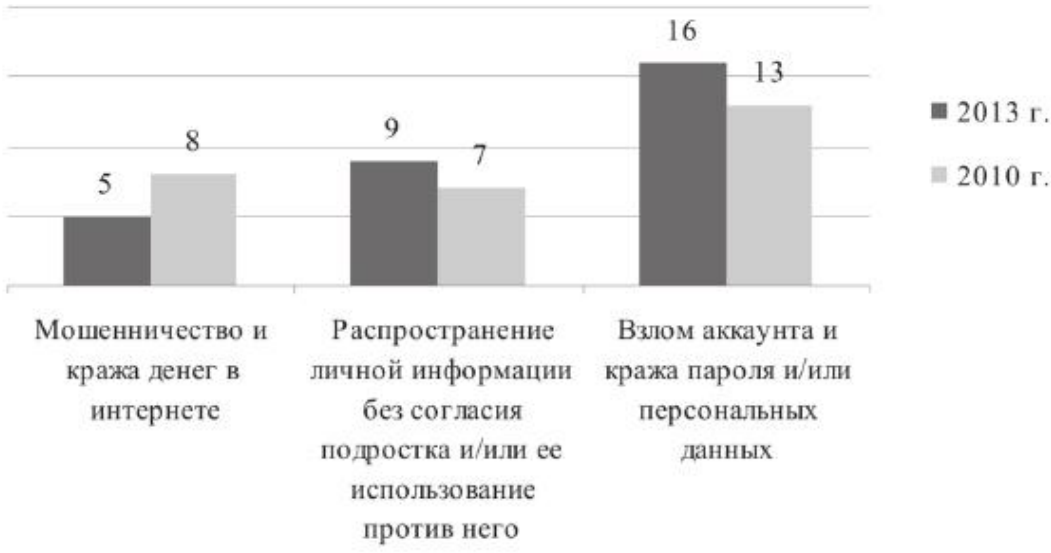


Рис. 9. Ответы родителей на вопрос:
«Случалось ли что-либо из перечисленного с вашим ребенком в интернете в течение последних 12 месяцев?», %

Низкий уровень осведомленности родителей о рисках, которым подвергаются их дети, выкладывающие данные о себе, означает, что родители не смогут своевременно оказать им поддержку в сложных ситуациях. Вообще, родители не всегда чувствуют себя способными помочь своему ребенку: каждый пятый указал, что «в чем-то он может помочь, а в чем-то нет». При этом треть родителей отмечает, что они либо практически не могут оказать помощь, либо ребенок в ней не нуждается, потому что знает все сам, либо родители сами обращаются за помощью к сыну или дочери.

Родители в качестве доверенных лиц по помощи в интернете занимают не первые места не только в нашей стране. В 2012 г. американский центр по изучению интернета и общественной жизни (Pew Research Center) провел опрос 802 подростков в возрасте 12–17 лет и их родителей. Основной целью было — выяснить, кто помогает детям, когда им нужно разобраться с настройками приватности в сети, и, если им необходима помощь, к кому они обращаются за советом (*Madden M., Cortesi S. etc.,* 2012).

В своем исследовании 2016 г. мы задали детям аналогичный вопрос. Согласно полученным данным, в отличие от Америки, где 70% подростков хотя бы к кому-то обращались за помощью по вопросам настройки приватности в интернете, у нас такое же число детей решает подобные проблемы самостоятельно. Если ребенок все же хочет обратиться за помощью, то в первую очередь он идет к друзьям или ищет информацию в интернете. Только каждый десятый попросит помочь родителей, а к учителям дети обращаются исключительно редко (рис. 10).

Итак, сравнительный анализ данных наших исследований показал, что ситуация в отношении рисков, связанных с персональными данными, за три года остается тревож-

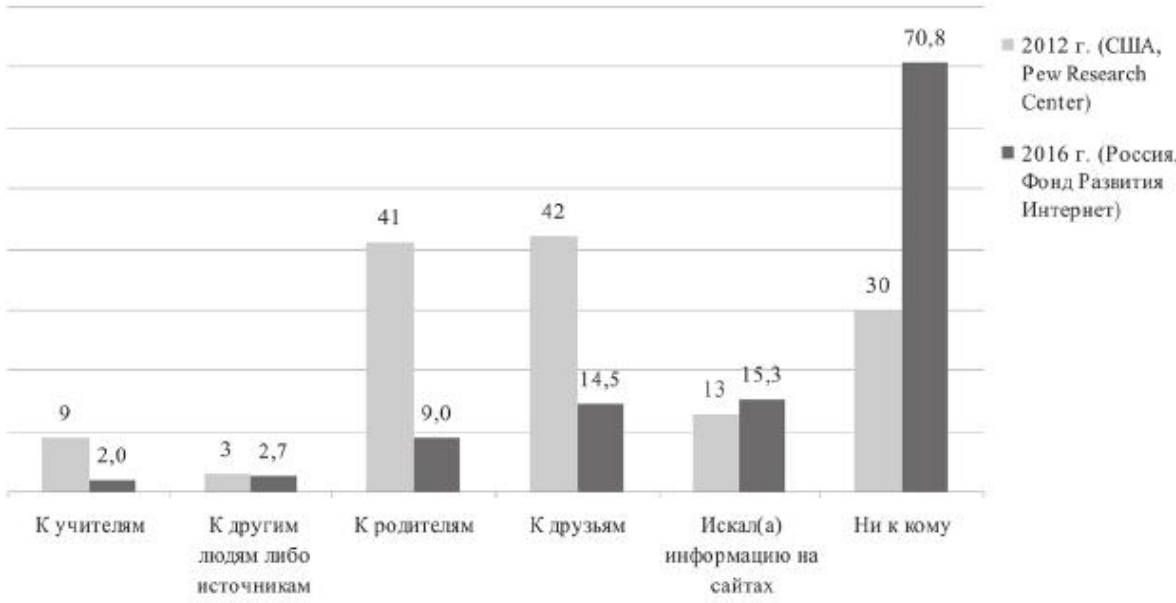


Рис. 10. Ответы подростков на вопрос:
«К кому ты обращался(ась) за помощью, когда тебе нужно было настроить приватность в социальной сети?», %

ной: в 2013 г. каждый второй ребенок пострадал от проблем, возникающих в результате ненадлежащего обращения с персональными данными в интернете. В 2016 г. этот уровень несколько снизился. Тем не менее как минимум треть российских подростков представляет собой группу риска по ненадлежащему хранению и распространению персональных данных и может пострадать от угроз, связанных с персональной информацией, поскольку эти дети:

- не всегда соблюдают принцип конфиденциальности в отношении своих паролей и сообщают их своему ближайшему окружению, некоторые дети готовы сообщить свой пароль незнакомому человеку;
- устанавливают открытый доступ к персональной страничке, то есть ее может видеть любой пользователь, зарегистрированный в социальной сети, а в личном профиле указывают достаточно много персональных данных;

- в том или ином объеме готовы передавать свои персональные данные незнакомым людям;
- ни к кому не обращаются за помощью по вопросам, связанным с настройками приватности в сети.

Несмотря на то что подростки все же начинают заботиться о приватности, они нередко выкладывают небезопасную информацию о себе, причем это делают даже те, кто проявил себя осторожным пользователем и обращается к взрослым за помощью в настройках приватности. Не только дети, но и их родители недооценивают скрытые угрозы беспечного использования и хранения персональных данных в сети, проблема обнаруживается лишь тогда, когда неблагоприятные последствия уже очевидны (взлом аккаунта, публикация материалов, списание денег со счета и т.д.).

Вышесказанное свидетельствует о необходимости организации специальных обучающих занятий для школьников по повышению знаний, умений и навыков грамотного обращения с персональными данными. У цифрового поколения во всем мире, несмотря на существующие культурные различия, формируется общий, но иной по сравнению с предыдущими поколениями взгляд на приватность в целом и персональные данные в частности. Учитывая высокую онлайн-активность детей и подростков, обучение их защите персональных данных в цифровом мире должно стать одной из приоритетных задач родителей и школы.

УРОКИ БЕЗОПАСНОСТИ

Цели, структура, принципы

Цели и задачи программы. Цель программы — повышение цифровой компетентности школьников в сфере управления персональными данными в интернете.

Формирование у школьников навыков эффективного управления персональными данными в интернете — новая и крайне актуальная педагогическая задача в информационном обществе. Среди подростков широко распространено представление об интернете как о пространстве свободы и вседозволенности, где, благодаря анонимности, можно делать все, что угодно, не опасаясь последствий своих действий (*Солдатова, Нестик и др.*, 2013). Тем не менее сегодня полноценное использование всех возможностей интернета практически неосуществимо без регистрации и предоставления онлайн-ресурсам определенного набора персональных данных. Делиться или не делиться личной информацией — этот вопрос каждый решает сам для себя. Сохранение полной приватности в интернете возможно лишь при условии цифровой изоляции — сознательного лишения себя всех тех уникальных возможностей, которые современные инфокоммуникационные технологии представляют для человека. Другая крайность — неведение и небрежное обращение с персональными данными, что делает пользователя уязвимым по отношению к многочисленным онлайн-рискам, начиная с кражи персональных данных и заканчивая преследованиями и шантажом. В такой ситуации осознанное управление персональными данными в интернете — это разумное решение, соответствующее «золотой середине» между этими крайними полюсами.

В ходе освоения программы учащиеся получат ответы на *три вопроса*, касающиеся эффективного управления персональными данными в сети:

1. Что такое персональные данные?
2. Почему необходимо защищать персональные данные?
3. Каким образом можно управлять персональными данными?

В соответствии с этими вопросами формулируются основные **задачи пособия**.

- Формирование у школьников представлений о приватности и персональных данных, а также способах попадания данных в интернет и их распространения в сети.
- Осознание школьниками ценности персональных данных, последствий неосторожного обращения с информацией личного характера в интернете и необходимости ее защиты.
- Формирование у школьников навыков управления персональными данными при работе с различными онлайн-ресурсами, приложениями и устройствами.

Основная целевая группа программы — ученики 6–10-х классов средних общеобразовательных школ. Проблема управления персональными данными наиболее актуальна именно для этого возраста. Ведущей деятельностью в жизни подростка становится интимно-личностное общение со сверстниками, удовлетворить потребность в котором в силу разных причин не всегда получается в реальной жизни. Взрослея, школьники начинают активно использовать инфокоммуникационные технологии для общения с друзьями. Как показывают исследования, более 80% подростков имеют аккаунты в социальных сетях, примерно половина из них использует интернет для общения и поиска новых друзей (*Солдатова, Нестик и др.*, 2013).

Хорошо известный в психологии феномен «случайного попутчика» объясняет, почему подросткам чаще бывает проще раскрыться и излить душу виртуальному знакомому, чем родным или друзьям. Тем не менее школьники не подозревают, что под личиной «случайного попутчика» может оказаться злоумышленник, выманивающий личную информацию с целью обмана, преследований, домогательств или шантажа. Поэтому крайне важно донести до подростков ценность личной информации, объяснить возможные последствия небрежного обращения с ней и научить их эффективным способам управления персональными данными.

Структура программы. Программа состоит из 10 уроков, которые в соответствии с поставленными задачами можно разделить на два основных раздела.

Раздел 1. Персональные данные: виды, пути распространения, защита.

- Урок 1 «Что такое персональные данные?»;
- Урок 2 «Какими бывают персональные данные?»;
- Урок 3 «Как персональные данные попадают в сеть?»;
- Урок 4 «Почему нужно управлять персональными данными?»;
- Урок 5 «Как защитить персональные данные?».

Раздел 2. Управление персональными данными.

- Урок 6 «Что такое приватность и личные границы?»;
- Урок 7 «Как настраивать приватность в сети?»;
- Урок 8 «Как управлять репутацией в интернете?»;
- Урок 9 «Что мой смартфон знает обо мне?»;
- Урок 10 «Как удалить персональные данные из интернета?».

Первый раздел программы направлен на формирование у школьников представлений о таких важных понятиях, как приватность и персональные данные, пути попадания личной информации в сеть и способы ее защиты. Подростковый возраст — это время, когда личность только начинает осознавать свои отношения с окружающим миром. Школьникам еще сложно определить для себя границу между личным и публичным в реальной жизни, а в интернете (в силу множества причин) сделать это еще сложнее. Как показывает практика работы Линии помощи «Дети Онлайн», в интернете проблемы зачастую возникают из-за того, что подросток просто не понимает, что является личной информацией, а что — нет. Во многом это связано с тем, что само понятие персональные данные — достаточно абстрактное и неоднозначное. В связи с этим на первых уроках программы школьники на конкретных примерах, взятых из жизни таких же пользователей-подростков, как и они, разбираются с тем, что такое персональные данные, какими они бывают и какими путями попадают в интернет.

Этот раздел направлен также на формирование мотивационной основы освоения программы. К сожалению, подростки не всегда осознают ценность персональных данных и последствия неосторожного обращения с ними. Многие из них, столкнувшись со взломом аккаунта в социальной сети, сразу же заводят себе новый, не задумываясь о рисках, которым они себя подвергают. Поэтому простые рассказы о способах защиты личной информации воспринимаются ими как нотации, далекие от их повседневных проблем. Как отмечает А.Г. Асмолов, бессмысленно давать детям ответы на вопросы, которые они не задавали сами (*Асмолов*, 2012). Главная цель данного раздела программы — поставить перед школьниками актуальные для них

задачи таким образом, чтобы вопросы о защите персональных данных исходили от них самих. Так, например, демонстрация реальных обращений на Линию помощи «Дети Онлайн» подростков, пострадавших от неосторожного обращения с персональными данными, способствует осознанию школьниками проблемы защиты персональных данных как актуальной жизненной задачи.

Второй раздел направлен на формирование у школьников навыков эффективного управления персональными данными. Как отмечалось выше, эта задача не имеет однозначного решения, и каждый пользователь решает сам для себя, как и где ему провести черту приватности в интернете. Поэтому данное пособие — это не просто набор рекомендаций по защите персональных данных, а система психолого-педагогических технологий, помогающих школьнику определить для себя границу приватности и выбрать те технические средства и приемы, которые помогут ему ее защитить.

Учитывая логику разделов, целесообразно проводить уроки с учащимися в той последовательности, в которой они представлены в пособии. Тем не менее учитель или классный руководитель могут самостоятельно составлять программу занятий в соответствии со спецификой аудитории и стоящими перед ними конкретными педагогическими задачами.

Структура урока. Каждый урок пособия имеет свои цели и задачи, а также определенную структуру, включающую разминку, основные упражнения и итоги занятия.

Разминка направлена на подготовку класса к работе: активизацию учеников, формирование у них интереса к теме урока, создание непринужденной и доброжелательной атмосферы в группе, повышение сплоченности.

Далее следуют основные упражнения, каждое из которых содержит описание:

- цели упражнения;
- необходимых материалов;
- процедуры проведения;
- вопросов для обсуждения.

Большинство упражнений носит проблемно-поисковый характер. Методические материалы и задания к ним построены таким образом, что они, актуализируя личный опыт учащихся, помогают им самостоятельно сформулировать проблему и найти ее решение. Обсуждение результатов упражнения — важный этап работы на уроке, помогающий учащимся отрефлексировать опыт, полученный в ходе выполнения заданий, а также подвести итоги. В некоторых случаях основные выводы по результатам упражнения приводятся в разделе «В помощь ведущему». Все необходимые методические материалы для учащихся, а также ключи к заданиям для ведущего содержатся в приложениях к упражнениям. Большинство уроков также содержит раздел «Полезная информация» с дополнительными материалами по теме урока, которые могут быть интересны всем участникам занятия.

В конце каждого занятия ведущий подводит итоги, используя материалы, представленные в одноименной рубрике. Главные задачи этого этапа — дать ответы на все вопросы, поставленные учащимися, обобщить опыт, полученный в ходе урока, а также предложить учащимся решение поставленной проблемы.

Ведущему целесообразно придерживаться предложенной схемы урока, а при подготовке к занятию необходимо внимательно ознакомиться с ее содержанием, обращая особое внимание на рубрики «В помощь ведущему» и «Итоги занятия».

Также следует заранее подготовить все необходимые для урока материалы.

В программе учитываются **возрастно-психологические особенности** учеников 6–10 классов. Традиционно психологами и педагогами подростковый возраст принято рассматривать как один из наиболее сложных и кризисных периодов жизни, что связано, в первую очередь, с гетерохронией физиологического, социального и психического развития подростка. В современном обществе подросток — все еще несовершеннолетний ребенок, чаще всего не готовый к самостоятельной жизни и трудовой деятельности. Статус подростка носит промежуточный характер. Как писал основоположник отечественной психологии Л.С. Выготский, подросток — уже не ребенок и должен отвечать за свои поступки, но он еще не взрослый и не может самостоятельно управлять своей жизнью (*Выготский*, 2000).

В качестве центрального новообразования подросткового возраста психолог Д.Б. Эльконин рассматривал чувство взрослости, которое выражается в стремлении подростка быть независимым, самостоятельно принимать решения и действовать, как взрослый. Довольно часто подростков не устраивает та степень свободы и самостоятельности, которую предоставляют им родители в реальной жизни. Поэтому они устремляются в виртуальную реальность, воспринимаемую ими как территорию безграничной свободы. Интернет — как раз то место, где подросток может почувствовать себя свободным от контроля со стороны родителей и учителей (*Эльконин*, 2001).

Поскольку общество в лице родителей и учителей не всегда готово увидеть «взрослого» в подростке, эта потребность чаще всего удовлетворяется в группе друзей-сверстников. Общение со сверстниками становится ведущей деятельностью подросткового периода и играет решающую роль в развитии личности

подростка. Именно в группе сверстников происходит усвоение новых социальных ролей, а также морально-нравственных норм поведения. Поэтому не случайно, что львиную долю пользователей различных социальных сетей составляют именно подростки, испытывающие колоссальную потребность в общении со сверстниками.

Подростковый возраст — это также возраст первой влюбленности, время, когда подростки учатся общаться с противоположным полом и устанавливать тесные эмоциональные взаимоотношения. Для младших подростков общение с представителями противоположного пола — это очень деликатный процесс, который часто сопровождается смущением и неловкостью. Поскольку знакомства через интернет в значительной мере упрощают процесс общения и помогают преодолеть многие коммуникативные барьеры, подростки все чаще предпочитают реальному общению виртуальное.

Развитие самосознания в подростковом возрасте приводит к стремлению подростка понять самого себя и найти свое место в этом мире. Л.И. Божович подчеркивала, что часто процесс самопознания может принимать формы самоиспытания в различных экстремальных ситуациях (*Божович*, 2001). Подросток как бы проверяет себя на прочность, пытается найти границы собственного «Я». Интернет предоставляет подросткам совершенно уникальные возможности для самопознания и самоопределения в различных социальных группах и контекстах, которых они не имеют в реальной жизни (*Божович*, 2001).

А.Н. Леонтьев определял подростковый возраст как время второго рождения личности, возраст формирования иерархии мотивов и ценностей путем выбора и подчинения одних мотивов другим — смыслообразующим мотивам личности (*Леонтьев*, 1983). Эти мотивы в дальнейшем играют судьбоносную роль

в жизни человека, определяя уникальную траекторию и стратегию его жизненного пути. Именно поэтому столь значимо овладение в подростковом возрасте информационными технологиями, открывающими новые возможности для компетентного и осознанного выбора (*Леонтьев*, 1983).

В наше время интернет становится ключевым фактором развития мотивационной сферы цифрового поколения, задавая подросткам новые цифровые ориентиры развития личности. С одной стороны, это неизбежно вызывает тревогу у представителей старшего поколения, поскольку эти ориентиры пока еще не прошли проверку временем, и довольно трудно предположить, куда они могут привести сегодняшних подростков. С другой стороны, интернет как уникальный по своим масштабам, форме и содержанию источник культурно-исторического опыта предоставляет массу возможностей для самоопределения и развития личности подростка.

Методические принципы. Уроки разрабатывались в соответствии со следующими принципами культурно-деятельностного подхода в психологии и педагогике.

Принцип активной включенности. Ученик является таким же равноправным участником учебного процесса, как и учитель. В связи с этим все задания направлены на формирование активной позиции учащихся и актуализацию их личного опыта, который обогащается и обобщается на уроке в ходе совместной деятельности с другими учениками. Благодаря этому, знания, которые школьники получают на занятиях, сразу могут быть использованы в их повседневной деятельности.

Принцип деятельностных технологий. На уроках широко используются интерактивные образовательные технологии (деловые и ролевые игры, обсуждение конкретных случаев, проектные задания, групповые дискуссии и т.д.), предполагающие

организацию совместной деятельности учеников и учителя. Ученики получают новые знания не в готовом виде, а в форме проблемно-поисковых задач, стимулирующих их собственную познавательную активность.

Принцип доступности. Все учебные материалы разработаны в соответствии с возрастно-психологическими особенностями школьников, а также имеющимся у них социальным опытом. Это обеспечивает соответствие упражнений реальным жизненным задачам, стоящим перед учащимися.

Принцип системности. Содержание предлагаемых уроков структурировано в соответствии с представлениями о деятельности детей среднего школьного возраста в интернете, а также о возможных рисках и угрозах в сети для детей данного возраста. На уроках школьники знакомятся с особенностями распространения персональных данных в интернете, основными рисками небрежного обращения с ними и способами эффективного управления информацией личного характера в сети.

Принцип рефлексивности. Важное место в структуре уроков занимает обсуждение результатов занятия. Критическое осмысление полученной на уроке информации и соотнесение ее со своим личным опытом формирует у школьников способность к рефлексии собственной «компьютерной» деятельности, что является залогом их безопасности в интернете.

Принцип мотивации. Значительное внимание в ходе занятий уделяется формированию мотивационной основы обучения. Благодаря методическим приемам, которые используются в ходе уроков, а также адекватно подобранному материалу, у школьников формируется интерес к проблеме управления персональными данными в интернете как к реальной жизненной задаче, стоящей перед ними.

Принцип открытости. Содержание уроков предполагает достаточно гибкое использование преподавателем предложенной

программы, при этом не допускает искажения логики, содержательной точности и достоверности информации.

Принцип кроссплатформенности. Темпы развития современных инфокоммуникационных технологий высоки, поэтому задача программы — сформировать у учащихся универсальные способы действий, которые носили бы кроссплатформенный характер и позволяли им эффективно управлять своими персональными данными при использовании различных устройств, приложений и ресурсов. Поэтому задания программы не привязаны к каким-то конкретным платформам, а знания, полученные учениками на занятиях, легко могут быть адаптированы для работы в любой онлайн-среде.

Рекомендации по проведению уроков. Занятия могут быть использованы как в рамках основной школьной программы, например, на уроках по информатике или ОБЖ, так и внеклассной работы, например, на классном часе или в работе клубов или кружков. Также программа может быть реализована в лагере во время каникул или в качестве дополнительного образования.

Целесообразно проводить занятия регулярно, с периодичностью 1 урок в 1–2 недели. Продолжительность каждого урока составляет 45 минут. В некоторых случаях ведущий может увеличить время занятия до 1–1,5 часов за счет более глубокого и подробного обсуждения результатов каждого упражнения.

Оптимальное количество учеников в классе — 15–25 человек. Если в классе более 25 человек, целесообразно разделить его на две равные подгруппы.

Занятия должны проходить в отдельном, просторном, хорошо проветриваемом помещении. Класс должен быть оснащен всем, что может понадобиться для работы: доской или флипчартом, стульями и партами. В ходе урока может использоваться как обычная рассадка учеников в ряд за партами, так и кругом на

стульях. В последнем случае учащимся необходимо раздать планшеты или любые другие устройства для письма.

Правила работы в группе. Большая часть упражнений предполагает, что ученики сообщают о себе определенную информацию личного характера в устной или письменной форме. В связи с этим полезно будет с самого начала обсудить те правила, которые будут регулировать работу с персональными данными в группе.

Правило добровольности. Если учащийся затрудняется сообщить о себе определенную личную информацию, он имеет право отказаться от выполнения задания. Тем не менее это не означает полного отказа от участия в упражнении. Наравне со всеми он может выполнять упражнения, не предполагающие разглашения персональных данных, принимать участие в обсуждении результатов либо ограничиться частичным выполнением задания.

Правило конфиденциальности. Ничто из того, о чем говорится в группе относительно конкретных участников, не должно стать достоянием третьих лиц. Это естественное этическое требование ответственного отношения к чужим персональным данным — базовое условие создания атмосферы доверия и безопасности в классе.

Принцип безоценочности. Задания, выполняемые в ходе урока, не имеют правильных или неправильных ответов, поэтому ведущий должен в первую очередь поощрять активность учащихся, а не результаты выполнения уроков. И учитель, и ученики должны, во-первых, избегать оценочных, в первую очередь негативных высказываний в отношении других учеников, и, во-вторых, уважать точку зрения каждого участника.

Принцип бережного обращения с персональной информацией. Если выполнение задания предполагает сообщение участниками

личной информации в письменном виде (заполнение различных бланков или опросников), ведущий после урока должен удостовериться, что все материалы были либо уничтожены, либо попали обратно в руки к их владельцам, тем самым подчеркивая необходимость аккуратного обращения с персональными данными как в реальной жизни, так и в интернете.

Все учебные материалы разработаны в соответствии с действующим российским законодательством, а также с учетом мирового опыта в сфере управления и защиты личных данных. Ниже представлен *перечень основных законодательных актов* по проблеме персональных данных.

- Всеобщая декларация прав человека (принята резолюцией 217 А (III) Генеральной Ассамблеи ООН от 10.12.1948).
- Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ).
- Конвенция о защите физических лиц при автоматизированной обработке персональных данных (ETS N 108) (рус., англ.) (от 28.01.1981 с изменениями, внесенными Международным договором от 15.06.1999). Ратифицирована Федеральным законом РФ от 19.12.2005 № 160-ФЗ.
- Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 29.06.2015) «О защите детей от информации, причиняющей вред их здоровью и развитию».
- Федеральный закон от 28.07.2012 № 139-ФЗ (ред. от 14.10.2014) «О внесении изменений в Федеральный закон “О защите детей от информации, причиняющей вред их

здоровью и развитию" и отдельные законодательные акты Российской Федерации».

- Федеральный закон от 28.12.2013 № 398-ФЗ «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации"».
- Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных» (с изм. и доп., вступ. в силу с 01.09.2015 в ред. Федеральных законов от 25.11.2009 № 266-ФЗ, от 27.12.2009 № 363-ФЗ, от 28.06.2010 № 123-ФЗ, от 27.07.2010 № 204-ФЗ, от 27.07.2010 № 227-ФЗ, от 29.11.2010 № 313-ФЗ, от 23.12.2010 № 359-ФЗ, от 04.06.2011 № 123-ФЗ, от 25.07.2011 № 261-ФЗ, от 05.04.2013 № 43-ФЗ, от 23.07.2013 № 205-ФЗ, от 21.12.2013 № 363-ФЗ, от 04.06.2014 № 142-ФЗ, от 21.07.2014 № 216-ФЗ, от 21.07.2014 № 242-ФЗ).
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями).
- Гражданский кодекс РФ, Часть 1, Раздел I, Глава 8, Статья 152 «Защита чести, достоинства и деловой репутации».
- Указ Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями и дополнениями от 23.09.2005, 13.07.2015).

Урок № 1

ЧТО ТАКОЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ?

Цель: знакомство с понятием «персональные данные».

Разминка «Интернет-викторина»

Задача: сформировать у учащихся интерес к теме занятий; актуализировать их знания об онлайн-ресурсах.

Необходимые материалы: карточки для викторины (см. Приложение к уроку № 1.1), доска.

Время проведения: 15–20 минут.

Процедура проведения

Начиная цикл занятий, ведущий предлагает участникам проверить их знания об интернете: насколько хорошо им знакомы различные онлайн-ресурсы. С этой целью проводится мини-викторина. Ведущий зачитывает карточки с фактами, а участники должны угадать, о каких известных интернет-ресурсах идет речь (см. Приложение к уроку № 1.1). Если задание вызывает затруднения у группы, ведущий может дать подсказку, которая также содержится на карточке. Названия угаданных сайтов ведущий выписывает на доске. По ходу викторины ведущий ведет счет: за каждый правильный ответ участник получает один балл. Побеждает участник, набравший больше всех баллов.

Обсуждение

- Что нового вы узнали из этого упражнения?
- Какие факты больше всего вас удивили?
- Что объединяет часть из отгаданных онлайн-ресурсов и чем отличаются некоторые из них?

Упражнение «Мой профиль»

Задача: объяснить учащимся, что такое персональные данные, и показать, как безличная информация становится персональной.

Необходимые материалы: форма для заполнения по количеству учеников (см. Приложение к уроку № 1.2), доска.

Время проведения: 20–25 минут.

Процедура проведения

Переходя от обсуждения результатов разминки к новому упражнению, ведущий обращает внимание участников группы на то, что некоторые из отгаданных онлайн-ресурсов объединяет одна важная особенность — для получения полного доступа ко всем возможностям этих сайтов на них необходимо зарегистрироваться.

Наверняка процедура регистрации хорошо знакома всем участникам группы: она, как правило, предполагает заполнение регистрационной формы. Чтобы разобраться в этом вопросе более глубоко, ведущий предлагает участникам выполнить следующее задание:

«Представьте, что в интернете появился новый популярный ресурс. Он объединяет возможности уже существующих ресурсов: социальных сетей, видеохостингов, викисред, онлайн-каналов, а также содержит новые уникальные возможности для учебы и отдыха. Большинство ваших друзей уже зарегистрированы на новом ресурсе, поэтому вам не терпится тоже туда поскорее попасть. Для этого вам всего лишь нужно заполнить простую регистрационную форму».

После этого ведущий раздает участникам формы регистрации и просит их заполнить (см. Приложение к уроку № 1.2). На

выполнение этого задания отводится 5 минут. Затем ведущий собирает заполненные формы и говорит участникам группы о том, что после регистрации на ресурсе вся информация из профиля, кроме пароля, становится доступной для всех пользователей, зарегистрированных на сайте, а если профиль открыт, то и для посторонних.

Что же говорит о нас информация, размещенная в профиле? Чтобы получить ответ на этот вопрос, ведущий в случайном порядке раздает заполненные профили участникам группы и ставит перед ними задачу: угадать, чей это профиль, и написать свою догадку на полученном листке с профилем. На выполнение этой задачи также отводится 5 минут. Важно, чтобы в это время участники группы не подсказывали друг другу и не высказывали свои догадки вслух.

Когда все участники выполнят задание, ведущий просит каждого по очереди озвучить логин хозяина профиля, а затем высказать и обосновать предположение по поводу его личности. Только после того, как все догадки будут высказаны, ведущий просит хозяев профилей подтвердить или опровергнуть правильность ответов. На эту часть упражнения может уйти от 10 до 15 минут в зависимости от числа участников и активности группы. Когда все ответы озвучены и проверены, можно переходить к обсуждению результатов упражнения.

После завершения упражнения ведущий возвращает каждому участнику заполненный им профиль и отмечает необходимость бережного обращения со своими персональными данными.

Обсуждение

- Какой профиль было угадать проще/труднее всего?
- Что помогло/помешало угадать личность хозяина профиля?
- Какими соображениями мы руководствуемся, заполняя профили?

Итоги занятия

Подводя итоги, ведущий говорит о том, что информация, размещенная в профилях, называется персональными данными.

Персональные данные — это любая информация, которая имеет отношение к конкретному человеку.

«Как можно было убедиться в ходе выполнения упражнения, персональные данные позволяют нам установить или идентифицировать личность человека. Чем больше информации о себе я размещаю в интернете, тем проще другим пользователям установить мою личность. Информация, размещенная нами в интернете, влияет на нашу репутацию в сети и помогает находить новых друзей со сходными увлечениями и интересами.

Каждый из нас имеет право самостоятельно принимать решение о том, какую информацию о себе размещать в интернете».

Что современные подростки знают о персональных данных?

Ученицы 8-го класса подмосковной гимназии отвечают на вопросы журнала «Дети в информационном обществе».

— Есть ли у вас страничка в социальной сети, и кто помогал вам настраивать там приватность? Что вы знаете про приватность вообще?

Вика: У меня есть несколько почт, и я сижу в анонимных чатах, но меня нет в социальных сетях. Я раньше там была, но мне не нравится именно то, что, хотя они вроде бы приватные, их могут видеть многие. А я не хочу, чтобы видели мои фото. И поэтому я просто удалилась из всех социальных сетей. А в чатах просто заходишь, вбиваешь никнейм и все, там не нужна регистрация. Там создается беседа для какого-либо количества человек, и если ты ее покидаешь, то это навсегда. И это анонимно. Я там общаюсь с незнакомыми людьми.

Настя: У меня есть странички в нескольких социальных сетях: на Фейсбуке, на Тамблере, в Инстаграме и еще электронная почта. Чаще всего, конечно, я использую ВКонтакте, в остальные даже не всегда захожу, потому что создавала их не для общения. Например, иногда для какого-то приложения или магазина обязательно нужна регистрация на Фейсбуке. Первый раз, когда я еще была совсем маленькой, мне помогала моя старшая сестра. Она вообще помогала осваиваться в интернете, создавать почту, ну и страничку тоже. Затем, когда я стала постарше, все настройки я делала сама. А вообще приватность — это то, как защищены наши данные в интернете. И мы можем настраивать, кто видит наши записи, публикации. Их могут видеть все или только избранные, друзья,

близкие, знакомые и т.д. Приватность — это очень спорное понятие в интернете, поскольку при особых знаниях и умениях можно обойти любые настройки.

Алина: Я чаще всего использую ВКонтакте, когда-то была в Одноклассниках, но сейчас не пользуюсь. Еще недавно зарегистрировалась в Instagram и на AskMe. Вообще, мне родители достаточно поздно разрешили зарегистрироваться ВКонтакте, классе в 4-м или 5-м. Интернетом уже умела пользоваться и настраивала все сама, прочитала правила — кого, как заблокировать — и сама настроила.

— Какую информацию о себе вы сообщаете и не сообщаете незнакомым людям в интернете?

Вика: Я сообщаю свой пол, возрастную группу (но не точный возраст) и примерное место проживания. Называю Москву, хотя живу в области. Я не публикую свои фото, даже если просят, не называю фактический адрес. Очень редко — говорю реальное имя, но обычно использую ник.

Настя: Я редко общаюсь в сети с незнакомыми людьми, только некоторое время назад я общалась в одном чате с американскими студентами. Я свободно сообщаю место проживания — Россия, Московская область, Балашиха; возраст, свое имя. Какие-то элементы нашей жизни описывала — например, про то, как мы учимся в школе. А если кто-то незнакомый пишет, я стараюсь вообще не продолжать разговор.

Алина: Я вообще не общалась с незнакомыми людьми в сети, переписываюсь только с теми, кого видела и с кем знакома лично. А если сами пишут — избегаю. Бывает, напишет знакомый знакомого, тогда могу сказать, где учусь и в каком классе. На страничке моей есть фотография, мой город и возраст, а свой точный адрес я не сообщаю.

— А вы сталкивались когда-нибудь со взломом вашего аккаунта? Что вы предприняли?

Вика: У меня раньше был аккаунт в Одноклассниках. Я его забросила где-то на полгода, а потом стало интересно посмотреть, что с ним стало. Я зашла и обнаружила кучу групп, на которые я точно не подписывалась. Это не мог быть кто-то из домашних, и, как я узнала из списка посещений по IP, посещался он людьми из Таиланда. Мне это совсем не понравилось. После этого я поменяла пароль, поскольку не нашла, как удалить эту страничку, и больше туда не захожу.

Настя: Я столкнулась со взломом буквально месяц назад, когда сидела на уроке, а кто-то из ребят говорит: «Настя, ты онлайн? Ты мне прислала какую-то ссылку». Я ответила, что не присылала. Поняла, что, скорее всего, это — взлом, и, когда уже стала заходить в социальную сеть, увидела что-то вроде «на ваш телефон отправлено СМС, введите код активации, вас взломали». Но поскольку номер был старый, я не смогла его восстановить, и пришлось зарегистрироваться заново. Ни к кому не обращалась, у меня не было там чего-то, что я хотела бы скрыть.

Алина: Со взломом я не сталкивалась. Буквально два месяца назад я сделала так, что при входе на страницу ВКонтакте мне приходит код на телефон: я его ввожу и захожу в свой аккаунт.

Приложение № 1.1

Foursquare Этот сервис позволяет любому пользователю стать мэром. **Подсказка** Название этого сервиса переводится как «четыре в квадрате»	**Instagram** Здесь возможен не только квадратный формат, но и альбомный, и портретный. **Подсказка** Это сервис быстрого обмена фотографиями и видеозаписями
Википедия Статистика свидетельствует, что пользователи чаще обращаются к этому сервису при плохой погоде. **Подсказка** Этот ресурс содержит в 65 раз больше статей, чем последнее издание Британской энциклопедии	**Twitter** Библиотека Конгресса США ведет архив всех сообщений, опубликованных пользователями этого ресурса. **Подсказка** Объем сообщения на этом сервисе ограничен 140 знаками
Facebook В Австралии повестка в суд, размещенная на странице пользователя этого ресурса, является юридически обязательной. **Подсказка** Сегодня этот ресурс — крупнейшая в мире социальная сеть	**YouTube** Если бы этот ресурс был голливудской кинокомпанией, у него было бы достаточно материала для выпуска 60 000 новых фильмов каждую неделю. **Подсказка** Для просмотра всех роликов, размещенных на этом ресурсе, понадобится более 1700 лет
ВКонтакте Этот ресурс начинался как закрытое приложение к форуму СПбГУ. **Подсказка** Сегодня это — самая популярная социальная сеть в России	**Live Journal** Символ этого ресурса — козел Фрэнк. **Подсказка** Название сервиса переводится как «живой журнал»
Яндекс Слоганом одной из рекламных кампаний этого ресурса была фраза «Найдется все!» **Подсказка** Этот ресурс — четвертый по популярности поисковик в мире	**WhatsApp** Это приложение позволяет пользователям смартфонов бесплатно обмениваться мгновенными сообщениями. **Подсказка** Название этого ресурса созвучно с фразой, которая переводится как «Что происходит?»

Приложение № 1.2

Создание учетной записи

Логин*	
Пол*	○ Мужской ○ Женский
Возраст*	
Электронная почта*	_____@_____
Номер мобильного телефона	+7 (_____) _____-_____-_____
Пароль*	
Подтверждение пароля*	
Страна	
Город	
Skype	
Семейное положение	
Образование	
Место работы/учебы	
Интересы	
Любимая музыка	
Любимые книги	
Любимые кинофильмы	
Любимые телепередачи	

Создать учетную запись

Урок № 2

КАКИМИ БЫВАЮТ ПЕРСОНАЛЬНЫЕ ДАННЫЕ?

Цель: знакомство с видами персональных данных.

Время: 45 минут.

Разминка «Личное — публичное»

Задача: сформировать у учащихся интерес к теме занятия.

Необходимые материалы: небольшой мячик.

Время проведения: 5–10 минут.

Процедура проведения

В начале урока ведущий напоминает участникам группы о понятии «персональные данные», введенном на прошлом занятии, и обращает внимание учеников на то, что любая безличная информация становится личной, как только мы сами или кто-то другой устанавливает отношение между этой информацией и собой. Эти отношения могут быть очень разными, например:

- Безличная информация: «Москва — город-герой». Персональная информация: «Я живу в Москве».
- Безличная информация: «Луна — искусственный спутник Земли». Персональная информация: «Я мечтаю побывать на Луне».
- Безличная информация: «Шарик — небольшая сфера». Персональная информация: «Моего пса зовут Шарик».

Для закрепления этого материала и подготовки к следующему упражнению ведущий предлагает группе поиграть в простую игру. Ведущий бросает одному из участников группы мячик вместе с сообщением, содержащим определенную безличную информацию, например: «Великая Китайская стена — самая длинная постройка в мире». В ответ участник должен переделать безличную информацию в личную (например: «Я никогда не видел Великую Китайскую стену») и вернуть мячик обратно ведущему. Игра продолжается 5–10 минут.

Обсуждение

- Насколько легко/трудно устанавливать связь между безличной информацией и собой?
- Как вы понимаете фразу: «отсутствие информации — это тоже информация»? Насколько информативным может быть отсутствие информации?
- Всякая ли безличная информация может стать личной? Если нет, попробуйте найти примеры такой информации.

Упражнение «Информационный светофор»

Задача: рассказать учащимся о существующих видах персональных данных и помочь им осознать уровень их значимости.

Необходимые материалы: разноцветные стикеры двух цветов (красные и зеленые) — по пять на каждого участника, доска или проектор.

Время проведения: 20 минут.

Процедура проведения

Упражнение выполняется в три этапа.

Первый этап. Ведущий говорит участникам группы о том, что каждый из нас сам принимает решение, какую персональ-

ную информацию выкладывать в интернет, а какую — нет. Он раздает по десять стикеров каждому участнику группы (пять красных и пять зеленых) и просит их подумать: какую информацию о себе они с легкостью готовы выложить в интернет, а какую — нет. Информацию, которой участник готов поделиться, он пишет на зеленых листочках (например, имя, возраст, пол и т.д.), а ту, которой не готов — на красных (например, номер телефона, адрес и т.д.). На выполнение этого задания отводится 5 минут. Упражнение можно усложнить, если выдать участникам группы также по пять желтых стикеров и попросить написать на них информацию, которой они готовы поделиться только с друзьями.

Второй этап. После того как первое задание выполнено, ведущий предлагает ученикам разделиться на несколько микрогрупп по 3–5 человек в каждой. Ведущий просит каждого участника пометить свои стикеры. Далее участники микрогруппы должны объединить все стикеры — и те, которыми готовы поделиться в сети, и те, которыми не готовы, и попытаться их классифицировать по видам и каждому из видов дать свое название. На выполнение этого задания отводится 5–7 минут. Затем ведущий просит представителя каждой микрогруппы назвать виды стикеров, которые у них получились, и описать их содержание. Названия выписываются на доску.

Третий этап. Ведущий показывает с помощью проектора или выписывает на доску виды персональных данных (см. Приложение к уроку № 2.1) и обсуждает их с группой. Затем он предлагает участникам выйти и наклеить свои стикеры рядом с названием соответствующего вида персональных данных. После этого группа обсуждает результаты упражнения.

Обсуждение

- Какой вид данных набрал больше всего красных/зеленых стикеров? Почему?
- Какой вид информации набрал меньше стикеров? Почему мы о нем забыли?
- Какой информацией мы делимся более/менее охотно? Почему?

Упражнение «Детективное бюро»

Задача: научить участников определять, какую персональную информацию могут содержать различные материалы, размещаемые в сети.

Необходимые материалы: карточки с заданиями (см. Приложение к уроку № 2.2), комментарии для ведущего (см. Приложение к уроку № 2.3).

Время проведения: 20 минут.

Процедура проведения

В начале упражнения ведущий говорит: «Мы с вами узнали, что существуют разные виды персональных данных. Сообщение, выложенное в интернет, может содержать сразу несколько видов персональных данных. Например, фотография или видеозапись может рассказать другим пользователям не только о нашей внешности, но и о нашем местоположении, наших друзьях и т.д. Важно научиться аккуратно обращаться с личными данными и по ошибке не выложить в сеть информацию, которую хотелось бы сохранить в тайне».

Ведущий предлагает участникам группы разделиться на несколько микрогрупп по 3–5 человек. Каждая микрогруппа —

это небольшое детективное агентство, которое получает в качестве улики карточку с постом из социальной сети. Задача группы — провести расследование и узнать как можно больше информации об авторе этого поста. На выполнение задания отводится 5–7 минут. Затем каждая группа кратко представляет результаты своего расследования. Участники других групп могут задавать вопросы и делать свои комментарии. Ведущий в процессе обсуждения сверяется с комментариями (см. Приложение к уроку № 2.3). В конце занятия общим открытым голосованием определяется группа, которая провела самое тщательное и точное расследование и собрала максимальное количество персональных данных.

Обсуждение

- Какие материалы содержат в себе больше информации: текст или изображение? Почему?
- Какие виды персональной информации, размещенной в сети, более/менее однозначны? Почему?
- Всегда ли информация, которую мы размещаем в интернете, говорит о нас то, что мы хотим?

Итоги занятия

Подводя итоги занятия, ведущий еще раз напоминает участникам, что существуют разные виды персональной информации. Некоторыми видами данных большинство из нас охотно делится с другими, в том числе в интернете, иные мы предпочитаем хранить при себе, а о некоторых вообще не задумываемся. В любом случае каждый из нас имеет право принимать решение, какой информацией о себе делиться с другими пользователями, а какой — нет.

Тем не менее необходимо помнить, что неосторожное обращение с персональными данными может привести к «утечке» важной и значимой для нас информации, которой мы не хотели бы делиться с другими. Прежде чем выкладывать в интернет какой-либо материал (иначе говоря, оставлять «цифровые следы»), следует хорошо подумать, какая персональная информация в нем содержится и как она может быть использована другими пользователями.

Приложение № 2.1

ВИДЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

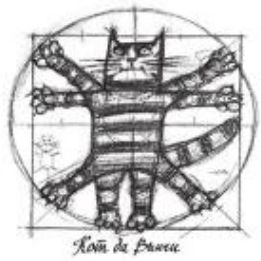
- **Регистрационные идентификационные данные** (паспортные данные, пароли, пин-коды).
- **Физические характеристики** (внешние данные, биометрические данные, состояние здоровья и др.).
- **Пространственная локализация** (фиксация местоположения и перемещения).
- **Материально-экономическое положение** (движимое, недвижимое имущество, зарплата, накопления и др.).
- **Официальные статусы** (семейное положение, достижения, награды, наличие судимостей и т.д.).
- **Профессиональная занятость** (включая образование).
- **Социальные связи** (информация о родственниках, друзьях, знакомых, принадлежность к различным формальным и неформальным группам).
- **Образ жизни и поведенческие установки** (мировоззрение, ценности, интересы и хобби, социальные привычки и действия, настроения, вкусы, особенности).
- **Психологические особенности** (черты характера, способности, знания, умения, навыки, личностные черты).
- **Хроника личных событий**.

Приложение № 2.2

КАРТОЧКИ С ЗАДАНИЯМИ

Карточка № 1	
 **Арина** Как же я люблю это время года!	
	Маша: Аринка, отлично выглядишь! Ты это где?)

Карточка № 2	
 **Анджела Гусева** Наконец-то вытащила Машку на прогулку!!!)))	
	Линочка Смирнова: молодец!!! Так и надо!!! Маму от дочки не отличишь!!!

Карточка № 3	
 **Денис Бобров** Принимаю поздравления!	
	Злой Фотограф Отличный кадр! Ждем продолжения!

Карточка № 4	
 **ЛеноК** Хорошо погуляли!	
	Дашутка Точно)))

Карточка № 5	
 **Каринка** Еще вопросы будут?	
	Тимур А еще СНИЛС и ИНН)))

Приложение № 2.3

КОММЕНТАРИИ ДЛЯ ВЕДУЩЕГО

При обсуждении результатов упражнения ведущий должен обратить внимание учеников на то, что информация, размещенная в интернете, никогда не может быть однозначно интерпретирована на 100%. Всегда существует вероятность того, что мы имеем дело с подставным профилем или информацией, намеренно искаженной автором. Еще более неоднозначную информацию содержат отдельные посты, вырванные из ленты. Во всех случаях по комментариям мы можем проследить социальные связи авторов постов.

Пример № 1. В данном случае можно предположить, что автор поста — молодая девушка или женщина. Мы можем сделать вывод о некоторых особенностях ее внешности, однако идентифицировать ее практически невозможно, так как на фото она стоит к нам спиной.

Пример № 2. Мы можем предположить, что на фотографии изображены мать и дочь. Фотография содержит информацию об их внешности, семейных отношениях, образе жизни, привычках, об их совместной поездке на природу. Комментарий к фотографии предоставляет нам информацию о родственной связи изображенных на ней женщин. Исходя из подписи под фото, можно предположить, что, скорее всего, автором поста является мама.

Пример № 3. На фотографии, по всей видимости, изображен автор поста и его невеста. В этом случае мы располагаем информацией об их внешнем виде, семейном положении, образе жизни, интересах, материальном положении. Изображение Эйфелевой

башни на заднем плане дает возможность установить местоположение пары.

Пример № 4. Скорее всего, на фото изображена автор поста. По-видимому, фотография сделана на память о значимом событии. Изображение Собора Василия Блаженного на заднем плане дает возможность установить, что фото сделано на Красной площади в Москве.

Пример № 5. Автор поста выложила собственную фотографию и паспорт: мы видим ее паспортные данные (Ф.И.О.; дата и место рождения; номер, серия, место и дата выдачи паспорта). Также мы совершенно точно знаем, как она выглядит.

Урок № 3

КАК ПЕРСОНАЛЬНЫЕ ДАННЫЕ ПОПАДАЮТ В СЕТЬ?

Цель: знакомство со способами попадания персональных данных в интернет и средствами защиты личной информации.

Разминка «Великий идентификатор»

Задача: помочь учащимся понять, как по «цифровым следам» можно идентифицировать пользователей сети.

Время проведения: 10 минут.

Процедура проведения

Даже небольшие фрагменты личной информации, которые на первый взгляд кажутся совершенно безобидными, можно, проанализировав, сложить воедино и довольно точно идентифицировать их владельца.

Классу предлагается следующая игра. Ведущий обращается к группе: «Сейчас я загадаю определенного человека. Это может быть как реально существующий или живший раньше, так и вымышленный человек, например, герой повести или кинофильма. Ваша задача — по очереди задавать мне вопросы, на которые можно дать ответ «да» или «нет», чтобы как можно быстрее угадать человека, которого я загадал. Давайте посмотрим, сколько потребуется вопросов, чтобы дать правильный ответ».

Как правило, чтобы дать правильный ответ, нужно задать не более 20 вопросов. Участник группы, первым давший правильный ответ, загадывает «своего» человека. Если игра понравилась участникам, ее можно повторить несколько раз.

Обсуждение

- Кого угадать было проще, а кого сложнее? Почему?
- Какая информация лучше всего помогает нам установить личность человека, т.е. идентифицировать его? Почему?
- Как вы думаете, легко ли установить личность человека в реальной жизни? Почему?

Упражнение «Цифровой след»

Задача: показать, какие «цифровые следы» могут храниться в компьютере и других устройствах, а также познакомить учащихся с тем, какими способами персональные данные попадают в интернет.

Необходимые материалы: набор из 9 карточек со скриншотами «цифровых следов» (см. Приложение к уроку № 3.1), лист с правильными ответами и пояснениями для ведущего (см. Приложение к уроку № 3.2).

Время проведения: 15 минут.

Процедура проведения

Упражнение состоит из двух этапов.

Первый этап. Класс делится на подгруппы по 3–4 ученика. Если класс небольшой, то можно работать в парах и даже по одному. Каждая группа получает карточку с изображением скриншота, содержащего «цифровой след» пользователя (см. Приложение к уроку № 3.1). Задача — определить, какой вид персональной информации содержит этот скриншот. Для того чтобы ребята поняли алгоритм выполнения задания, ведущий приводит пример анализа одной из карточек по выбору, пользуясь ключами (см. Приложение к уроку № 3.2). На выполнение

задания отводится 5 минут. Затем каждая подгруппа по очереди озвучивает свой ответ. Ведущий сверяет ответы с ключами и в случае необходимости задает участникам наводящие вопросы (см. Приложение к уроку № 3.2).

Второй этап. Все карточки выкладываются на один стол или прикрепляются на доску. Ведущий обращает внимание группы на то, что карточки имеют разную маркировку (белый, серый или черный квадрат в верхнем левом углу) и предлагает участникам определить, по какому принципу маркированы карточки. Если группа не может дать правильный ответ, его дает ведущий. Затем ведущий подводит итоги данного этапа.

Обсуждение

- О каких способах попадания информации в интернет вы узнали впервые, а о каких уже знали?
- Как вы думаете, каким способом информация чаще всего попадает в сеть? Почему?
- Как вам кажется, каким способом ваша персональная информация чаще всего попадает в сеть? Почему?

В помощь ведущему. Карточки разделены на три группы в соответствии с тем способом, с помощью которого личные данные попадают в сеть:

- 1-я группа (белый квадрат) — пользователь выкладывает в интернет информацию о себе сам;
- 2-я группа (серый квадрат) — информацию об активности пользователя в сети собирают приложения и онлайн-ресурсы;
- 3-я группа (черный квадрат) — информацию о пользователе в сеть выкладывают третьи лица.

Упражнение «Заметаем следы»

Задача: познакомить учащихся с основными средствами и приемами защиты персональных данных на компьютере и других устройствах.

Необходимые материалы: набор из 9 карточек со скриншотами «цифровых следов» (см. Приложение к уроку № 3.1), ключи с правильными ответами и пояснениями для ведущего (см. Приложение к уроку № 3.2), 3 копии памятки о средствах защиты персональных данных (см. Приложение к уроку № 3.3).

Время проведения: 20 минут.

Процедура проведения

Подводя итоги предыдущего упражнения, ведущий подчеркивает, что сегодня персональные данные пользователей с легкостью проникают в интернет, причем довольно часто это происходит без нашего ведома. Тем не менее есть много способов контролировать персональные данные в сети и даже удалять их оттуда. Задача группы — познакомиться с такими способами.

Ведущий делит группу на три подгруппы. Каждая из них получает памятку с информацией о средствах защиты персональных данных (см. Приложение к уроку № 3.3). На ее изучение дается 5 минут. Затем ведущий предлагает проверить, насколько хорошо усвоен материал, и закрепить его на практике. Он дает каждой группе по три карточки со скриншотами (см. Приложение к уроку № 3.1). Задача — проанализировать каждый «цифровой след» и предложить наиболее адекватное в каждом случае средство защиты персональных данных. На выполнение этого задания отводится 5 минут. Затем подгруппы представляют свои реше-

ния, а ученики из других групп могут задать вопросы и высказать свое мнение. В конце ведущий сверяет ответы с ключами (см. Приложение к уроку № 3.2) и поправляет участников в случае, если была допущена ошибка.

Обсуждение

- О каких средствах защиты персональных данных вы уже знали и имели опыт их использования, а о каких услышали впервые?
- В каких случаях можно контролировать попадание персональных данных в интернет, а в каких это сделать достаточно сложно? Почему?
- Какие средства защиты персональных данных вы бы стали использовать, а какие — нет? Почему?

Итоги занятия

Существует много каналов, по которым наши персональные данные попадают в интернет. Что-то выкладываем мы сами, что-то пишут о нас наши друзья и знакомые, определенную информацию собирают приложения и онлайн-ресурсы. Все наши «цифровые следы» хранятся в наших компьютерах и смартфонах. Если мы хотим сохранить определенный уровень конфиденциальности и хорошую репутацию в сети, эти «следы» необходимо контролировать. Важно знать, что «цифровые следы» также хранятся на серверах разработчиков приложений и онлайн-ресурсов и удалить их оттуда практически невозможно. Поэтому всегда нужно крайне внимательно относиться к той информации, которую мы выкладываем в сеть, а также к тому, что мы делаем в интернете: какие ресурсы посещаем, какие файлы скачиваем, какие делаем поисковые запросы и т.д.

На первый взгляд может показаться, что отдельные «цифровые следы» не представляют угрозы для нашей конфиденциальности. Например, многое ли можно узнать о человеке по его хобби или гастрономическим предпочтениям? Однако важно понимать, что в интернете потоки персональных данных объединяются друг с другом, как ручьи сливаются в реки, а реки — в моря и океаны. В целом такая обобщенная информация может дать достаточно полное представление о человеке. Современные технические средства легко позволяют объединить «цифровые следы» одного пользователя в единый портрет или профайл и идентифицировать его. Существуют сайты, которые специально собирают информацию о пользователях в коммерческих целях, например, для рекламы, маркетинговых исследований. Сбор персональных данных приложениями и онлайн-ресурсами — условие бесплатного и даже платного использования этих ресурсов, поэтому оградить себя полностью от этого невозможно. Всегда нужно помнить о том, что практически любое наше действие в интернете оставляет после себя неизгладимый «цифровой след», и по возможности стремиться контролировать свои персональные данные, попадающие в сеть.

Приложение № 3.1

КАРТОЧКИ С «ЦИФРОВЫМИ СЛЕДАМИ»

☐ Карточка № 1

- ***Марина, с днем рождения!!!*** 08.10.2015

@Поэтесса

Сегодня день рождения моей любимой поэтессы! Когда я читаю её стихи, мне кажется, что она писала про меня:

***

Спасибо вам и сердцем и рукой
За то, что вы меня - не зная сами! -
Так любите: за мой ночной покой,
За редкость встреч закатными часами,
За наши не-гулянья под луной,
За солнце, не у нас над головами,-
За то, что вы больны - увы! - не мной,
За то, что я больна - увы! - не вами!

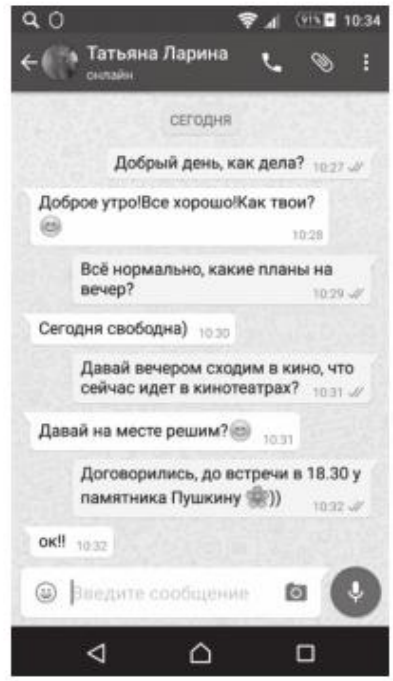
(с) М. Цветаева

А какой ваш любимый поэт?

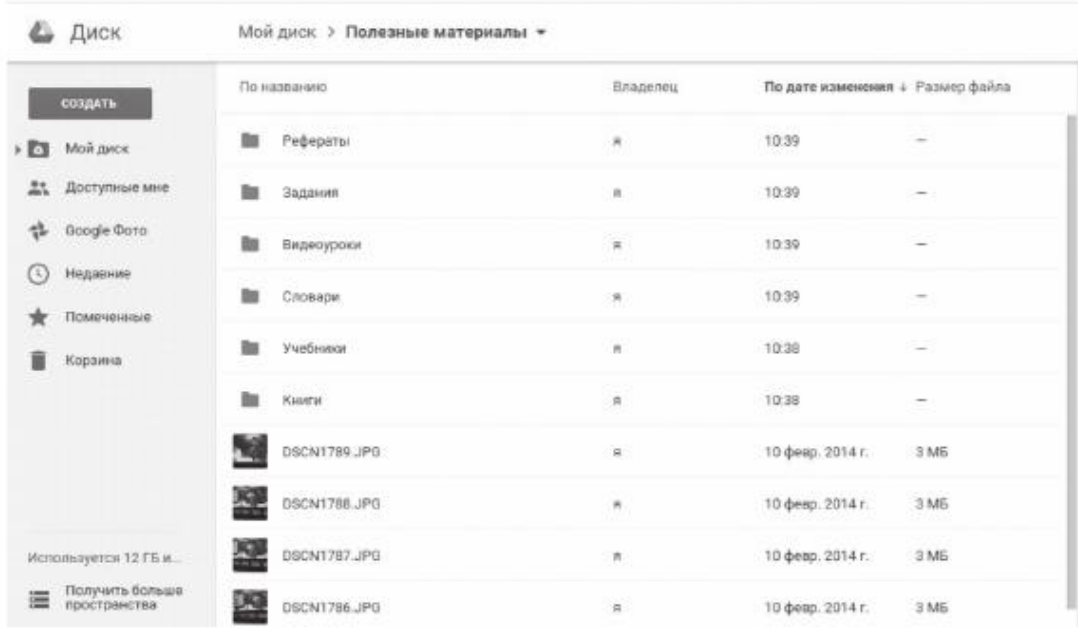
Тэги: *осень, стихи, погода, Цветаева*

10 комментариев Оставить комментарий

☐ Карточка № 2

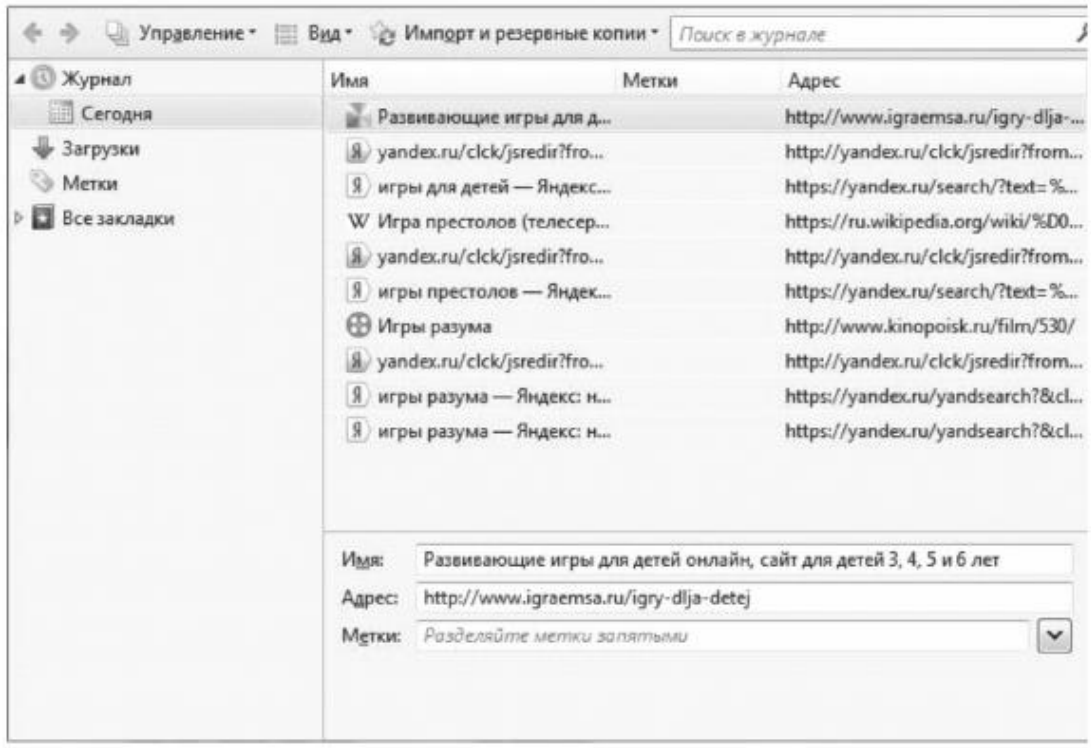


Карточка № 3



Карточка № 4

Карточка № 5



Карточка № 6

Карточка № 7

- *Корова на льду.*

01.12.2015

@Хулиганка

Сегодня была такая хорошая погода – очень не хотелось идти в школу! Решили прогулять вместе с @Отличница. Все думают, что она вся из себя такая хорошая, а она прогульщица, каких только поискать! Сказала учительнице, что у неё бабушка заболела, и её надо навестить. И ей поверили, а мне бы ни за что не поверили! Обидно (((

Зато погуляли мы отлично. Сначала сходили в кино, а потом парке катались на роликах.

А @Отличница на роликах, как корова на льду, пять раз падала, равновесия совсем не держит! А ведь пишет у себя, что занимается фигурным катанием и танцами! Да, с её чувством равновесия не то, что танцами, ходить опасно!

Надо будет @Отличница родителям и учительнице заложить! Чтобы слишком сильно не задавалась!

Тэги: *кино, ролики, друзья, гуляю*

270 комментариев Оставить комментарий

Карточка № 8

- *Подружки)))*

01.09.2015

@Отличница

Карточка № 9

- ***По большому секрету!***

31.08.2015

@Волшебница

На эти выходные ездила с друзьями загород на водопады. Волшебное место – очень красиво и совсем безлюдно. Только шум воды и ветра!

А как прошли ваши выходные?

Тэги: *выходные, природа, друзья, водопады*

3 комментария Оставить комментарий

@Хулиганка

Да, ладно, я тебя на выходных во дворе видела! Никуда ты не ездила **@Волшебница**)))))

Ответить

@Поэтесса

А, ведь, **@Хулиганка** права! И вообще деревья на фотографиях больше напоминают начало июнь, а не август!!!

Ответить

@Отличница

Вообще-то, эти водопады расположены в Карелии. Там ещё фильм «А зори здесь тихие» снимали!!!))

Ответить

Приложение № 3.2

КЛЮЧИ С ПРАВИЛЬНЫМИ ОТВЕТАМИ И ПОЯСНЕНИЯМИ ДЛЯ ВЕДУЩЕГО

№	Информация	Способ попадания в сеть	Способ защиты или удаления информации
1-я группа (маркировка белая): пользователь сам выкладывает в интернет информацию о себе			
1.	Пост, размещенный в одной из социальных сетей, в котором пользователь открыто делится персональной информацией с другими пользователями данного ресурса	Пользователь выкладывает информацию самостоятельно, определяя уровни доступа к посту других пользователей	Содержание поста должно определяться самим пользователем в соответствии с *правилами управления персональными данными*. Доступ к аккаунту защищается *паролем*. Уровни доступа других пользователей к посту определяются *настройками приватности*
2.	Личная переписка двух пользователей в мессенджере	Происходит между двумя пользователями. В публичный доступ переписка может попасть, во-первых, в случае перехвата данных, во-вторых, при взломе аккаунта пользователя. В случае если один из аккаунтов будет взломан, злоумышленники получат доступ ко всей истории	Защитить свою переписку можно, используя мессенджеры с шифрованием передачи данных, а также защищая аккаунт надежным паролем
3.	Папка с файлами, размещенная в облачном хранилище	Пользователь выкладывает самостоятельно, определяя уровни доступа к файлам других пользователей	Доступ к облачному хранилищу, размещенному на удаленном сервере, осуществляется с помощью *пароля*. Уровни доступа к файлам, размещенным в хранилище, определяет сам пользователь в *настройках приватности*

№	Информация	Способ попадания в сеть	Способ защиты или удаления информации
2-я группа (маркировка серая): информацию об активности пользователя в сети собирают приложения и онлайн-ресурсы			
4.	История поисковых запросов (напротив прошлых поисковых запросов стоит надпись «Удалить»)	Собирается с помощью инструментов аккаунта пользователя на сайте поисковой системы	Удалить историю поисковых запросов можно в своем аккаунте на сайте поисковика. Чтобы история поисковых запросов не сохранялась, можно использовать режим браузера *инкогнито* или не заходить в свой аккаунт поискового сервиса при использовании обычного режима браузера
5.	Вкладка «Журнал посещения страниц» в браузере, виден список страниц, посещенных пользователем в хронологическом порядке	Собирается браузером, может храниться как на компьютере, так и на удаленном сервере	Удалить лог-файлы, историю посещения страниц, временные файлы из интернета и cookies можно с помощью штатных инструментов операционной системы и браузера или при помощи специализированных приложений. *Программы сетевой защиты* позволяют ограничить загрузку временных файлов из интернета и cookies
6.	Вкладка «Загрузки» в браузере — виден список файлов, скачанных пользователем в хронологическом порядке	Собирается браузером и хранится на устройстве в папке «Загрузки»	*Удалить загрузки* можно из вкладки браузера или из папки «Загрузки» на диске

№	Информация	Способ попадания в сеть	Способ защиты или удаления информации
3-я группа (маркировка черная): информацию о пользователе в сеть выкладывают третьи лица			
7.	Пост, в котором один пользователь **@Хулиганка** упоминает другого пользователя **@Отличница**, разглашая персональные данные последней	Выкладываются другими пользователями социальных сетей	Если пост, на котором отмечен пользователь, нарушает законадательство и/или правила сообщества, то, чтобы его удалить, необходимо обратиться в *службу поддержки социальной сети или к регулятору (в России — Роскомнадзор).* Запретить другим пользователям упоминать себя в их постах можно с помощью *настроек приватности*, например, добавив их в *«черный список»*
8.	Фотография, размещенная в социальной сети, на которой пользователь **@Хулиганка** отметил других пользователей: **@Отличница, @Волшебница, @Поэтесса**	Делаются другими пользователями социальной сети	Запретить другим пользователям отмечать себя на фотографиях можно с помощью *настроек приватности.* Если пользователь сообщает ваши персональные данные, необходимо сообщить в *службу поддержки*
9.	Комментарии других пользователей к посту **@Волшебница**, которые могут содержать персональные данные автора поста	Делаются другими пользователями социальных сетей	Запретить другим пользователям оставлять комментарии к постам можно в *настройках приватности.* Неприятный комментарий можно просто *удалить*

Приложение № 3.3

СРЕДСТВА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

«Три кита» защиты персональных данных:

- *Надежные пароли* позволят защитить от третьих лиц ваши аккаунты на онлайн-ресурсах и в приложениях.
- *Настройки приватности* дадут вам возможность определить уровень доступа других пользователей к вашим персональным данным, размещенным на различных онлайн-ресурсах.
- *Правила управления персональными данными* помогут вам понять, как персональные данные, размещенные в интернете, влияют на вашу репутацию в сети.

Осторожно, онлайн-мошенники!

Прежде чем вводить свои персональные данные в интернете, необходимо убедиться, что вы находитесь именно на том ресурсе, на который хотели попасть, а не на поддельной (фишинговой) странице, созданной мошенниками.

Существует несколько простых способов убедиться в подлинности ресурса:

- Всегда обращайте внимание *на адресную строку браузера*. Адрес поддельной странички может отличаться всего на одну букву, которую легко не заметить, например: в адресе www.odnoklassniki.ru может быть пропущена всего одна буква «s», но это будет уже совсем другой сайт.
- Не стоит переходить на ресурсы *по ссылкам*, которые вы получили по электронной почте или в личной переписке и которые требуют *ввода персональных данных* — многие из

них ведут на поддельные сайты. Забейте адрес в адресную строку самостоятельно, а еще лучше — используйте для поиска нужных ресурсов надежные поисковые системы, например, Яндекс.

- Прежде чем вводить персональные данные в интернете, убедитесь, что ресурс, на котором вы находитесь, использует *защищенное соединение*. Если в адресной строке браузера присутствует иконка замка, а сам адрес начинается с аббревиатуры *https://* вместо привычной *http://*, то такое соединение использует шифрование при передаче ваших персональных данных. В этом случае злоумышленникам будет гораздо сложнее перехватить ваши персональные данные и воспользоваться ими.
- Комплексные *антивирусные программы* также могут помочь защититься от мошенников. Многие из них содержат базы данных опасных и ненадежных ресурсов и способны предупреждать о возможной опасности, блокируя переход по фишинговым ссылкам.

Следует помнить о том, что только одновременное соблюдение всех этих правил может надежно защитить от мошенников.

Защита персональных данных на своем устройстве

- Для удаления «цифровых следов» с компьютера после работы в интернете очистите *журнал посещений* (в браузере) и *историю поисковых запросов* (в аккаунте сайта-поисковика). С помощью средств операционной системы и браузера или специализированных приложений вы можете удалить автономные веб-страницы, временные файлы из интернета, а также cookies (небольшие фрагменты данных, которые отправляются онлайн-ресурсом и хранятся на компьютере

пользователя; они помогают сайтам «запоминать» пользователей и их индивидуальные предпочтения), которые также могут многое рассказать о вашей работе в сети. Все это вы сможете сделать, только если обладаете необходимыми правами (например, администратора).

- В настройках *программ сетевой защиты* также можно установить запрет на загрузку временных файлов и cookies с незнакомых сайтов, ограничившись лишь проверенными и надежными ресурсами.
- Будьте внимательны с *настройками мобильных приложений*: отключите опцию «автосинхронизации» данных, автоматического проставления «геометок» и т.д., если хотите избежать случайного попадания персональных данных в сеть.

Защита персональных данных на чужом устройстве

- При входе в свой аккаунт с чужого устройства всегда выбирайте опцию *«чужой компьютер», «не сохранять пароль», «безопасный ввод»* и т.д. (на странице онлайн-ресурса). В этом случае вы можете быть уверены, что никто не войдет в ваш аккаунт после вас.
- Чтобы не оставить цифровых следов на чужом устройстве, используйте режим *инкогнито* (в браузере). Благодаря ему история поисковых запросов и посещенных страниц не сохраняется в браузере, а сайты не загружают cookies на устройство.

Защита персональных данных от третьих лиц

- Используя вкладку *«настройки приватности»* (на странице онлайн-ресурса), запретите другим пользователям отмечать

вас на фотографиях и упоминать в постах. Ограничьте круг лиц, которые могут комментировать ваши записи. Как правило, добавление пользователя в *«черный список»* автоматически лишает его возможности просматривать и комментировать ваши посты, а также упоминать вас в своих постах.

- Если другой пользователь использует ваши персональные данные, например фотографии, без вашего согласия, вы можете пожаловаться в *службу поддержки ресурса* (на странице онлайн-ресурса), приложив доказательства нарушения. Если другой пользователь, разместив недостоверную или устаревшую информацию, нанес существенный урон вашим чести и достоинству, вы можете обратиться в суд.

Урок № 4

ПОЧЕМУ НУЖНО УПРАВЛЯТЬ ПЕРСОНАЛЬНЫМИ ДАННЫМИ?

Цель: знакомство с основными рисками, связанными с распространением персональных данных в сети (спам, фишинг, репутационные риски, кибербуллинг и т.д.).

Разминка «По секрету всему свету»

Задача: помочь учащимся в осознании утраты контроля над информацией после того, как она выложена в сеть, а также сложности контроля за персональными данными в интернете.

Необходимые материалы: листы бумаги и ручки по количеству учащихся, клеевой карандаш.

Время проведения: 15 минут.

Процедура проведения

В качестве разминки к занятию ведущий предлагает классу поиграть. Каждый ученик берет небольшой листочек бумаги и записывает на него секрет про себя. Ведущий должен отметить, что секреты не будут зачитываться вслух, но тем не менее они не должны быть слишком личными и значимыми для участников. Затем листочки складываются несколько раз. Их можно также «запечатать» (заклеить) клеевым карандашом. Затем группа садится в круг. По команде ведущего каждый участник передает свой листочек с секретом участнику, сидящему справа, и берет листок у сидящего слева. Через несколько секунд ведущий дает команду, и участники снова меняются секретами. Эти действия продолжаются до тех пор, пока «секреты» не вернутся к своим

хозяевам. Теперь участники могут проверить, сохранна ли печать, поставленная клеевым карандашом. На этом игра заканчивается, и можно переходить к обсуждению.

Если в классе нет возможности сесть в круг, упражнение можно выполнять, разбившись на пары. В этом случае напарники встают лицом друг к другу, берут листок с секретом в правую руку и подставляют левую руку ладонью вверх. По команде ведущего ученики меняются секретами, получая чужой секрет в свою левую руку. Ведущий дает возможность группе побыть в таком состоянии несколько минут. Затем по команде все возвращают секреты обратно. Этот вариант упражнения технически проще и безопаснее. Поэтому если ведущий не уверен, что в группе установился достаточно высокий уровень доверия, лучше выполнять его. Чтобы подстраховаться, ведущий может предложить участникам выбрать себе в пару человека, которому они больше всего доверяют.

В помощь ведущему. Когда мы делимся информацией с другими людьми — не важно, лично или выкладывая ее в сеть, — мы теряем над ней контроль. Как правило, в реальной жизни потеря контроля вызывает у людей чувство дискомфорта и тревоги. В интернете потеря контроля над персональной информацией, которая, по сути, является секретом, часто не замечается и не ощущается. Это упражнение помогает ученикам осознать чувство дискомфорта, связанное с потерей контроля над информацией, и осознать, что аналогичная ситуация происходит в интернете.

Следует отметить, что выполнение этого упражнения предполагает достаточно высокий уровень сплоченности и доверия внутри группы. Если ведущий не уверен в этом, он может предложить участникам выписать на листочки шутливые, безобидные секреты. Напротив, если ведущий чувствует, что уровень

доверия в группе высок, секреты могут быть более значимыми, что усилит эффект упражнения.

Обсуждение

- Что вы чувствовали, когда ваш секрет находился в чужих руках? Почему?
- Что вы чувствовали, когда чужой секрет находился в ваших руках? Почему?
- Хотелось ли вам узнать чужой секрет? Если бы вы узнали секрет, поделились ли бы вы им с другими? Почему?
- Случалось ли вам выкладывать личную или секретную информацию о другом человеке в сеть? Зачем вы это делали? Что вы чувствовали при этом?

Упражнение «Скорая помощь онлайн»

Задача: помочь учащимся осознать потенциальные риски, связанные с распространением персональных данных в сети, и научить прогнозировать возможные последствия размещения личной информации в интернете.

Необходимые материалы: информация о Линии помощи «Дети Онлайн» (см. Приложение к уроку № 4.1), карточки с примерами обращений на Линию помощи «Дети Онлайн» (см. Приложение к уроку № 4.2), комментарии для ведущего (см. Приложение № 4.3).

Время проведения: 30 минут.

Процедура проведения

Чувство дискомфорта — это самое меньшее, что может возникнуть в результате потери контроля над персональными данными. Дети и подростки довольно часто сталкиваются с куда

более серьезными последствиями неаккуратного обращения с персональными данными. В таких ситуациях многие из них обращаются на Линию помощи «Дети Онлайн» (подробнее о Линии помощи см. Приложение к уроку № 4.1).

В ходе этого упражнения учащиеся познакомятся с примерами реальных проблем, которые появляются у их сверстников в результате неаккуратного обращения с персональными данными, и смогут разобраться в их причинах, способах решения и профилактики возникновения*. Для этого ведущий делит класс на несколько групп по 3–5 человек, каждая из которых получает карточку с примером обращения на Линию помощи «Дети Онлайн» (см. Приложение к уроку № 4.2). Задача группы — внимательно изучить пример и сформулировать ответы на следующие вопросы:

- Почему произошла эта ситуация? Что стало причиной возникновения проблемы?
- Что можно посоветовать подростку, обратившемуся за помощью, чтобы решить возникшую проблему?
- Что нужно делать, чтобы подобные ситуации впредь не возникали? Каких действий для этого следует избегать?

На выполнение этого задания отводится около 10 минут.

Когда все готовы, представитель от каждой группы описывает проблему, представленную в карточке, называет причины, которые, по мнению группы, привели к ее возникновению, а затем предлагает пути решения проблемы и способы, позволяющие ее избегать. Каждой группе на выступление отводится 2–3 минуты. Остальные участники могут задать вопросы выступающему и

* В упражнении используются материалы Линии помощи «Дети Онлайн» (подробнее о работе Линии помощи см. Журнал «Дети в информационном обществе» (№ 21). URL: http://detionline.com/assets/files/ journal/21/issl_LP.pdf).

высказать свои комментарии, например, выразить несогласие и предложить свое решение проблемы. В целом на эту часть упражнения отводится 10–15 минут.

В ходе дискуссии ведущий выписывает на доску все рекомендации по решению и профилактике проблем, сформулированные участниками группы, а также дополняет их, используя комментарии для ведущего (см. Приложение к уроку № 4.3). В результате получается набор рекомендаций по решению и профилактике проблем, возникших в результате неаккуратного обращения с персональными данными в интернете.

Обсуждение

- Приходилось ли вам или вашим знакомым сталкиваться с подобными проблемами?
- Как вы думаете, какова основная причина возникновения подобных ситуаций?
- Что можно посоветовать человеку, оказавшемуся в таких обстоятельствах?

Итоги занятия

Когда мы делимся информацией с окружающими нас людьми, то теряем над ней контроль, что может вызвать у нас чувство тревоги и дискомфорта. Выкладывая персональные данные в интернет, довольно часто мы не замечаем потери контроля — в этом и состоит основной риск неаккуратного обращения с личной информацией.

Любая персональная информация, выложенная в сеть, может стать причиной серьезных проблем. Наши фамилия, имя, номер телефона помогают хакеру подобрать пароль к нашему аккаунту, наши хобби, интересы и увлечения позволяют многое о нас узнать и использовать эти знания в своих целях. Поскольку

мы не думаем об этом заранее, такая ситуация становится для нас досадной неожиданностью. Именно поэтому необходимо бережно относиться к персональным данным, попадающим в интернет.

Можно назвать три главные составляющие, обеспечивающие более или менее надежную защиту персональных данных:

- Надежный пароль.
- Управление уровнями доступа к персональным данным (настройки приватности).
- Сознательное отношение к информации, размещаемой в интернете.

Приложение № 4.1

ИНФОРМАЦИЯ О ВСЕРОССИЙСКОЙ ЛИНИИ ПОМОЩИ «ДЕТИ ОНЛАЙН»

Сталкиваясь с проблемами в сети, дети и подростки часто не знают, как поступить в неприятной или опасной ситуации и куда можно обратиться за помощью. В 2009 г. в рамках Года Безопасного Интернета в России была создана Линия помощи «Дети Онлайн» для оказания психологической и информационной поддержки детям и подросткам.

Линия помощи «Дети Онлайн» — это служба телефонного и онлайн-консультирования по вопросам безопасного использования интернета и мобильной связи для детей, подростков, родителей и работников образовательных учреждений.

На Линии помощи работают профессиональные психологи-эксперты Фонда Развития Интернет и факультета психологии МГУ имени М.В. Ломоносова.

Обратиться на Линию помощи можно как по телефону, так и по электронной почте или в онлайн-чате.

Часы работы: с 9 до 18 часов в будние дни (перерыв с 13 до 14 часов), звонок по России бесплатный.

Телефон: 8-800-25-000-15.

Электронная почта: helpline@detionline.com

Онлайн-чат: http://detionline.com/

Все обращения на Линию полностью анонимны и конфиденциальны.

Приложение № 4.2

ПРИМЕРЫ ОБРАЩЕНИЙ НА ЛИНИЮ ПОМОЩИ «ДЕТИ ОНЛАЙН»

Пример № 1

Добрый день! Меня зовут Марина, мне 14 лет. Недавно кто-то взломал мой аккаунт в ВКонтакте и стал размещать на моей стене неприличные изображения. А еще оскорблять от моего имени друзей в комментах и в личке. Обо всем я узнала от подруги, так как на даче, где я была, не было интернета. Я восстановила доступ к аккаунту и поменяла пароль, но было уже поздно. Многие удалили меня из друзей и добавили в «черный список», а кое-кто даже перестал со мной разговаривать. Я несколько лет вела эту страницу, у меня была почти тысяча подписчиков, а теперь все пропало. Подскажите, как мне поступить? Как вернуть доверие подписчиков?

Пример № 2

Доброго времени суток! Я Артем, учусь в 9-м классе. Однажды на уроке информатики я зашел в свой аккаунт в социальной сети и забыл выйти. Через неделю один из моих одноклассников создал паблик, в которой он выкладывает скриншоты моей личной переписки с друзьями и гадкие комментарии к ним. Там нет ничего такого, но это все равно неприятно. Надо мной все смеются. Я и раньше не был самым популярным в классе, а теперь стал настоящим изгоем. Что мне делать? Можно ли удалить этот паблик? Как наказать одноклассника?

Пример № 3

Здравствуйте! Меня зовут Настя, мне 15 лет. Недавно я познакомилась с парнем в социальной сети. Он был знакомым моей подруги и показался мне интересным. Мы стали общаться, оказалось, что у нас много общего. Мы рассказывали друг другу о себе, о том, где учимся, путешествуем. Вообще-то я скрытная, и профиль у меня только для друзей, но с ним я, кажется, позволила себе лишнего. Однажды он предложил встретиться. Я немного испугалась и отказала ему. Он сказал, что знает, где я учусь и где живу, обещал подстеречь по дороге из школы домой. Я не знаю, правда это, или он меня просто запугивает. Мне действительно страшно. Теперь одна, без подруги, я в школу не хожу. Подскажите, как мне быть?

Пример № 4

Добрый день! Меня зовут Егор, мне 12 лет. Я тут увидел в интернете рекламу новой игры Dragons&Unicorns. Для того чтобы в нее поиграть, нужно было зарегистрироваться на сайте и указать номер мобильного, что я и сделал. В результате игра мне совсем не понравилась, и я быстро забыл про нее. А через несколько дней мне на телефон стали приходить СМС-ки с рекламой с разных номеров. Я удалил свой аккаунт на сайте игры, но это не помогло, СМС-ки продолжают приходить. Подскажите, как от них избавиться?

Пример № 5

Добрый день, меня зовут Лена! Мне 15 лет. Меня обманула моя «подруга» из социальной сети. Мы общались больше года. Познакомились в паблике про ролевые игры. Я говорила ей, что мечтаю приобрести последний сет игры Dungeons&Dragons, но у нас он не продается. Заказать по интернету я не могу. У меня нет банковской карты, а родители свою не дают. Подруга предложила мне помочь купить сет. Она уже студентка, и у нее есть карта. Она предложила мне перевести ей деньги на Яндекс-Кошелек и обещала сделать заказ с доставкой на мой адрес. Я с радостью согласилась и перевела ей деньги. Прошел месяц, а посылка не приходила. Когда я спрашивала ее об этом, она отвечала, что нужно подождать. Потом она стала появляться в сети все реже и реже, пока совсем не пропала. Совершенно случайно я узнала, что она обманула еще несколько человек аналогичным способом. Подскажите, можно ли что-то сделать? Вернуть деньги или наказать эту мошенницу?

Приложение № 4.3

КОММЕНТАРИИ ДЛЯ ВЕДУЩЕГО

Пример № 1. В данном случае мы имеем дело со взломом аккаунта школьницы с целью нанесения вреда ее репутации. Это довольно распространенная проблема. По статистике Фонда Развития Интернет, более четверти российских школьников (28%) сталкивались со взломом аккаунта в социальных сетях.

Из письма довольно сложно установить причину произошедшего. Наиболее распространенные причины взлома аккаунта: использование простых паролей; неправильное хранение паролей; вход в аккаунт с чужого устройства; ввод пароля на поддельной страничке; действие вредоносных программ; передача пароля третьим лицам.

В этой ситуации для восстановления репутации школьнице можно порекомендовать следующие действия:

- Сменить пароли к аккаунтам на других онлайн-ресурсах.
- Удалить все неприятные сообщения со своей страницы.
- Разместить на странице пост, разъясняющий причины произошедшего, извиниться перед читателями.
- Постараться лично поговорить с самыми близкими друзьями и объяснить им ситуацию.

Чтобы избежать подобной проблемы, следует предпринять следующие шаги:

- Использовать сложные пароли и двухэтапную систему аутентификации*.

* Метод двухэтапной аутентификации гораздо более надежен, чем метод «логин — пароль», так как для аутентификации пользователя используется не только пароль, но и его мобильный телефон, на который приходит СМС с кодом доступа. Поскольку передача пароля и

- Установить антивирусные программы на все устройства, с которых осуществляется выход в интернет.
- Соблюдать правила предосторожности при входе в аккаунт с чужого компьютера (см. Урок № 5).
- Соблюдать правила поведения при столкновении с поддельными страницами (см. Урок № 5).

Пример № 2. В данном случае мы имеем дело с кибербуллингом — травлей, организованной с помощью электронных средств связи. По статистике Фонда Развития Интернет, каждый четвертый российский школьник (24%) сталкивался с оскорблениями, унижениями, преследованиями и обидами в сети*. Из письма становится ясно, что одной из причин буллинга стала кража аккаунта и персональных данных, которые произошли из-за неосторожного входа в социальную сеть на чужом компьютере.

В этой ситуации школьнику можно порекомендовать следующие действия:

- Сменить пароль от аккаунта и временно закрыть его.
- Написать в службу поддержки социальной сети письмо с

кода доступа происходит по разным каналам связи, это практически полностью исключает перехват пароля злоумышленниками. Тем не менее метод двойной аутентификации может сыграть злую шутку с его хозяином, если он попал под прицел профессиональных мошенников. Чаще всего телефонный номер, к которому привязан аккаунт — это основной контактный номер. Почти все сервисы сообщают его первые или последние цифры любому желающему, если попытаться восстановить доступ к аккаунту. Поэтому выяснить номер, связанный с аккаунтом, несложно. Для злоумышленников не составит труда перевыпустить симкарту по поддельным документам и получить доступ к желанному аккаунту.

* Подробнее о кибербуллинге см. журнал «Дети в информационном обществе» (№ 16). URL: http://detionline.com/journal/numbers/16.

просьбой удалить паблик, приложив скриншоты из самого паблика и из личной переписки, подтвердив тем самым неправомерное использование личных данных одноклассником.

- Если ситуация повторится, и после удаления будет создан новый паблик, написать в службу поддержки социальной сети письмо с просьбой удалить аккаунт пользователя, нарушившего правила пользования ресурсом.
- Рассказать о ситуации взрослым (родителям или учителям) и попросить их вмешаться в ситуацию в школе.

Для того чтобы избежать подобной проблемы в будущем, следует предпринять следующие шаги:

- Использовать двухэтапную систему аутентификации.
- Соблюдать правила предосторожности при входе в аккаунт с чужого компьютера (см. Урок № 5).
- Соблюдать осторожность в личной переписке в социальных сетях.

Пример № 3. В данном случае мы имеем дело с преследованием и шантажом, которые могут быть частью как буллинга, так и сексуальных домогательств*.

Из письма можно заключить, что причиной проблемы стала некоторая личная информация, которую автор письма сообщил шантажисту.

В этой ситуации школьнице можно порекомендовать следующие действия:

- Внимательно перечитать историю переписки и понять, какая персональная информация могла попасть к шантажисту.
- Внимательно изучить общие контакты и понять, какую информацию о школьнице шантажист мог узнать косвенно

* Подробнее о домогательствах см. журнал «Дети в информационном обществе» (№ 11). URL: http://detionline.com/assets/files/journal/11/issl11.pdf.

от третьих лиц, например прочитать на страницах и в профилях друзей.

- Рассказать или показать историю переписки взрослым (родителям, учителям), чтобы они могли предпринять действия по защите школьницы, вплоть до обращения в правоохранительные органы.
- В случае если шантажист снова выйдет на связь, сообщить ему обо всех предпринятых действиях и добавить его в «черный список».

Чтобы избежать подобной проблемы, следует предпринять следующие шаги:

- С большой осторожностью добавлять незнакомцев в друзья и вступать с ними в переписку, даже если они являются друзьями друзей.
- Не сообщать личную информацию незнакомцам. Даже если она кажется безобидной, она может быть легко использована против жертвы.

Пример № 4. В данном случае мы имеем дело со спамом — рассылкой коммерческой и иной рекламы или подобных коммерческих видов сообщений лицам, не выражавшим желания их получать. Как видно из письма, проблема, скорее всего, возникла после того, как школьник ввел свой номер телефона на сайте игры.

В этом случае необходимо обратиться к оператору, предоставляющему услуги сотовой связи, и подключить опцию «блокировка отправлений с коротких номеров». Также это можно сделать самостоятельно в личном кабинете на сайте оператора.

Для того чтобы подобные проблемы не возникали вновь, важно не оставлять номер мобильного телефона на незнакомых и непроверенных онлайн-ресурсах.

Пример № 5. Мы имеем дело с «мошенничеством на доверии». По статистике Фонда Развития Интернет, каждый десятый российский школьник сталкивался с кражей денег в сети. Судя по письму, мошеннице удалось втереться в доверие к школьнице благодаря той личной информации, которую она могла узнать как от нее самой, так и из ее профиля в социальной сети. Как правило, «мошенники на доверии» действуют очень осторожно и ждут удобного случая, чтобы обмануть жертву. В данном случае школьница сама спровоцировала событие, рассказав «подруге» о своем желании приобрести игровой сет.

В такой ситуации помочь школьнице очень трудно. Доказать факт мошенничества и вернуть похищенное практически невозможно, так как деньги были переданы по собственному желанию и без давления со стороны. Единственный способ решения проблемы — это коллективное заявление в прокуратуру. В этом случае все пострадавшие лица должны собрать доказательства противоправных действий мошенницы (личная переписка, реквизиты платежей и т.д.). Можно поискать других жертв мошенницы в социальных сетях. Чем больше пострадавших подадут заявление, тем больше шансов призвать мошенника к ответственности.

Для того чтобы подобные проблемы не возникали вновь, нужно:

- С большой осторожностью добавлять незнакомцев в друзья и вступать с ними в переписку.
- Никогда не обсуждать с незнакомцами финансовые вопросы, например, касающиеся дорогих покупок или путешествий.

Урок № 5

КАК ЗАЩИТИТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ?

Цель: знакомство с основными средствами технической защиты персональных данных и правилами поведения в сети.

Разминка «Сто к одному»

Задача: ввести участников в тему занятия и познакомить с критериями надежности паролей.

Необходимые материалы: список десяти самых популярных паролей для ведущего (см. Приложение к уроку № 5.1), памятка «Правила составления надежных паролей» (см. Приложение к уроку № 5.2).

Время проведения: 10 минут.

Процедура проведения

Дом, в котором мы храним личные вещи, нуждается в прочной двери и надежном замке. Так же и наши персональные данные, которые мы размещаем в социальных сетях или облачных сервисах, должны храниться под замком, ключом к которому является пароль. По данным Международного союза электросвязи, в 2015 г. интернетом пользовались более 3,2 млрд человек по всему миру, и, конечно, у всех этих людей имелся хотя бы один аккаунт и пароль к нему*. Поскольку пользователей интернета так много, неудивительно, что пароли, которые они используют, могут повторяться. Чтобы узнать, какие же пароли чаще всего

* URL: http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

используют в интернете, ведущий предлагает классу сыграть в игру, похожую на телепередачу «Сто к одному».

Группа делится на две равные команды. Им дается несколько минут на то, чтобы придумать как можно больше ответов на вопрос: «Какой пароль — самый популярный среди пользователей интернета?». Ведущий может напомнить ученикам, что все пароли записываются латиницей.

Затем от каждой команды к доске по очереди подходят участники и предлагают свой вариант ответа. Ведущий сверяет ответы с ключом и выписывает правильные варианты на доску (см. Приложение к уроку № 5.1). Повторяться или давать сходные ответы нельзя. Игра заканчивается, когда каждый игрок даст по одному ответу на вопрос. Побеждает та команда, которая даст больше всего правильных ответов. В конце игры ведущий должен выписать неотгаданные варианты паролей из ключа на доску.

Обсуждение

- Легко ли угадать пароли из этого списка? Почему?
- Использовали ли вы пароли из этого списка? Если да, то почему? В каких случаях?
- Как вы думаете, почему так много людей используют простые пароли?
- Каким, по-вашему, должен быть надежный пароль?

В помощь ведущему. Аккаунты, защищенные паролями из этого списка, очень легко взломать, поскольку такие пароли можно относительно быстро угадать с помощью перебора информации, имеющей личное отношение к пользователю. Такой метод взлома аккаунтов профессиональные хакеры называют методом логического угадывания.

Часто пользователи используют простые пароли для аккаунтов к ресурсам, которые не представляют для них особой важности. Тем не менее сложные пароли необходимо использовать для всех ресурсов, так как один взломанный аккаунт может быть использован злоумышленниками для доступа к другим связанным аккаунтам, защищенным более надежными паролями.

Если кто-то из участников группы использует пароль из приведенного списка, его нужно срочно сменить.

В конце упражнения ведущий рассказывает ученикам правила составления надежных паролей (см. Приложение к уроку № 5.2).

Упражнение «Занимательная криптография»

Задача: познакомить участников со способами составления надежных паролей и приемами, позволяющими запомнить составленные пароли.

Необходимые материалы: памятка «Правила составления надежных паролей» по количеству участников (см. Приложение к уроку № 5.2).

Время проведения: 15 минут.

Процедура проведения

Надежный пароль — это не просто пароль, который сложно угадать, это еще и пароль, который легко запомнить. Хотя сегодня и существуют специальные программы, позволяющие генерировать и хранить сложные пароли на компьютере, гораздо надежнее хранить пароль в голове. Для того чтобы научиться создавать сложные, но легко запоминающиеся пароли, ведущий предлагает группе познакомиться с основами

криптографии (метод тайнописи) и выполнить следующее задание.

Класс делится на 2–4 микрогруппы, каждый участник которой получает небольшую памятку «Правила составления надежных паролей» (см. Приложение к уроку № 5.2). Задача группы — придумать самый надежный и вместе с тем запоминающийся пароль, следуя правилам и рекомендациям из памятки. На выполнение этого задания отводится 5 минут.

После окончания работы каждая группа по очереди выписывает свой пароль на доску, а другие участники должны попытаться угадать, какое «послание» было зашифровано при составлении этого пароля (иными словами, понять, как он был получен). Если классу это не удается, группа в качестве подсказки может назвать способы шифрования, использованные для составления пароля. В конце упражнения методом открытого голосования выбирается самый удачный пароль — надежный и запоминающийся (голосовать за свой пароль нельзя).

Обсуждение

- Какой пароль (способ шифрования) понравился вам больше всего? Почему?
- Какие из предложенных способов шифрования вам уже были знакомы, а о каких вы услышали впервые?
- Планируете ли вы использовать эти правила при составлении паролей к своим аккаунтам?

Упражнение «Конкурс социальной рекламы»

Задача: познакомить учащихся с наиболее распространенными путями потери паролей и правилами поведения в сети, позволяющими избежать их потери.

Необходимые материалы: карточки с заданиями (см. Приложение к уроку № 5.3), белые листы бумаги формата А4, цветные карандаши, фломастеры, маркеры и т.д.

Время проведения: 20 минут.

Процедура проведения

Даже если ваш аккаунт защищен надежным паролем, это не повод расслабляться. Часто пользователи теряют доступ к своему аккаунту по собственной невнимательности и доверчивости. Чтобы уберечь свои персональные данные, необходимо сохранять бдительность и бережно относиться к своим паролям. Соблюдение простых правил позволяет избежать многих проблем. Но как убедить пользователей их соблюдать? Один из способов сделать это — *социальная реклама*, т.е. реклама, направленная на изменение социального поведения и привлечение внимания к общественно значимым проблемам.

Ведущий предлагает группе попробовать себя в роли проектных групп, работающих над созданием социальной рекламы, призванной убедить пользователей соблюдать правила поведения в сети, позволяющие избежать потери паролей. Для этого ведущий делит класс на 4–5 групп, каждая из которых получает карточку с заданием, содержащим описание одного из наиболее распространенных способов потери пароля и правила поведения, позволяющие его избежать (см. Приложение к уроку № 5.3). Также каждая группа получает белый лист бумаги формата А4 и набор цветных карандашей, фломастеров и т.д. Задача группы — внимательно изучить полученные материалы и придумать эскиз плаката-мотиватора, призывающего пользователей соблюдать правила безопасности. На выполнение этого задания отводится 10 минут.

Когда все эскизы готовы, каждая группа по очереди делает мини-презентацию своего плаката на 1–1,5 минуты. Затем класс выбирает лучшую работу путем открытого голосования.

По желанию в качестве домашнего задания ведущий может предложить группам сделать полноценные плакаты и организовать выставку «Правила безопасного интернета» для своей школы.

Обсуждение

- Приходилось ли вам сталкиваться с ситуациями, описанными в карточках? Если да, то как вы поступали в подобных случаях?
- Соблюдаете ли вы правила, описанные в карточках? Если нет, то почему?
- Как вы думаете, почему многие пользователи не соблюдают простые правила безопасности, которые могли бы уберечь их от многих проблем?

Итоги занятия

Ключ от дома защищает наши ценности в реальном мире, а пароль защищает в мире виртуальном. Всегда используйте надежные пароли для всех своих аккаунтов в интернете и в мобильных приложениях. Один плохо защищенный аккаунт может стать причиной взлома остальных аккаунтов.

Особенно надежным должен быть пароль от электронной почты, который используется для регистрации на других ресурсах. Лучше всего защитить его с помощью процедуры двухэтапной аутентификации. В этом случае всегда можно будет использовать мобильный телефон для восстановления пароля и контроля за несанкционированным доступом к аккаунту.

Хороший пароль — это не только тот пароль, который трудно взломать, это еще и тот пароль, который легко запомнить. Использование различных приемов для шифрования и запоминания поможет вам создать хороший пароль. Аккаунты взламываются либо методом логического угадывания, либо методом простого перебора. Использование длинных паролей, включающих в себя бессмысленный для других людей набор букв, цифр и специальных символов значительно усложнит задачу злоумышленникам.

Берегите свои пароли: не храните их записанными на рабочем месте, не передавайте другим людям, не сохраняйте на чужих компьютерах, не вводите их на подставных страницах. Будьте бдительны, оберегая свои персональные данные.

Как работают хакеры?

Чтобы защититься от злоумышленников, стоит разобраться в тех средствах, которые они используют в своей работе. Лучше защитить аккаунт на онлайн-ресурсе поможет знание приемов, которые применяют в работе хакеры.

На современном интернет-жаргоне хакерами (или крэкерами) называют компьютерных взломщиков — программистов, злонамеренно добывающих конфиденциальную информацию в обход систем защиты. Среди них встречаются как любители, промышляющие взломом аккаунтов социальных сетей, так и настоящие профессионалы, представляющие серьезную угрозу информационной безопасности целых стран.

Как правило, личный почтовый ящик или аккаунт в социальной сети становится предметом интереса начинающих хакеров и мошенников, которые в своей работе используют относительно простые приемы. Приведем ниже самые известные.

Метод грубой силы. Угадывание пароля с помощью простого перебора всех возможных комбинаций символов. Этот метод может использоваться как «вручную», так и с помощью специальных аппаратных средств. Время, которое в данном случае требуется на взлом аккаунта, пропорционально количеству возможных комбинаций, которое можно определить по формуле:

$$X^y,$$

где X — это количество символов, используемых при составлении пароля, а y — это длина пароля.

Соответственно, чем длиннее пароль и чем больше видов символов в нем используется, тем больше времени уйдет у

злоумышленников на взлом аккаунта. Если использовать в восьмизначном пароле буквы в верхнем и нижнем регистрах, цифры и специальные символы, то количество возможных комбинаций составит число с 15 нулями. Очевидно, что если ваш пароль не ведет к пещере Али-Бабы, то, скорее всего, злоумышленники не станут тратить на него свои силы и время. Именно поэтому необходимо использовать длинные пароли.

Метод логического угадывания. Для того чтобы сузить потенциальный круг возможных комбинаций и сократить время взлома, злоумышленники могут попытаться угадать пароль, используя персональную информацию, размещенную на странице в социальной сети. Многие пользователи используют в качестве пароля свое имя или фамилию, год рождения, номер телефона и другие личные данные. Безусловно, такую комбинацию легче запомнить, но и взломать ее гораздо проще. Также злоумышленники могут использовать для подбора списки наиболее популярных паролей. Вы удивитесь тому, как много людей используют простейшие комбинации для защиты персональных данных. Для многих автоматических систем безопасности пароль ФЫВА1234!»№; выглядит достаточно сложным, но взломать его очень просто. Поэтому необходимо использовать сложные пароли, представляющие собой бессмысленную комбинацию символов.

Фишинг. В данном случае речь идет не об угадывании пароля, пользователь сам вводит нужную комбинацию на поддельной странице, созданной злоумышленниками. Сложный пароль не в состоянии уберечь от фишинга. Бдительность — вот лучшая защита от взломщиков. Внешне отличить поддельную фишинговую страницу от настоящей практически невозможно, поэтому необходимо обращать внимание на адресную строку. Следует с осторожностью относиться

к письмам от службы технической поддержки сайтов, сообщающим о взломе или попытке доступа к вашему аккаунту. Не стоит переходить по ссылкам, содержащимся в таких письмах, а также следует внимательно проверять адресную строку, прежде чем вводить свои логин и пароль.

Вредоносные программы. Еще один способ кражи аккаунтов, к которому могут прибегать злоумышленники, — это использование различных вредоносных программ. Чаще всего они незаметно проникают на устройство пользователя или скачиваются под видом полезных приложений, а затем высылают персональные данные своему создателю. Единственная защита от этой проблемы — использование антивирусных программ.

Социальная инженерия. Это методы взлома, основанные на хорошем знании злоумышленником психологии и поведения пользователя. Втираясь в доверие к жертве, мошенник буквально выуживает у него информацию, необходимую для взлома аккаунта. Например, не так уж сложно узнать сведения, которые содержат ответ на контрольный вопрос, использующийся некоторыми системами для восстановления доступа к аккаунту. Вы и не заметите, как сообщите в приватной беседе новому онлайн-френду девичью фамилию своей матери, кличку вашей первой собаки или название любимой футбольной команды. Однако это еще не все, опытный мошенник под благовидным предлогом может даже убедить выдать пароль.

В принципе, злоумышленники могут взломать практически любой аккаунт. Тем не менее если вы не являетесь главой государства или суперзвездой, то здравого смысла и соблюдения простых правил безопасности достаточно, чтобы надежно обезопасить свои данные в интернете.

Приложение № 5.1

ДЕСЯТЬ САМЫХ ПОПУЛЯРНЫХ ПАРОЛЕЙ СРЕДИ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТА*

- **PASSWORD** или слово **ПАРОЛЬ** в транслитерации латиницей (**gfhjkm**).
- **QWERTY** и другие варианты раскладки клавиатуры.
- Простые числовые последовательности (**12345678**, **87654321**, **11111111** и т.д.).
- Сочетание простых числовых и буквенных последовательностей (**абвг1234**, **аааа1111** и т.д.).
- Сочетание личных имен собственных (имя, фамилия и т.д.) и значимых чисел (года рождения, номера телефона и т.д.), например, **САША2000**, **ИВАНОВ1001010** и т.д.
- Популярный молодежный сленг, например, **ФИТОНЯШКА**, **ОЛОЛО** и т.д.
- Фразы типа **ОТКРОЙСЯ**, **ВПУСТИМЕНЯ** и т.д.
- **ILOVEYOU** или **ЯТЕБЯЛЮБЛЮ** в транслитерации латиницей.
- Популярные виды спорта, например **ХОККЕЙ.**
- Популярные имена, например **АНАСТАСИЯ**, **ВИКТОРИЯ** и т.д.

---

* URL: http://ng72.ru/dosug/view/20-01-2016-samye-populyarnye-paroli-2015-goda-ot-polzovateley-interneta-20-yanvarya-2016-goda; http://www.chaskor.ru/article/top-20_parolej_runeta_2150.

Приложение № 5.2

ПРАВИЛА СОСТАВЛЕНИЯ НАДЕЖНЫХ ПАРОЛЕЙ

Признаки надежного пароля

- Надежный пароль должен:
  – состоять из 8–16 символов;
  – включать в себя буквы, цифры и специальные символы;
  – включать в себя символы в верхнем и нижнем регистре.
- Не следует использовать слова, словосочетания, а также комбинации, которые можно легко угадать.
- Целесообразно использовать двухэтапную аутентификацию с помощью мобильного телефона.
- Для каждого аккаунта необходимо иметь свой пароль.
- Необходимо менять пароли ко всем аккаунтам раз в 3–6 месяцев.
- При столкновении с попыткой взлома одного из аккаунтов необходимо поменять пароли на всех аккаунтах.

Способы составления надежного пароля

Для получения сложного, но легко запоминающегося пароля можно использовать любое слово, зашифровав его с помощью одного из следующих методов:

- *Транслитерация.* Если взять любое слово русского языка и набрать его на клавиатуре с латинской раскладкой, то получится бессмысленное сочетание символов. Например **RJYUHTUFWBZ** — это слово «конгрегация». К сожалению, этот метод плохо подходит для устройств с виртуальной клавиатурой, где отсутствует двойная подпись клавиш.

- *Смещение по клавиатуре.* Если при написании слова каждый раз смещаться по клавиатуре на одну клавишу влево, мы используем *простое смещение*, например **ВПЬЦЩ** — это слово «арбуз». Если менять направление смещения по или против часовой стрелки, мы используем *сложное смещение*, например **ЛПТВЛПР** — это слово «барабан».
- *Акроним.* Если взять первые буквы слов из известной фразы, то мы получаем акроним, который можно использовать в качестве пароля. Например **МДСЧПКНВШЗ** — это первые две строки из романа А.С. Пушкина «Евгений Онегин».
- *Известные последовательности.* Также для составления пароля можно использовать первые буквы известных последовательностей слов. Например **ЯФМАМИИАСОНД** — это двенадцать месяцев. Всегда можно усложнить последовательность, например изменив направление и величину шага. **ДОАИАФНСИММЯ** — это последовательность месяцев наоборот и через один.
- *Чередования символов.* Любой пароль можно усложнить, добавив последовательность цифр или знаков, которые можно чередовать с зашифрованным словом. Например **П1А2Р3О4Л5Ь6**.
- *Псевдографика.* Достаточно сложный, но хорошо запоминающийся пароль можно создать с помощью псевдографики — использования символов шрифта для создания графических изображений. Например набор символов **_>(0:o:0)<_** похож на кошачью мордочку.

Чтобы сделать надежный пароль, необходимо использовать несколько различных видов шифрования. Возьмем слово **ПАРОЛЬ**, транслитерируем — **GFHJKM**, добавим через одну букву шесть цифр, но в обратном порядке — **G6F5H4J3K2M1**,

а теперь поменяем цифры через одну на соответствующие им символы — **G6F%H4J#K2M!**.

Одну и ту же систему шифрования можно использовать для разных паролей, добавив систему индексов, например: **ПАРОЛЬ**MAIL.RU, **ПАРОЛЬ**GMAIL.COM, **ПАРОЛЬ**VK.COM. Это существенно упростит процедуру запоминания паролей и сделает их достаточно надежными и безопасными.

Приложение № 5.3

КАРТОЧКИ С ЗАДАНИЯМИ

Пути потери паролей	Правила хранения и защиты паролей
Карточка № 1. Пароль на бумажке	
Исследования компании ESET, специализирующейся на разработке антивирусного ПО, показали, что 16% россиян записывают пароли и PIN-коды на бумаге — в блокнотах и на стикерах*. Однако бумажку с паролем можно потерять, а главное, она легко может попасть в руки злоумышленнику, который не преминет использовать ее против доверчивого пользователя	Не стоит хранить пароли к аккаунтам онлайн-ресурсов записанными на листе бумаги, особенно там, где их легко можно найти. Лучше всего хранить пароли в голове или использовать специальные программы-менеджеры паролей

Карточка № 2. Обманутое доверие	
По данным исследований Фонда Развития Интернет, почти каждый второй российский школьник давал свой пароль от аккаунта в социальной сети друзьям (22%), родителям (14%), братьям или сестрам (8%), онлайн-друзьям (8%) и даже незнакомцам (1%). Излишней доверчивостью пользователя могут воспользоваться как случайные знакомые, так и друзья	Никому не стоит доверять пароль к своему аккаунту в социальной сети, особенно малознакомым людям. Если все же случилось так, что пароль попал в чужие руки, нужно сразу же сменить пароли ко всем имеющимся у вас аккаунтам

* URL: https://www.esetnod32.ru/company/press/center/16-rossiyan-zapisyvayut-paroli-i-pin-kody-na-bumazhke/.

Карточка № 3. Осторожно, чужой компьютер	
Как показывает статистика обращений на Линию помощи «Дети Онлайн», одна из основных причин взлома подростковых аккаунтов в социальных сетях — вход, выполненный с чужого компьютера, например, в классе или в гостях. Завершая сеанс работы, многие школьники забывают выйти из социальной сети и просто закрывают окно браузера. В этом случае логин и пароль сохраняются на компьютере, и любой пользователь может войти в оставленный без присмотра аккаунт	Работая на чужом компьютере, всегда нужно использовать опцию «чужой компьютер» или «не сохранять пароль». Завершая сеанс, нужно выйти из аккаунта и убедиться, что войти в него без повторного ввода пароля невозможно. Чтобы исключить случайный доступ других пользователей к аккаунту, нужно использовать двухэтапную систему аутентификации пользователя с помощью мобильного телефона. Если вам все-таки кажется, что кто-то мог войти в ваш аккаунт без вашего ведома, обязательно поменяйте пароли ко всем имеющимся у вас аккаунтам

Карточка № 4. Онлайн-мошенничество	
По данным исследований Фонда Развития Интернет, 28% российских школьников сталкивались со взломом аккаунта в социальной сети. Как правило, это происходит в результате действий онлайн-мошенников. Пользователь получает поддельное письмо от «службы поддержки», в котором сообщается, что его аккаунт был подвергнут атаке. Далее пользователю предлагается пройти по ссылке на поддельную (фишинговую) страницу для замены пароля. Для подтверждения действия требуется ввести старый пароль. Стоит это сделать — и «ключ» от аккаунта попадет в руки злоумышленника	Не доверяйте письмам и сообщениям о взломе вашего аккаунта. Никогда не переходите по подозрительно длинным ссылкам, которые пришли к вам по электронной почте. Не поленитесь вручную набрать ссылку в адресной строке. Если страница запрашивает ввод пароля, убедитесь, что у нее верный адрес, а данные передаются через безопасное соединение по протоколу *https*

Карточка № 5. Кейлогер	
Кейлогеры — это специальные программы и устройства, позволяющие регистрировать нажатие клавиш на клавиатуре компьютера. Они могут быть использованы для кражи паролей от онлайн-аккаунтов и ПИН-кодов банковских карт. Чаще всего кейлогеры проникают на устройства простых пользователей незаметно и работают как шпионские программы	Используйте программы комплексной сетевой защиты, предотвращающие попадание программ-кейлогеров на ваш компьютер. Используйте программы безопасного ввода данных и виртуальные клавиатуры при совершении оплат через интернет

Урок № 6

ЧТО ТАКОЕ ПРИВАТНОСТЬ И ЛИЧНЫЕ ГРАНИЦЫ?

Цель: знакомство с понятиями «приватность», «личные границы», «зона персонального пространства»; исследование собственных личных границ.

Разминка «Мои границы»

Задача: познакомить участников с понятиями «личные границы» и «приватность».

Необходимые материалы: мел, клубок яркой плотной нити или веревки.

Время проведения: 10–15 минут.

Процедура проведения

Ведущий начинает занятие с рассказа о том, что право каждого человека на свои границы и личное пространство, свободное от вмешательства других людей и организаций, называется *приватностью*. В жизни она наиболее ярко проявляется в том, что каждый человек проводит вокруг себя невидимые персональные границы и обычно позволяет другим приближаться к себе физически и психологически лишь до определенного расстояния, на котором он чувствует себя комфортно.

Для проверки своих границ участникам предлагается упражнение в виде демонстрационного эксперимента с несколькими парами (можно каждый раз выбирать новую пару, а можно менять только одного из участников). Ведущий вызывает двух человек

и просит их встать друг напротив друга на расстоянии около 2–3 м. По сигналу один из участников начинает медленно подходить к другому участнику, стоящему неподвижно. В какой-то момент, когда неподвижный участник чувствует, что нарушаются его границы, он говорит «Стоп!» и останавливает подходящего. Ведущий мелом отмечает это расстояние. Процедура подхода к стоящему человеку повторяется сзади, потом справа и слева. В конце упражнения ведущий соединяет метки меловой линией и таким образом обозначает персональные границы. Упражнение может быть повторено два-три раза, каждый раз на новом месте, чтобы можно было сравнить размеры личного пространства разных учеников.

Обсуждение

- Различаются ли радиусы личного пространства у разных людей?
- От чего может зависеть терпимость к нарушению личных границ?
- Что может чувствовать человек в тот момент, когда нарушают его личные границы?
- Важны ли личные границы в интернете?

Упражнение «Персональные данные и личные границы»

Задача: дать участникам возможность исследовать соотношение различных категорий персональных данных с зонами личного пространства.

Необходимые материалы: доска, мел, раздаточные материалы по количеству участников (см. Приложение к уроку № 6.1, Приложение к уроку № 6.2), ручки или карандаши,

листы формата А1 (2 шт.), маркеры (7–8 шт.), кнопки или скотч (для прикрепления листов к доске).

Время проведения: 25–30 минут.

Процедура проведения

Упражнение состоит из нескольких этапов.

Первый этап. Ведущий объясняет участникам, что личные границы и приватность имеют большое значение и в интернете. Именно они регулируют обмен личными (персональными) данными в сети: какими-то из них мы делимся легко, а какие-то храним в секрете. Ведущий раздает детям таблицы с категориями (см. Приложение к уроку № 6.1) и круговые диаграммы (см. Приложение к уроку № 6.2) и просит участников ознакомиться с ними.

Второй этап. Ведущий рисует идентичную круговую диаграмму (см. Приложение к уроку № 6.2) на доске и объясняет участникам, что с разными людьми мы общаемся на разной дистанции. Таких дистанций или зон общения можно выделить пять.

- Зона конфиденциальности — принадлежит самому человеку. В нее, за исключением критических ситуаций, не имеет права вторгаться никто.
- Интимная (0–45 см) — зона, в которой мы общаемся только с самыми близкими людьми, теми, кому мы доверяем больше всего: родителями, близкими друзьями.
- Личная (45–120 см) — зона, в которой мы общаемся с теми, с кем мы регулярно видимся и кого достаточно хорошо знаем: одноклассниками, приятелями, знакомыми.
- Социальная (120–360 см) — зона, которая подходит для общения с малознакомыми людьми: например, с продавцами в магазине, почтальонами, водителями и т.д.

- Публичная (или общественная, более 360 см) — зона, в которой мы общаемся с человеком, которого видим впервые, а также когда мы выступаем перед незнакомой группой людей.

Третий этап. Учитель дает ученикам задание: расположить каждый из видов персональных данных, представленных в таблице (см. Приложение к уроку № 6.1), в одной из зон персонального пространства (см. Приложение к уроку № 6.2) — той, которая, по их мнению, является наиболее подходящей для того или иного вида информации.

Четвертый этап. После того как каждый участник заполнил свою личную диаграмму, ведущий предлагает детям разделиться на две подгруппы и найти общую для каждой подгруппы точку зрения на распределение персональных данных в соответствующих зонах персонального пространства. Таким образом, предыдущий этап работы повторяется в групповом формате: дети изображают диаграмму подгруппы (Приложение к уроку № 6.2) на листе А1 и маркерами вписывают в нее те или иные категории персональных данных из таблицы (Приложение к уроку № 6.1). На выполнение задания дается 7–10 минут. Затем каждая подгруппа выбирает участника, который выходит с получившейся диаграммой к доске и кратко комментирует результат. Диаграммы обеих подгрупп крепятся к доске с двух разных сторон так, чтобы в центре доски осталось свободное пространство.

Пятый этап. После презентации работ подгрупп ведущий чертит на доске финальную таблицу (см. Приложение к уроку № 6.3). В левый столбик он выписывает названия зон общения, а в правый — те категории персональной информации, которые попали в одну и ту же зону в диаграммах обеих подгрупп. После заполнения данной таблицы ведущий предлагает участникам обсудить результаты упражнения и подвести итоги.

Обсуждение

- Какие виды персональной информации одинаково классифицированы обеими подгруппами? Почему?
- Какие виды данных вызвали разногласия? Чем это можно объяснить?
- Сильно ли ваша личная диаграмма отличается от конечного варианта, представленного в финальной таблице?
- Насколько вы согласны с финальной таблицей? Поменялся ли ваш взгляд на расположение персональных данных в зонах личного пространства? С чем это связано?

Итоги занятия

В обычной жизни мы защищаем свое персональное пространство и личные границы с помощью управления личной дистанцией. Мы можем подойти ближе, если захотим пообщаться с понравившимися нам людьми, либо, наоборот, отдалиться от подозрительных личностей. В виртуальном мире невозможно присутствовать физически. Тем не менее наша личность также там представлена — в виде информации о нас, циркулирующей в интернете. От ее неприкосновенности могут зависеть наши здоровье, безопасность, отношения с окружающими людьми и деловая репутация. Именно поэтому необходимо различать, какой информацией и в каком случае можно поделиться с тем или иным человеком, когда лучше ограничиться лишь самыми основными сведениями, а какие данные всегда надо держать в строгом секрете.

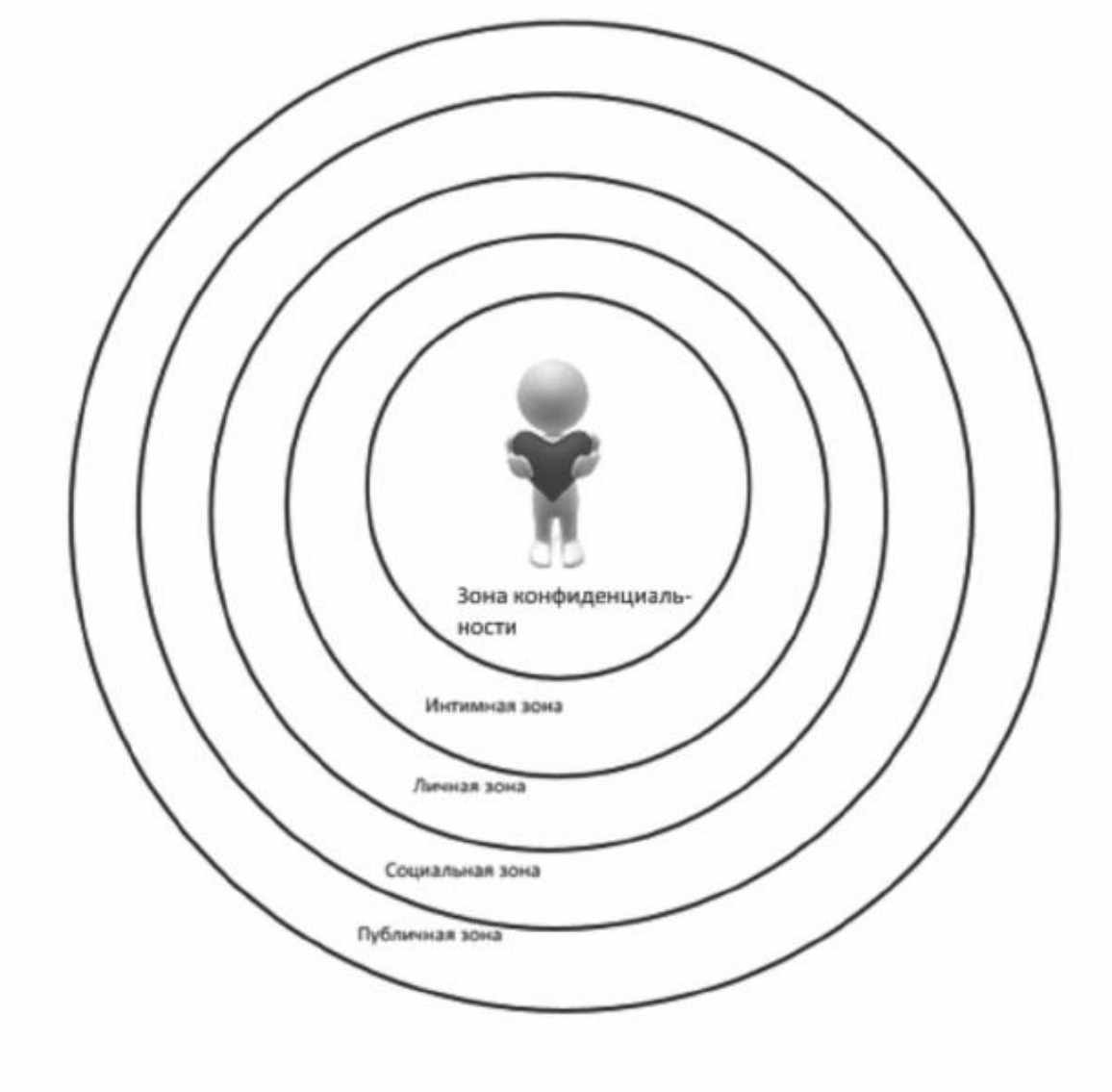
Приложение № 6.1

ТАБЛИЦА С КАТЕГОРИЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ

• Имя и фамилия
• Логин и пароль
• Номер паспорта
• Фотография
• Рост, вес, телосложение
• Состояние здоровья
• Место жительства
• Место учебы
• Места досуга и отдыха
• Информация о совершенных покупках
• Информация об имуществе (интерьер, квартиры, украшения, вещи)
• Информация о наличии денежных средств
• Состав семьи
• Участие в конкурсах, достижения, награды, дополнительная учеба
• Участие в кружках и секциях
• Основной вид занятости
• Информация о родителях
• Информация о других родственниках
• Информация о друзьях
• Принадлежность к различным неформальным группам
• Хобби
• Интересы, ценности
• Подробности личной жизни
• Настроения, вкусы
• Черты характера
• Знания, умения, навыки
• События из жизни (дни рождения, вечеринки)

Приложение № 6.2

КРУГОВАЯ ДИАГРАММА



Урок № 7

КАК НАСТРАИВАТЬ ПРИВАТНОСТЬ В СЕТИ?*

Цель: дать учащимся возможность исследовать собственный баланс «открытости — закрытости» и познакомить их с основными настройками приватности в сети.

Разминка «Открытость — закрытость»

Задача: помочь участникам исследовать личный баланс «открытости — закрытости» своих персональных границ.

Необходимые материалы: доска, мел.

Время проведения: 5–10 минут.

Процедура проведения

Ведущий говорит участникам о том, что каждый человек выстраивает свои личные границы в общении с окружающими людьми. Проницаемость и прочность этих границ зависит от степени нашей «закрытости — открытости» миру. Например, кто-то замкнут и тщательно дозирует информацию о себе, а кто-то, напротив, охотно делится различного рода сведениями с окружающими людьми. Участникам предлагается исследовать свой личный баланс «открытости — закрытости». В двух противоположных концах аудитории обозначаются два полюса — «открытость» и «закрытость», и каждому участнику дается задание мысленно представить, к какому из полюсов ближе он находится. Затем ведущий предлагает всей группе

---

* Этот урок может проводиться как самостоятельный либо как продолжение урока № 6.

выстроиться в шеренгу, образовав шкалу «открытости — закрытости». Каждый участник занимает в ней место, которое считает нужным.

Обсуждение

- Быстро ли вам удалось определить свой уровень «открытости — закрытости»?
- Насколько совпадает положение других участников на шкале «открытости — закрытости» с вашим представлением о них?
- Какие преимущества и недостатки имеет каждый из полюсов? Почему лично вам комфортен тот или иной из них?

Упражнение «Золотая середина»

Задача: предоставить участникам возможность измерить собственный уровень «открытости — закрытости» в интернете и найти свою «золотую середину».

Необходимые материалы: бланки с тестом по количеству участников (см. Приложение к уроку № 7.1).

Время проведения: 10–15 минут.

Процедура проведения

Ведущий говорит участникам о том, что чувствовать себя комфортно в физическом пространстве и в виртуальном мире возможно, когда установлен баланс между открытостью и закрытостью, найдена «золотая середина», причем у каждого человека она может быть своей. В межличностном общении «золотая середина» означает то расстояние, на котором нам комфортно и безопасно общаться с разными людьми: с роди-

телями или одноклассниками, знакомыми или незнакомыми. В виртуальном пространстве мы устанавливаем ее с помощью *настроек приватности* — системы специальных параметров, позволяющих пользователю онлайн-ресурса настраивать уровень внешнего доступа к различным видам персональной информации. «Золотая середина» в интернете подразумевает, что пользователь отрегулировал свои настройки приватности так, что каждый вид или категория персональной информации доступны только той аудитории, для которой сам человек хотел бы сделать ее открытой.

Упражнение состоит из двух этапов.

Первый этап. Индивидуальное заполнение теста каждым участником. Для измерения личного уровня «открытости — закрытости» в виртуальном мире участникам предлагается заполнить тест, позволяющий оценить уровень внешнего доступа к различным категориям персональной информации об участнике (см. Приложение к уроку № 7.1). В каждой строке предложенного бланка необходимо обвести одну цифру напротив каждого вопроса. В последнюю графу нужно вписать сумму набранных баллов. Максимальное количество баллов не может превышать 60.

Второй этап. Построение группового распределения. После подсчета участниками баллов ведущий чертит на доске шкалу «открытости — закрытости» (см. Приложение к уроку № 7.2а), выделяет на ней пять интервалов в соответствии с приведенными ниже и объясняет, как участники могут оценить полученные результаты.

- Менее 15 баллов — крайне выраженное смещение в сторону полюса «закрытости»; может свидетельствовать о чрезмерной замкнутости и склонности к самоизоляции в сети.

- 15–25 баллов — личный баланс в интернете смещен в сторону полюса «закрытости».
- 26–34 балла — промежуточное значение, которое может говорить о том, что полюса «открытости/закрытости» в интернете сбалансированы.
- 35–45 баллов — личный баланс в интернете смещен в сторону полюса «открытости».
- Более 45 баллов — крайне выраженное смещение в сторону полюса «открытости»; может свидетельствовать о том, что участник склонен сообщать другим пользователям избыточную персональную информацию.

Ведущий называет каждый интервал по очереди и просит участников, набравших сумму баллов из названного диапазона, поднять руку, затем считает количество поднятых рук и записывает получившееся количество человек над шкалой. По итогам подсчета ведущий строит распределение группы (см. Приложение к уроку № 7.2б) и переходит к обсуждению полученных результатов.

Обсуждение

- Насколько совпадает количество баллов по тесту с тем, какое положение на шкале «открытости — закрытости» вы выбрали в начале урока?
- В какой диапазон вы попали? Захотелось ли вам поменять что-либо в своих настройках приватности после получения данного результата?
- Каким получилось групповое распределение ответов? Есть ли у членов вашей группы склонность к одному из полюсов?

Упражнение «Моя приватность в сети»

Задача: привить учащимся навыки управления приватностью в социальной сети с учетом пользовательских предпочтений.

Необходимые материалы: карточки с заданиями (см. Приложение к уроку № 7.3) и таблицы с настройками приватности (см. Приложение к уроку № 7.4) по числу мини-групп, ключи для ведущего (см. Приложение к уроку № 7.5).

Время проведения: 10–15 минут.

Процедура проведения

Ведущий еще раз подчеркивает, что «золотая середина» у каждого человека своя. Более того, она может меняться со временем и зависеть от разных обстоятельств. Настройки приватности в социальных сетях помогают нам найти именно то место на шкале «открытости — закрытости», которое адекватно нашему внутреннему состоянию и жизненной ситуации. Они позволяют регулировать уровень внешнего доступа к различным видам данных в зависимости от предпочтений пользователя, его онлайн-активности, целей посещения ресурса и целого ряда других условий. Поэтому при регистрации на онлайн-ресурсах необходимо уделять специальное внимание тому, чтобы настроить свою приватность. Чтобы лучше разобраться в этом вопросе, ведущий предлагает участникам разделиться на 4 подгруппы. Каждая подгруппа получает карточку с заданием (см. Приложение к уроку № 7.3) и таблицу с настройками приватности (см. Приложение к уроку № 7.4). Участникам необходимо ознакомиться с индивидуальной ситуацией героя, определить подходящие для данного пользователя настройки приватности и заполнить таблицы. На обсуждение карточек и заполнение

таблиц дается 5–7 минут. После этого участники каждой подгруппы зачитывают свой случай и представляют результаты заполнения таблицы, делая акцент на тех настройках, которые были особенно важны герою ситуации. В конце упражнения ведущий комментирует выступление каждой подгруппы с учетом ключей (см. Приложение к уроку № 7.5).

Обсуждение

- Удалось ли вам настроить приватность героев с учетом их предпочтений?
- На основании чего вы определяете уровень внешнего доступа к тем или иным видам ваших собственных данных?
- Был ли у вас опыт жизненных ситуаций, после которых вы принимали решение о смене настроек приватности?

Итоги занятия

Каждый человек имеет право на выбор собственной «золотой середины» — личного уровня открытости или закрытости. Мы вправе свободно и самостоятельно решать, какая информация и при каких условиях может быть сохранена в секрете или передана другим людям. При этом следует помнить: если информация о нас лежит на поверхности, мы становимся уязвимыми; когда же мы, напротив, отгораживаемся от людей, устанавливая неприступные барьеры и сохраняя любые сведения в тайне, — есть риск остаться в одиночестве и лишиться тех возможностей, которые предоставляет нам цифровой мир. Настройки приватности в социальных сетях — наши помощники, которые позволяют нам регулировать личную «золотую середину» — оставаться открытыми для общения с миром и при этом оберегать свое персональное пространство от нежелательного вторжения.

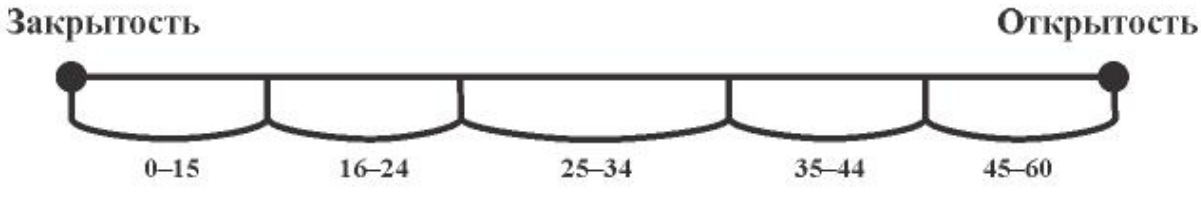
Приложение № 7.1

ТЕСТ «ЗОЛОТАЯ СЕРЕДИНА»

		Никто (Только я)	Некоторые друзья или группы друзей	Все друзья	Друзья и друзья друзей	Все пользователи
Кому ты позволишь видеть следующие типы твоей персональной информации?						
1.	Список друзей в социальной сети	0	1	2	3	4
2.	Адрес электронной почты	0	1	2	3	4
3.	Номер мобильного телефона	0	1	2	3	4
4.	Связанные аккаунты (веб-сайт, скайп и др.)	0	1	2	3	4
5.	Домашний адрес	0	1	2	3	4
6.	Фотографии с тобой	0	1	2	3	4
7.	Видеозаписи с тобой	0	1	2	3	4
8.	Список твоих групп	0	1	2	3	4
9.	Карту с твоими фотографиями	0	1	2	3	4
10.	Чужие записи на твоей странице	0	1	2	3	4
11.	Комментарии к твоим записям	0	1	2	3	4
Кто может осуществлять следующие действия в твоей социальной сети?						
12.	Оставлять записи на твоей странице	0	1	2	3	4
13.	Комментировать твои записи	0	1	2	3	4
14.	Писать тебе личные сообщения	0	1	2	3	4
15.	Приглашать тебя в сообщества	0	1	2	3	4
Общая сумма баллов:						

Приложение № 7.2а

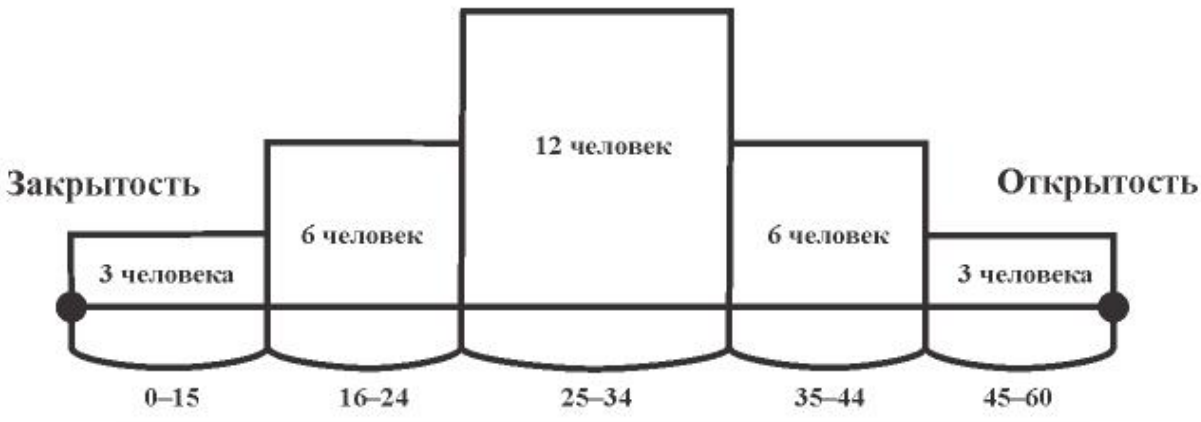
ШКАЛА «ОТКРЫТОСТИ — ЗАКРЫТОСТИ»



Приложение № 7.2б

ОБРАЗЕЦ РАСПРЕДЕЛЕНИЯ

Образец построения распределения (для группы из 30 человек, из которой 3 человека набрали 0–15 баллов, 6 человек — 16–24 балла, 12 человек — 25–34 балла, 6 человек — 35–44 балла, 3 человека — 45–60 баллов). В данной группе наблюдается оптимальное распределение: большинство участников попали в средний промежуток, у 12 человек наблюдается смещение в сторону одного из полюсов, и только 6 человек склонны к чрезмерной открытости либо закрытости в интернете.



Приложение № 7.3

КАРТОЧКИ С ЗАДАНИЯМИ

Карточка № 1

Лиза — юная и очень известная киноактриса. У нее много поклонников, которые следят за обновлениями ее странички, новыми видео с ней, и она хочет, чтобы их количество увеличивалось. Лиза хотела бы, чтобы любой поклонник мог связаться с ней через интернет. Однако ей необходимо оградить себя от нежелательных поздних звонков, визитов домой и встреч с поклонниками в тех местах, которые она посещает с близкими друзьями — это четыре подруги, объединенные списком под названием «близкие друзья». Также у Лизы есть недоброжелатели: недавно некто Михаил М. оставил на ее стене обидный комментарий, а незнакомка Ольга В. написала ей оскорбительные личные сообщения. Помогите Лизе отрегулировать приватность так, чтобы она могла комфортно общаться со своими друзьями и поклонниками и при этом не страдать от обидчиков.

Карточка № 2

Марина зарегистрировалась в социальной сети для того, чтобы найти новых друзей и группы по интересам. Она любит общаться по скайпу и вступать в дискуссии с пользователями, которые оставляют комментарии на ее страничке. Однако она знает, что в интернете есть разные люди и не все из них могут быть настроены доброжелательно. Она готова общаться со всеми, но не хочет, чтобы посторонние люди знали, где она проводит время, фотографируется. Еще Марина учится на курсах иностранного языка и вступила в группу, в которой преподаватель выкладывает задания. В связи с этим она добавила несколько человек — Вику, Дашу и Сережу — к себе в друзья. Марина хотела бы делиться с ними впечатлениями и фотографиями из своих поездок в Англию. Тем не менее видеозаписи с уроков английского языка, на которых она отмечена и которые обсуждает в личной переписке с преподавателем Маргаритой Степановной, Марина открывать для тех, кто не входит в группу английского языка, не готова, поскольку она еще не очень хорошо разговаривает на английском языке. Помогите Марине отрегулировать настройки приватности в соответствии с ее пожеланиями.

Карточка № 3

Кирилл зарегистрирован в социальной сети и использует ее для общения с одноклассниками и друзьями, с которыми он познакомился в интернете и иногда вместе играет в онлайн-игры. Кирилл вступил в сообщество, посвященное любимой онлайн-игре Lineage, для того чтобы обсуждать игровые события, и добавил некоторых участников сообщества в друзья. Несколько дней назад он поссорился с одним из них — Артемом Д., который писал обидные комментарии к записям Кирилла в группе и на его странице. Он даже звонил Кириллу на мобильный телефон и угрожал. Теперь Кирилл хочет оградить доступ к личной информации и записям на стене для всех, кого он ни разу не видел. Также Кирилл получает много рекламы и приглашений в различные группы от пользователей, которых он не знает, и это его раздражает. Помимо игр, Кирилл слушает музыку в социальной сети. Ему нравятся классические произведения, но, поскольку все одноклассники слушают или рок, или популярные песни, Кирилл стесняется и не хотел бы, чтобы кто-либо из них видел список его видео- и аудиозаписей. Помогите Кириллу настроить приватность так, чтобы ему было комфортно общаться в социальной сети.

Карточка № 4

Саша — довольно замкнутый молодой человек, у него совсем немного друзей. В социальной сети ему предложил зарегистрироваться его старший брат Игорь, который живет в другом городе: так им проще переписываться и следить за новостями друг друга. Саша хочет выкладывать новости и фотографии так, чтобы их мог видеть только его брат и близкие друзья: Вова и Петя. Еще в сети Саша познакомился со своим сверстником по имени Максим, который, как и Саша, увлекается шахматами. Саше интересно с ним переписываться и играть в шахматы онлайн, однако давать Максиму свой адрес и номер телефона Саша не готов, к тому же он не хочет, чтобы старший брат знал об этой переписке. Иногда Саша добавляет посторонних пользователей к себе в друзья «из вежливости», но в целом личные сообщения от них его мало интересуют. Помогите Саше отрегулировать настройки приватности так, чтобы ему было комфортно общаться.

Приложение № 7.4

НАСТРОЙКИ ПРИВАТНОСТИ

Настройки приватности	**Только я**	**Некоторые друзья**	**Некоторые списки друзей (указать)**	**Все друзья**	**Друзья и друзья друзей**	**Все, кроме... (указать)**	**Все пользователи**
Кто может видеть...							
Мой список друзей в социальной сети							
Мой адрес электронной почты							
Номер моего мобильного телефона							
Мои связанные аккаунты (веб-сайт, скайп, др.)							
Мой домашний адрес							
Фотографии со мной							
Видеозаписи со мной							
Список моих групп							
Карту с моими фотографиями							
Чужие записи на моей странице							
Комментарии к моим записям							
Кто может...							
Оставлять записи на моей странице							
Комментировать мои записи							
Писать мне личные сообщения							
Приглашать меня в сообщества							

Приложение № 7.5

КЛЮЧИ ДЛЯ ВЕДУЩЕГО

Пример № 1. Поскольку Лиза — публичная персона, ее «золотая середина» сильно смещена в сторону открытости. Она может оставить открытой основную информацию своей страницы, видео с ней и связанные аккаунты, чтобы ее поклонники могли связаться с ней, но не тревожили поздними звонками, и она могла ответить им в удобное для нее время. Адрес и номер мобильного телефона, а также карту с фотографиями можно оставить доступными для всего списка друзей, только для некоторых друзей (четырех подруг) либо не показывать никому. Ольгу В. следует исключить из числа лиц, которые могут писать Лизе личные сообщения (настройка «все, кроме Ольги В.»), и, поскольку она и Михаил М. — явные недоброжелатели Лизы, от них нужно максимально закрыть свой профиль: в частности, в настройках «кто может оставлять записи на моей странице и комментировать мои записи» следует указать «все, кроме Михаила М., Ольги В.».

Пример № 2. В целом можно сказать, что «золотая середина» Марины умеренно смещена в сторону открытости. Основную информацию ее страницы, список групп и связанные аккаунты можно сделать доступными всем пользователям. При этом более «чувствительные» категории данных — номер мобильного телефона, адрес, фотографии и карту посещенных мест — Марине стоит ограничить и сделать доступными только друзьям либо друзьям и друзьям друзей. Видеозаписи Марина может полностью закрыть для просмотра других пользователей, или ограничить просмотр, разрешив его только Вике, Даше и Сереже, с помощью параметра «всем, кроме...», либо используя параметр «Некоторые друзья» и, отметив преподавателя Маргариту Степановну, открыть доступ к видео только ей.

Пример № 3. Можно сказать, что в целом баланс «открытости — закрытости» Кирилла имеет небольшой уклон к полюсу «закрытости». Ему можно посоветовать оставить свои адрес и номер мобильного телефона доступными только для друзей (либо некоторых групп друзей), оставив открытой только общую информацию и, возможно, данные о связанных аккаунтах. Также Кириллу следует в настройках «кто может приглашать меня в сообщества и отправлять мне личные сообщения» установить уровень доступа «только друзья» или «друзья и друзья друзей». В соответствии с пожеланиями Кирилла, ему следует целиком ограничить для просмотра список своих аудиозаписей, используя настройку доступа «только я». В ситуации с Артемом Д. Кириллу можно порекомендовать удалить его из списка друзей либо в настройках «кто видит мои записи», «кто может оставлять записи на моей странице, комментировать мои записи и отправлять мне личные сообщения» Кириллу следует установить уровень доступа «все, кроме Артема Д.».

Пример № 4. В целом можно говорить о том, что Сашина «золотая середина» сильно смещена к полюсу «закрытости», поэтому при настройке приватности следует руководствоваться тем, чтобы предоставлять другим пользователям как можно меньше информации. Самый простой вариант — использовать в большинстве настроек параметра «некоторые друзья» и включать туда Игоря, Вову и Петю либо создать список друзей «самые близкие» и включить в него этих людей. В таком случае будет использоваться вариант «видно некоторым спискам друзей». При использовании данных настроек друг Саши по переписке Максим автоматически не будет видеть адрес и номер Сашиного телефона. Единственным исключением будет параметр «кто может писать мне личные сообщения», чтобы Максим смог и дальше с ним переписываться.

Урок № 8

КАК УПРАВЛЯТЬ РЕПУТАЦИЕЙ В СЕТИ?

Цель: познакомить участников с понятием «репутация» и научить основным правилам представления себя и управления репутацией в интернете.

Разминка «Испорченный перепост»

Задача: продемонстрировать процесс искажения личной информации в процессе ее передачи в интернете.

Необходимые материалы: карточка с заданием (см. Приложение к уроку № 8.1).

Время проведения: 10–15 минут.

Процедура проведения

В начале урока ведущий предлагает участникам поговорить о репутации. Он объясняет, что репутация — это закрепившееся в обществе мнение о человеке, группе людей или организации. Ведущий подчеркивает, что репутацией обычно дорожат, и приводит пословицу: «Береги честь смолоду» (можно предложить участникам вспомнить еще пару пословиц на эту тему). Репутацию можно долго создавать, но иногда даже случайный поступок может ее испортить. Сегодня интернет — часть нашей жизни. Наши персональные данные формируют уникальный «цифровой след», соединяющий прошлое, настоящее и будущее. Раньше собранное огромными усилиями персональное досье могло сгореть в одночасье и исчезнуть навсегда. В современном же мире наш «цифровой

отпечаток», например браузер со всеми плагинами, действиями, геометками, закладками, дополненный списком френдов и организаций, — лучшее досье, созданное нами самими, которое, как тень, всегда будет следовать за нами и влиять на нашу репутацию в реальной жизни.

Ведущий приглашает в качестве добровольцев пять человек. Четырех он просит на несколько минут выйти из аудитории, а один остается. Ведущий говорит, что сейчас зачитает вслух текст поста, взятого из интернета (см. Приложение к уроку № 8.1). Задача добровольца — внимательно его выслушать и постараться максимально запомнить, чтобы потом как можно точнее пересказать своему однокласснику, который сейчас находится за дверью. Ведущий зачитывает текст, после чего приглашает в аудиторию следующего добровольца. Первый участник объясняет второму задание (выслушать — запомнить — пересказать), а затем пересказывает ему текст поста. Ситуация повторяется до тех пор, пока все добровольцы не выполнят задание, причем последний из них пересказывает текст всей группе. В конце упражнения ведущий еще раз зачитывает исходный текст поста, чтобы ученики могли сравнить исходный результат с полученным.

Обсуждение

- Сильно ли отличается содержание первоначального поста от последнего пересказа? Почему?
- Какая информация больше всего искажается в процессе ее передачи?
- Что может влиять на степень искажения информации?

Упражнение «Деловая репутация»

Задача: помочь ученикам осознать возможные последствия неуместных публикаций в социальных сетях.

Необходимые материалы: карточки с заданиями (см. Приложение к уроку № 8.2).

Время проведения: 10–15 минут.

Процедура проведения

Ведущий предлагает участникам разделиться на четыре мини-группы. Каждая группа выступает в роли совета директоров компании, которому предстоит проанализировать ситуацию и поступок своего сотрудника, изложенные в карточке (см. Приложение к уроку № 8.2). Ведущий должен акцентировать внимание на том, что в процессе анализа необходимо учитывать потенциальные последствия этой ситуации для репутации компании. В течение нескольких минут группа должна ознакомиться с историей и вынести групповое решение о том, как поступить с этим сотрудником:

- проигнорировать этот случай;
- наказать сотрудника (объявить выговор, наложить штраф, лишить премии и т.д.) с сохранением за ним его рабочего места;
- уволить сотрудника.

После обсуждения команды по очереди представляют свои ответы. Команды выбирают участника, который выступает перед остальными: кратко рассказывает историю и представляет групповое решение.

Обсуждение

- Почему вы приняли решение так поступить с сотрудником?
- Что вы подумали об этом сотруднике, прочитав историю?
- Как, на ваш взгляд, эта публикация может отразиться на репутации компании?

После обсуждения ведущий обращает внимание участников на то, что все приведенные в карточках истории основаны на реальных случаях, которые произошли в России и других странах. Во всех рассматриваемых ситуациях сотрудник был уволен.

Упражнение «С разных точек зрения...»

Задача: дать возможность участникам осознать особенности восприятия публикаций в интернете разными пользователями.

Необходимые материалы: карточки с заданиями (см. Приложение к уроку № 8.3), пять копий фрагмента ленты из социальной сети (см. Приложение к уроку № 8.4).

Время проведения: 10–15 минут.

Процедура проведения

Информация, размещенная нами в интернете, может по-разному восприниматься людьми — в зависимости от тех отношений, в которых мы с ними состоим. Ведущий предлагает группе выполнить следующее задание. Класс делится на пять подгрупп. Каждая из них получает карточку с заданием (см. Приложение к уроку № 8.3) и карточку с фрагментом ленты из социальной сети, которую ведет школьник — их ровесник по имени Тёма (см. Приложение к уроку № 8.4). Ученики должны внимательно ознакомиться с содержанием ленты и принять реше-

ние в соответствии с условиями и вопросами, содержащимися в карточке с заданием. На это отводится 5–7 минут.

Затем представители от каждой подгруппы по очереди делятся своими впечатлениями и отмечают, что понравилось и что не понравилось им в ленте, а также озвучивают принятое группой решение. В конце упражнения ведущий обращает внимание класса на то, что посты одного и того же человека в социальной сети по-разному воспринимаются людьми. Поэтому прежде чем выкладывать пост в интернет, нужно хорошо подумать, как эта информация будет оцениваться родителями, друзьями, учителями и просто виртуальными знакомыми.

Обсуждение

- От чего зависит восприятие одной и той же информации разными людьми?
- Какая информация способствует созданию положительного впечатления об авторе рассмотренной записи, а какая, напротив, характеризует его в негативном ключе?
- Какие рекомендации вы бы дали автору блога для того, чтобы улучшить его репутацию?

Итоги занятия

Сегодня репутация в интернете так же важна, как и в реальной жизни. Более того, репутация в сети может напрямую влиять на реальную жизнь. Есть информация, что большинство работодателей просматривают социальные профили потенциальных сотрудников при приеме на работу.

Опубликовав в интернете информацию, люди сразу же теряют над ней контроль, поэтому важно понимать, с какой целью мы выкладываем те или иные сведения в сеть, и знать, какие у нас есть инструменты для управления своей репута-

цией и профилактики негативных последствий. Запомните следующие правила:

- Пословица «Слово не воробей, вылетит — не поймаешь» справедлива и для интернет-пространства. Нельзя выкладывать в открытый доступ то, что может навредить вашей репутации сейчас или в будущем.
- Необходимо тщательно настраивать уровень доступа к различным категориям персональной информации или сделать свой профиль закрытым. Если по каким-либо причинам это невозможно или влечет неудобства — еще строже оценивайте информацию, которую размещаете.
- Нельзя выкладывать информацию, когда вас переполняют эмоции. Все мы иногда говорим и делаем такие вещи, о которых потом сожалеем. Остановитесь и задумайтесь о том, как ваши посты могут повлиять на вашу репутацию. Публикация гневного поста может принести вам облегчение, однако минутное удовольствие не стоит того потенциального вреда, который оно может причинить.
- Нужно внимательно просматривать всю информацию и контент своих профилей в социальных сетях 1–2 раза в год. У вас будет возможность обнаружить и удалить потенциально опасные для вашей репутации фотографии и видео до того, как вы пойдете на собеседование при приеме в институт, на стажировку, на работу и т.д.

Лайкни и уволься: как потерять работу из-за активности в социальных сетях[*]

Если вы хотите быть уволенным за собственные взгляды, не обязательно разражаться резкими речами при начальнике или публиковать эмоциональные посты в соцсетях. Иногда достаточно одного движения: клика указательным пальцем по иконке «лайк». «Лента.ру» вспоминает самые красноречивые из подобных случаев и размышляет, что именно не стоит отмечать как понравившееся, чтобы не остаться без работы.

Молчаливое одобрение

Соцсети все глубже проникают в нашу профессиональную деятельность, даже если мы этого не хотим: достаточно иметь аккаунт и время от времени проявлять в нем активность. В ноябре 2015 г. житель Великобритании Трой Гаррорд был уволен из книжного издательства Bertrams Book, где работал с 2011 г., после того как поставил в Facebook лайк под опубликованной коллегой фотографией.

На снимке, из-за которого разгорелся весь сыр-бор, был изображен свитер одного из сотрудников компании с принтом в виде волчьей стаи. Коллега Гаррорда выложила фотографию неэстетичного, с ее точки зрения, предмета гардероба с подписью: «Боже мой, я рыдаю!.. Уверена, это подойдет для группы “Почитатели одежды с волками”, ха-ха-ха». 27-летний Трой поставил лайк под фото, за что и поплатился: в электронном письме, которое Гаррорд получил от своего начальника через несколько дней, было сказано, что «лайк неприемлемого фото» является издевательством над владельцем предмета

* По материалам портала Лента.ру. URL: http://lenta.ru/articles/2015/11/08/betternotlike/.

одежды. Ему предложили избавить компанию от своего присутствия. Автор поста про свитер также была уволена.

Один лайк — шесть увольнений

В штате Виргиния сразу шесть сотрудников окружной полиции были уволены после того, как отметили в качестве понравившейся страничку главного политического оппонента своего шефа. Шериф Би-Джей Робертс увидел в лайках подчиненных отсутствие корпоративного единства. Один из уволенных, Дэниэл Рэй Картер, не захотел сдаваться без боя и обратился в суд, требуя признать, что лайки тоже подпадают под гарантированный первой поправкой к Конституции закон о свободе слова. Однако судья отверг его аргумент, посчитав, что закон о свободе слова не может защитить то, что, в сущности, не было высказано.

Воспаление хитрости

Одна из сотрудниц Национального банка Швейцарии решила устроить себе день, полный маленьких удовольствий: прогул работы, диван и интернет. Начальству женщина заявила, что у нее приступ мигрени, единственное верное средство от которой — лежать в полной тишине и темноте в постели. Ей позволили отлежаться. Но «больная» вдруг начала проявлять активность в соцсетях, ставя лайки под постами друзей. Очевидно, швейцарка забыла, что внесла руководство в список друзей. За свою забывчивость женщина и была уволена.

Лайкать правильно

Соцсети — не только мощный инструмент для работы, но и потенциальная угроза карьере. Все чаще работников (особенно тех, кто трудится в крупных компаниях со шта-

том более тысячи человек) увольняют за лайки, ретвиты, фото и посты. Более того, если публикация была особенно скандальной, могут возникнуть проблемы с дальнейшим трудоустройством: слухи о подобных прецедентах распространяются очень быстро — благодаря все тем же социальным медиа. Несколько правил онлайн-этикета помогут избежать ситуаций вроде описанных выше.

- Отмечая страницу в соцсети как понравившуюся, лучше убедиться, что она никак не конфликтует с ценностями компании, в которой вы работаете.
- Важно помнить: в Facebook выбранная для сообщения мера конфиденциальности «только для друзей» не защитит информацию на 100%. Любой из них может сделать репост или скриншот, и сообщение увидят не те, кому оно предназначалось.
- Не пишите в соцсетях о своей работе, офисе, коллегах и боссе ничего, кроме 100% позитивного. Всегда найдутся люди, готовые трактовать обсуждение рабочих моментов как негатив.
- Не надо писать о работе в комическом ключе: чувство юмора у всех разное, и всегда найдутся те, кому шутка покажется не смешной, а оскорбительной.
- Лучшее качество дорожащего карьерой пользователя соцсетей — умеренность. Демонстрация радикальных взглядов и убеждений всегда может выйти боком. А такой демонстрацией, как мы уже убедились, в наши дни считается даже простой лайк.

Приложение № 8.1

ПОСТ ДЛЯ ПЕРЕСКАЗА

Спасибо всем за поздравления с Днем рождения! Вчера, 13 марта, когда я пошла на прогулку, мои друзья организовали сюрприз для меня! Это было неожиданно и очень приятно! Они подарили мне Сертификат на присвоение моего имени — Маркиза Габриэла — звезде 12-й величины в Созвездии Рыбы. Я получила и другие подарки — орхидеи, телефон, ноутбук. К сожалению, на встрече не было Леры Хомовской и Насти Осиповой, потому что они живут в других городах. Спасибо огромное Эрику Назаревичу, который все сумел организовать! Теперь я планирую улететь на Кубу на три месяца. Я уже подготовила Диди и Риту к поездке, сделала им прививки, купила новые переноски, корм любимый с собой в поездку, новый гардероб. Рита уже отдыхала на Кубе, наверное, она рассказала об этом Диди! ☺ Думаю, что отдых получится замечательным!

Приложение № 8.2

КАРТОЧКИ С ЗАДАНИЯМИ

Карточка № 1

Вы входите в совет директоров международной корпорации, которая очень дорожит своей репутацией. Одна из ваших сотрудниц утром отпросилась с работы, пожаловавшись на плохое самочувствие. Она утверждала, что у нее очень сильно болит голова и ей тяжело работать за компьютером. Спустя пару часов она опубликовала заметку на своей странице в популярной социальной сети. В заметке она предлагала друзьям сходить в кино на ближайший сеанс. Вы:

- *не обратите внимания;*
- *накажете сотрудницу;*
- *уволите сотрудницу.*

Карточка № 2

Вы тренируете волейбольную команду и дорожите ее безупречной репутацией. Ваша команда недавно выиграла чемпионат России и готовится к международным соревнованиям. Один из спортсменов был отмечен в социальной сети на фотографиях с дружеской вечеринки. На одной из фотографий он позирует рядом со спящим молодым человеком, разрисованным оскорблениями и свастиками. Вы:

- *не обратите внимания;*
- *накажете спортсмена;*
- *исключите спортсмена из команды.*

Карточка № 3

Вы владеете крупной фармацевтической компанией, производящей витамины и биодобавки для похудения. Вы дорожите вашей безупречной репутацией. Ваш агент по связям с общественностью опубликовал на своей странице в социальной сети фотографию с соревнований по поеданию гамбургеров и картошки фри. Вы:

- *сделаете вид, что не видели публикации;*
- *накажете сотрудника;*
- *уволите сотрудника.*

Карточка № 4

Вы управляете банком. Ваша репутация у вкладчиков оказывает прямое влияние на конкурентоспособность вашего банка. Один из сотрудников службы по связям с общественностью вашего банка на следующей неделе уходит в отпуск. Вчера он опубликовал запись в своем твиттере: «Мы заработали кучу денег на вкладчиках, можно ехать тусить!». Вы:

- *сделаете вид, что не видели публикации;*
- *накажете сотрудника;*
- *уволите сотрудника.*

Приложение № 8.3

КАРТОЧКИ С ЗАДАНИЯМИ

Карточка № 1

Представьте, что вы — Тёмин отец. Время близится к Новому году, и ваш сын уже несколько раз спрашивал вас о том, где вы с женой будете его отмечать. Вы догадываетесь, что он хочет собраться в квартире со своими друзьями. Ваша жена пока об этом не знает, а вы еще не решили, пойти ли ему навстречу.

- *Какое у вас осталось впечатление от блога вашего сына?*
- *Какие записи произвели на вас положительное впечатление, а какие — отрицательное?*
- *Разрешите ли вы вашему сыну организовать новогоднюю вечеринку у себя дома? Аргументируйте свое решение.*

Карточка № 2

Представьте, что вы — лучший друг Тёмы. Вы давно и близко знакомы, вместе учитесь, и у вас нет друг от друга секретов. Недавно он попросил у вас в долг пять тысяч рублей, которые, по его словам, он хотел потратить на покупку собаки. У вас есть некоторые сбережения, поэтому вы можете одолжить ему эту сумму, однако пока не приняли окончательное решение о том, пойти ли ему навстречу.

- *Какое у вас осталось впечатление от блога вашего лучшего друга?*
- *Какие записи произвели на вас положительное впечатление, а какие — отрицательное?*
- *Одолжите ли вы своему лучшему другу денег на покупку собаки? Аргументируйте свое решение.*

Карточка № 3

Представьте, что вы — классный руководитель Тёмы. Неделю назад директор школы сообщил вам о том, что вам необходимо выбрать из класса пять учеников, которым на каникулах в качестве поощрения предоставят возможность поехать в зимний лагерь во Францию. Вам необходимо принять решение о том, включите ли вы автора блога в список участников поездки.

- *Какое у вас осталось впечатление от блога вашего ученика?*
- *Какие записи произвели на вас положительное впечатление, а какие — отрицательное?*
- *Включите ли вы своего ученика в список участников поездки? Аргументируйте свое решение.*

Карточка № 4

Представьте, что вы — девушка, которая посещает тот же спортзал, что и Тёма. Недавно он подошел к вам после тренировки и попросил номер вашего телефона. Вчера он позвонил вам и пригласил на свидание в кино. Пока вы не приняли окончательного решения о том, соглашаться на встречу с ним или отказать, и обещали подумать до следующей недели.

- *Какое у вас осталось впечатление от блога?*
- *Какие записи произвели на вас положительное впечатление, а какие — отрицательное?*
- *Пойдете ли вы в кино с автором данного блога? Аргументируйте свое решение.*

Карточка № 5

Представьте, что вы — сотрудник по подбору персонала в компании, которая на данный момент ищет сотрудников из числа старшеклассников для временной работы на выставке в новогодние каникулы. Работа не требует особых знаний и навыков, но вам важно, чтобы соискатели были вежливыми и приветливыми, умели грамотно общаться с посетителями выставки и приходили на работу вовремя. Вы нашли блог пользователя Артема и теперь размышляете, приглашать ли его на собеседование.

- *Какое у вас осталось впечатление от блога?*
- *Какие записи произвели на вас положительное впечатление, а какие — отрицательное?*
- *Пригласите ли вы автора данного блога на собеседование? Аргументируйте свое решение.*

Приложение № 8.4

ФРАГМЕНТ БЛОГА СТАРШЕКЛАССНИКА ТЁМЫ

09.11 ПН	Только ноябрь, а я уже хочу Новый год))) подарки, новогоднее настроение, елки, каток и прочую тему! 🎄
01.11 ВС	Вчера отметили ДР Санька. Нормально поугорали! Особенно, когда шли за кое-чем;)))) В магазе не продают, хорошо хоть знаем где взять 👌 По-моему, сегодня с утра впервые узнал что такое «сушняк» 😷 p.s. Прости, мам, надеюсь, ты не заметишь разбитых бокалов.
15.10 ЧТ	Нашел по пути домой клевый смартфон, почти новый. Решил оставить себе — прошлому владельцу по ходу не нужен, раз такими девайсами раскидывается 📱
02.10 ПТ	Мне кажется, я уже вполне созрел, чтобы завести собаку, но я не хочу вставать в 7, чтобы ее выгуливать(((Хотя может стоит потренироваться перед взрослой жизнью на работе. Интересно, а те, кто пишет в резюме «пунктуальность» всегда говорят правду?
27.09 ВС	Меня не затащишь в спортзал, но если я все же там оказался — уже не вытащишь! Хоть где-то польза от моего упрямства! 💪
22.09 ВТ	Подрался с Ивановым. Достал уже. Втащил ему, завтра с родителями в школу. Вину не признаю, он сам *****!
21.09 ПН	Сегодня нес сумку одноклассницы, тяжелее моей раза в два. Спрашиваю: «Кать, че у тебя там?» Она: «Ну, книги там, тетради. И 38 (!!!) лаков» Впадаю в ступор: «Катя, СКОЛЬКО?! ЗАЧЕМ?» — «Подруге мама привезла, мне надо было два выбрать, а я утром не успела. Ну и взяла в школу»... ТЕЛКИ!!!
02.09 СР	УЧИТЕЛЯ НУ ВЫ ВООБЩЕ год только начался какого черта уже столько домашки??!!! 😠

Урок № 9

ЧТО МОЙ СМАРТФОН ЗНАЕТ ОБО МНЕ?

Цель: знакомство с вариантами распространения персональных данных через мобильные приложения.

Разминка «Никто, кроме моего смартфона, не знает, что я...»

Задача: помочь учащимся осознать, какие персональные данные хранятся на их смартфоне.

Необходимые материалы: небольшой мячик.

Время проведения: 5 минут.

Процедура проведения

«У каждого из нас есть мобильный телефон или смартфон, в котором хранится много важной и полезной информации, в том числе и наши персональные данные. Записная книга хранит контакты, мессенджеры — переписку с друзьями, игровые приложения — историю наших побед и поражений и т.д. Иногда создается впечатление, что наш телефон знает о нас гораздо больше, чем наши родственники и друзья».

Ведущий предлагает учащимся сыграть в следующую игру. Ведущий берет мяч в руки и говорит фразу, начинающуюся со слов *«Никто, кроме моего смартфона, не знает, что я...»* (возможные варианты ответов: *выиграл в онлайн-шахматы 90 партий из 100, переписываюсь с другом из Люксембурга, пробежал в прошлое воскресенье 25 км и т.д.*). Затем ведущий бросает мяч любому участнику группы. Задача участника — придумать свое окончание фразы *«Никто, кроме моего смарт-*

фона, не знает, что я...» и передать мяч следующему игроку. Игра продолжается до тех пор, пока все учащиеся не скажут свой вариант ответа.

Обсуждение

- Легким или сложным показалось вам это упражнение? Почему?
- Какой из вариантов фразы показался самым необычным или запомнился больше всего? Почему?
- Как по-вашему, то, что наши смартфоны так много знают о нас — хорошо или плохо? Почему?

Упражнение «Умные вещи»

Задача: помочь учащимся осознать, каким образом персональные данные попадают в смартфоны и другие «умные» устройства.

Необходимые материалы: карточки с заданиями (см. Приложение к уроку № 9.1).

Время проведения: 15 минут.

Процедура проведения

Сегодня в мире появляется все больше и больше «умных» устройств, задача которых — облегчить и улучшить нашу жизнь. Помимо смартфонов («умных» телефонов), существуют «умные» одеяла, плиты, кроссовки и другие полезные вещи, которыми можно управлять с помощью смартфонов. Эти устройства оснащены датчиками, которые позволяют им собирать всю необходимую информацию о нас, чтобы сделать нашу жизнь максимально комфортной и удобной. И, конечно, все эти устройства подключены к сети. Это явление нередко называют

«интернетом вещей»*. Для лучшего понимания устройства «умных» вещей и того, какую личную информацию они знают о нас, ведущий предлагает учащимся разделиться на пять микрогрупп и выполнить следующее упражнение. Каждая группа получает карточку с описанием «умной» вещи (см. Приложение к уроку № 9.1). Задача — внимательно изучить описание устройства и высказать предположение, какие персональные данные о пользователе оно может собирать. Когда задание выполнено, каждая группа озвучивает результаты своей работы, а ведущий корректирует ответы в соответствии с ключами к упражнению (см. Приложение к уроку № 9.2).

В помощь ведущему. «Умные» устройства собирают персональные данные для того, чтобы работать в соответствии с запросами пользователей и обеспечивать максимально индивидуальный подход к каждому из них. «Умному» одеялу необходимо «знать» температуру тела человека, чтобы обеспечить комфортный и здоровый сон именно для него, с учетом всех индивидуальных особенностей его организма. «Умным» кроссовкам нужно «знать» маршрут, а также физиологические показатели владельца, чтобы максимально точно рассчитать оптимальную для него нагрузку и программу тренировок. Таким образом, мы «обмениваем» свои персональные данные на удобство и комфорт, позволяющие достигать максимальных результатов на пути к поставленной цели.

Обсуждение

- Какое из устройств вам больше всего понравилось? Почему?

---

* Подробнее см. журнал «Дети в информационном обществе» (№ 18). URL: http://detionline.com/assets/files/journal/18/inf-obshestvo.pdf.

- Зачем «умным» устройствам нужны наши персональные данные?
- Стоят ли комфорт и удобство того, чтобы делиться нашими персональными данными? Если да, то почему?

Упражнение «Лаборатория мобильных приложений»

Задача: помочь учащимся осознать, что при выборе мобильных приложений необходимо ориентироваться на соотношение возможностей, предлагаемых ресурсом, и запрашиваемых им персональных данных.

Необходимые материалы: листы ватмана формата А1, цветные маркеры, наклейки.

Время проведения: 25 минут.

Процедура проведения

«Существует множество “бесплатных” приложений для смартфонов, которые помогают нам в повседневной жизни и скрашивают досуг. Однако все они являются “бесплатными” лишь условно. На самом деле пользователи расплачиваются за них своими персональными данными. Поэтому нам приходится выбирать между сохранностью персональных данных и нашим удобством». Чтобы этот выбор был осознанным, участникам предлагается встать на место разработчиков мобильных приложений.

Ведущий делит учащихся на несколько микрогрупп, каждая из которых становится «командой разработчиков». Перед ее участниками стоит задача создать мобильное приложение, которое пользовалось бы популярностью у пользователей. Для этого необходимо придумать оригинальную идею приложения и сделать презентацию для потенциальных покупателей. Мате-

риал для презентации создается на листах ватмана с помощью маркеров и содержит название приложения, краткое описание основных функций, а также виды персональных данных, которые потребуются при работе с приложением. Участники могут изучить iTunes или Google Play, чтобы понять, какие приложения существуют на рынке, каким они обладают функционалом и как их рекламируют. На выполнение этой части задания отводится 10 минут.

После того как все команды выполнят задание, можно переходить к презентации проектов. Каждая группа получает 2 минуты на выступление и ответы на вопросы. Когда все презентации прозвучали, путем простого открытого голосования выбирается лучшее приложение. Голосовать за свое приложение запрещается.

В помощь ведущему. Выбирая мобильное приложение, следует задуматься, какую личную информацию оно запрашивает у пользователя взамен на предоставляемые возможности. Если набор персональных данных соответствует прямому функционалу программы, например, сервис вызова такси онлайн запрашивает информацию о вашем местоположении, то это разумный выбор. Однако если набор персональных данных очень велик и выходит за пределы функционала программы, например, погодный информер требует доступа к вашему аккаунту в социальной сети, то устанавливать ее будет не слишком разумно.

Обсуждение

- Какое приложение набрало больше всех голосов? Какое — меньше всех? Почему?
- Какими правилами следует руководствоваться, устанавливая приложение на смартфон?

Итоги занятия

Смартфоны и другие «умные» устройства все активнее проникают в нашу жизнь, делая ее более комфортной и удобной. Однако за это удобство нам приходится платить — нашими персональными данными. Без преувеличения можно сказать, что наши смартфоны порой знают о нас больше нас самих. Поэтому мы должны с осторожностью использовать смартфоны и другие гаджеты, защищать их антивирусными программами и надежными паролями. Устанавливая новые приложения на смартфон, следует внимательно ознакомиться с условиями, предлагаемыми разработчиками. Нормально, если фитнес-трекер запрашивает у вас доступ к геоданным, чтобы отследить маршрут вашей утренней пробежки, но если приложение требует от вас доступ ко всем вашим контактам в социальной сети — это может стать причиной отказа от его установки.

Защищают ли мессенджеры персональные данные пользователей?

Сегодня все больше пользователей предпочитают общаться с помощью мессенджеров. Удобство и существенная экономия — их основные достоинства. Однако, как показали исследования Фонда Электронных Рубежей (EFF)*, далеко не все мессенджеры обеспечивают необходимую защиту персональных данных своих пользователей и гарантируют конфиденциальность личной переписки.

Эксперты Фонда оценили более сорока программ по следующему набору критериев:

- использование шифрования при передаче данных;
- защита сообщения от доступа со стороны провайдера связи;
- возможность установить личность собеседника;
- защищенность переписки в случае кражи или потери устройства;
- наличие строгой документации в области политики защиты персональных данных пользователей;
- открытый доступ к коду программы, позволяющий проводить независимые проверки экспертным сообществом;
- наличие заключения по результатам экспертной проверки.

Сразу следует отметить, что среди наиболее популярных мессенджеров (WhatsApp, Viber, Google Hangouts, Facebook Chat, Skype) более двух баллов из семи по этим критериям не набрала ни одна программа. Большее, на что способны эти программы — это шифрование сообщения при передаче данных, которое тем не менее не защищает сообщение от доступа

* URL: https://www.eff.org/secure-messaging-scorecard/.

со стороны провайдеров, предоставляющих услуги связи. В случае кражи устройства вся личная переписка оказывается доступной для злоумышленников. Закрытый код и отсутствие четкой документации заставляют задуматься, все ли в порядке с безопасностью у этих приложений.

Абсолютными лидерами по результатам проверки оказались программы ChatSecure, Orbot, CryptoCat, Off-The-Record Messaging for Windows (Pidgin), Signal/RedPhone, Silent Phone, Silent Text, Text Secure — им удалось набрать семь баллов из семи возможных, а вот аутсайдером оказалась программа Mxit, которая даже не умеет шифровать сообщения.

Результаты исследования заставляют задуматься, почему далеко не самые защищенные приложения оказались самыми популярными среди пользователей. Очевидно, выбирая мессенджер, мы ориентируемся на удобство и простоту использования, а также на возможность сэкономить на услугах связи. Возможно, такой подход оправдан, если программа используется для разговоров о погоде, в противном случае пользователям необходимо задуматься, сколько стоит их личная безопасность.

Приложение № 9.1

КАРТОЧКИ С ЗАДАНИЯМИ

«Умное» одеяло

«Умное» одеяло способно контролировать температуру тела спящего человека и поддерживать ее оптимальный уровень, соответствующий биологическим потребностям человеческого организма. В основе устройства лежит так называемая программа приятного сна. Ее суть состоит в том, что разным фазам сна человека соответствует разная оптимальная температура тела, и одеяло будет стараться поддерживать нужный уровень, соответствующий текущей фазе сна. Одеяло устанавливает достаточно высокую температуру (34°С) на стадии засыпания, затем температура опускается до 30°С и вновь повышается уже перед самым пробуждением. Эта технология помогает пользователю быстро заснуть и спокойно спать. После пробуждения человек чувствует себя отдохнувшим и бодрым.

«Умные» кроссовки

«Умные» кроссовки снабжены светодиодными индикаторами, которые отражают настроение своего хозяина. На боковых сторонах обуви появляются улыбающиеся смайлики или сердечки. Благодаря встроенному в кроссовки сенсору движения, регистрирующему также давление, информация о прогулках и занятиях фитнесом их владельца собирается и анализируется приложением на смартфоне. Также кроссовки считают сожженные хозяином калории во время пробежки и следят за сердцебиением. Кроме того, в них встроена система спутниковой навигации, которая может определить и указать направление движения.

«Умный» браслет

«Умный» браслет — упругая спираль, представляющая собой мини-фитнес-центр с множеством функций. Помимо обычного сбора статистических данных, браслет нужен и для мотивации. Он вибрирует при долгом сидении на месте (призывая тем самым к активности), предлагает наметить цель на день (например, 10 тыс. шагов) и объединяет пользователей с такими браслетами в небольшую социальную сеть. Благодаря этому можно узнать, кто из друзей пробежал 10 км, а кто пролежал весь вечер на диване. На основе данных, полученных с браслета, в приложении на смартфоне выстраиваются графики суточной активности пользователя. Также браслет определяет фазы сна хозяина и может функционировать в качестве умного будильника, помогая просыпаться бодрым и отдохнувшим.

«Умный» воздухоочиститель

Внешне устройство мало чем отличается от обычных воздухоочистителей. Зато внутри «умного» воздухоочистителя находится целая система, включающая Bluetooth — для передачи сообщений на смартфон владельца, датчики, отслеживающие состояние воздуха, и систему управления устройством. Этот воздухоочиститель находит в помещении вещества, потенциально опасные для владельца (аллергены), сообщает ему об этом с помощью смартфона и уничтожает их. Помимо этого, устройство позволяет узнать, насколько загрязнен воздух в квартире, показывает состояние фильтров и прогноз погоды.

«Умный» холодильник

«Умный» холодильник — устройство, которым можно управлять с помощью смартфона или планшета. Холодильник умеет искать в интернете рецепты, основываясь на имеющихся в наличии продуктах, следить за сроками их годности, регулировать температуру и самостоятельно выбирать один из энергосберегающих режимов. Всю необходимую информацию о состоянии холодильника и продуктов хозяин может получить через компьютер или портативное устройство с доступом в интернет.

Приложение № 9.2

КЛЮЧИ К УПРАЖНЕНИЮ «УМНЫЕ ВЕЩИ»

«Умное» одеяло. Состояние здоровья, режим дня, температурные предпочтения.

«Умные» кроссовки. Состояние здоровья, образ жизни, перемещения в пространстве.

«Умный» воздухоочиститель. Состояние здоровья, состояние жилища.

«Умный» холодильник. Информация о кулинарных пристрастиях хозяев.

«Умный» браслет. Состояние здоровья, образ жизни, режим дня, перемещения в пространстве, контакты.

Урок № 10

КАК УДАЛИТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ИЗ ИНТЕРНЕТА?

Цель: знакомство со способами удаления персональных данных из интернета.

Разминка «История Марио Гонсалеса»

Задача: сформировать у учащихся интерес к теме занятия и познакомить их с «правом на забвение» на примере реального случая.

Необходимые материалы: распечатка текста для ведущего (см. Приложение к уроку № 10.1).

Время проведения: 15 минут.

Процедура проведения

В начале урока ведущий озвучивает участникам тему занятия и в формате мини-лекции рассказывает им историю, положившую начало мировым дискуссиям о «праве на забвение» в интернете (см. Приложение к уроку № 10.1).

После этого участники переходят к обсуждению этого случая в формате беседы с ведущим.

Обсуждение

- Какими последствиями для Марио Гонсалеса обернулась его попытка удалить персональные данные из интернета?
- Стали бы вы на его месте обращаться в суд с требованием удалить информацию? Аргументируйте ответ.

- Пытались ли вы хотя бы однажды удалить какие-либо сведения о себе из интернета? Насколько это было трудно? Какие шаги вы для этого предприняли? Удалось ли достичь результата?

Упражнение «Право на забвение»

Задача: знакомство учащихся с категориями данных, подлежащих удалению из интернета, и возможными способами их удаления из сети.

Необходимые материалы: пять копий памятки «Как удалить персональные данные из интернета?» (см. Приложение к уроку № 10.2), карточки с историями (см. Приложение к уроку № 10.3).

Время проведения: 30 минут.

Процедура проведения

«Все мы можем столкнуться с ситуацией, когда кто-то без нашего согласия выложил информацию о нас в интернет. Такая информация, выставленная на всеобщее обозрение, может причинить нам ущерб и навредить нашей репутации. Конечно, можно обратиться с просьбой об удалении этой информации к человеку, разместившему наши данные в сети, или к администрации ресурса, на котором они были размещены. Однако администрация сайта обязана удалять только ту информацию, которая нарушает правила использования ресурса или законодательство РФ. В частности, удалению подлежат недостоверные данные, порочащие честь, достоинство или деловую репутацию пользователя (ГК РФ Ч. 1, Разд. I, Гл. 8, Ст. 152). Нужно понимать, что удаление данных из сети — серьезная юридическая процедура».

Ведущий предлагает группе выполнить следующее упражнение. Оно состоит из трех этапов.

Первый этап. Ведущий делит класс на три равные подгруппы, каждая из которых получает карточку с историей запроса на удаление данных и памятку «Как удалить персональные данные из сети?». Задача — внимательно изучив историю, представить себя на месте героя и принять решение: удаления какой информации они вправе требовать от администрации ресурса, на котором эти данные были размещены. Затем подгруппа должна написать аргументированное письмо администрации этого ресурса. На выполнение задания отводится около 10 минут.

Второй этап. Подгруппы обмениваются письмами, прилагая к ним карточки с историями. Теперь каждая подгруппа выступает в роли администратора ресурса, который должен принять решение, стоит ли удовлетворять поступивший запрос (и если да, то в каком объеме), учитывая интересы всех пользователей ресурса. Участники подгруппы должны написать письмо пользователю — герою истории — с аргументированным ответом: отказом или согласием на удаление данных. На выполнение этого задания отводится 10–15 минут.

Третий этап. Представители подгрупп по очереди зачитывают письмо, полученное от другой группы, историю, связанную с этим письмом, и затем озвучивают свой ответ. Авторы запроса должны ответить, согласны ли они с решением администрации сайта. В случае возникновения разногласий третья подгруппа, не участвующая в споре, может предложить свое решение проблемы. После того как все подгруппы выступят, можно переходить к обсуждению и подводить итоги упражнения.

Обсуждение

- В какой роли — пользователя или администратора сайта — сложнее принимать решение об удалении данных? Почему?
- Есть ли такие виды персональных данных, которые должны немедленно удаляться из сети? Аргументируйте ответ.
- Представьте, что однажды пользователи получат право удалять любую информацию из интернета по первому требованию. К каким последствиям это приведет?

Итоги занятия

Пословица «Что написано пером, не вырубишь топором» полностью оправдывает себя. Даже если нам удастся удалить первоисточник информации, она все равно сохранится в кэше десятков ресурсов, занимающихся сбором и индексацией данных в сети. Некоторые из этих ресурсов хранят информацию в кэше из технических соображений, например, чтобы ускорить работу поисковиков. Другие ресурсы собирают персональные данные с коммерческими целями. К сожалению, мошенники также занимаются сбором личной информации. Выкладывая свои данные в сеть, нужно помнить, что после этого удалить их полностью будет практически невозможно. Во всяком случае, потребуется много времени и усилий, чтобы полностью стереть «цифровой след».

Тем не менее в жизни бывают ситуации, когда персональные данные попадают в интернет не по нашей вине — например, их может выложить кто-то другой. В этом случае решение есть. В первую очередь необходимо обратиться к администратору ресурса с мотивированной просьбой об удалении этих данных.

Если наша просьба действительно обоснована, а удаление материала не затрагивает интересов других пользователей, то, скорее всего, нам пойдут навстречу. Если вы получите отрицательный ответ, не стоит сдаваться — нужно обратиться за помощью к взрослым, а они могут направить просьбу в вышестоящие инстанции.

Приложение № 10.1

ИСТОРИЯ МАРИО ГОНСАЛЕСА

С 2006 г. в мире активно обсуждается и внедряется идея «права на забвение», которая предполагает возможность стереть «клеймо прошлого» в интернете. Иными словами, удалить персональную информацию, «всплывающую» в сети. Это относится к устаревшим, неуместным, не соответствующим действительности, неполным или избыточным персональным данным.

«Право на забвение» было реализовано после судебного разбирательства в мае 2014 г.: Высший суд Евросоюза поддержал иск гражданина Испании Марио Гонсалеса, который обратился в Национальное агентство по защите данных с требованием удалить электронную версию статьи 1998 г. в архиве испанской газеты о продаже своего дома на аукционе в счет уплаты долга. Этот долг был погашен, и господин Гонсалес не хотел, чтобы компрометирующие его данные были доступны пользователям интернета. Первоначальная жалоба об удалении статьи на сайте газеты была отклонена, поскольку опубликованные сведения являлись достоверными. Однако в части требований по удалению ссылки на данный архив в поисковой выдаче суд пошел навстречу истцу. Он обязал Google удалить ссылку, поскольку Марио Гонсалес больше не является должником, следовательно, обладает «правом на забвение». Встречный иск компании-поисковика был передан в Верховный суд Испании, а затем в Европейский суд, но был отклонен. Суд обязал поисковик удалить все ссылки на испанском поддомене Google.es, содержащие имя Гонсалеса. В настоящий момент информация по-прежнему доступна на сайте газеты, но не показывается при поиске.

В мае 2014 г. компания Google разместила в интернете электронную форму, заполнив которую, европейские пользователи могут потребовать стереть свой «цифровой след» — информацию о себе в поисковиках. Уже в течение первых суток от европейских жителей поступило более 12 тысяч запросов на удаление информации о себе. Около половины из них касались наличия судимости. Первыми тремя обратившимися за «правом на забвение» были: бывший политик, который пожелал удалить ссылки на статьи о своем неподобающем поведении, мужчина, ранее осужденный за хранение запрещенных изображений, и доктор, чьи пациенты оставляли о нем негативные отзывы. Всего же за первый год действия Закона поступило более 240 тысяч запросов на удаление личной информации, из которых 40% были удовлетворены.

В июне 2014 г. Общественная палата РФ поддержала решение Европейского суда в отношении ограничения права доступа к персональной информации в сети, которая является не соответствующей действительности и/или устаревшей. В мае 2015 г. законопроект о «праве на забвение» был внесен на рассмотрение в Государственную думу РФ, а 13 июля 2015 г. соответствующий Федеральный Закон № 264 был подписан Президентом России. Он вступил в силу с 1 января 2016 г. Таким образом, история Марио Гонсалеса с продажей дома приобрела мировую известность и положила начало многочисленным дискуссиям о необходимости «права на забвения» для граждан разных стран мира. При этом информация, которую Гонсалес вначале собирался утаить, в итоге распространилась в масштабах всей планеты.

Приложение № 10.2

КАК УДАЛИТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ИЗ ИНТЕРНЕТА?

В первую очередь необходимо удалить личную информацию с ресурса-первоисточника, на котором она впервые была размещена. Для этого:

а) внимательно изучите условия и правила использования ресурса, уделив особое внимание разделам «Конфиденциальность» и «Безопасность». Многие крупные ресурсы, например социальные сети или поисковые системы, имеют автоматизированные системы приема жалоб от пользователей;

б) воспользуйтесь подобной системой, если она есть, в противном случае вам необходимо напрямую связаться с администрацией ресурса по электронной почте либо отправить заявление в печатной форме (заказное письмо с уведомлением о вручении);

в) письмо в администрацию ресурса должно быть написано в форме вежливой и хорошо аргументированной просьбы об удалении персональных данных;

г) письмо должно содержать: данные о заявителе (Ф.И.О., паспортные данные, контактную информацию — телефон и адрес электронной почты); ссылки на сайты и страницы, которые, по вашему мнению, должны исчезнуть из поисковых выдач (желательно приложить к письму скриншоты публикаций, содержащих информацию, которую вы имеете в виду); основание для прекращения выдачи этих ссылок (т.е. указание, что «не так» с этой информацией — недостоверна, неактуальна, незаконна) и подтверждение ваших

аргументов (факты, желательно подкрепленные ссылками на соответствующие законодательные акты); согласие на обработку персональных данных;

д) администрация ресурса должна рассмотреть вашу жалобу в течение десяти рабочих дней. Если поисковая служба сочтет, что предоставленная в заявлении информация является неполной, неточной и/или содержит юридические ошибки, вас могут попросить уточнить детали вашего заявления, а также документ, удостоверяющий личность. Вы должны ответить на данный запрос в течение десяти рабочих дней, после чего у поисковика есть еще две недели на принятие окончательного решения;

е) если вы получили от администрации ресурса мотивированный отказ в удалении информации, внимательно изучите его и попробуйте понять, что вы сделали неправильно. Возможно, эта информация действительно не подлежит удалению, и вам придется с этим смириться;

ж) если вы не получили ответа от администрации ресурса или на вашу просьбу ответили немотивированным отказом, не отчаивайтесь. Обращайтесь за помощью к взрослым, например к операторам ***Линии помощи «Дети Онлайн»*** *(8-800-25-000-15).* Существуют другие способы удаления информации из интернета.

Важно понимать, что процедура удаления информации из интернета может занять значительное время.

После того как персональные данные были удалены с сайта первоисточника, они все еще остаются в сети в кэше ресурсов, занимающихся сбором и индексацией информации в интернете: например, на сайтах-поисковиках, в социальных сетях, на сайтах, занимающихся сбором информации в маркетинговых целях и т.д.

В случае с поисковыми системами информация в кэше регулярно обновляется, поэтому устаревшие сведения со временем перестанут появляться при поиске. Обычно это занимает много времени, поэтому нужно запастись терпением.

Если возникла необходимость экстренного удаления персональных данных из поисковой выдачи, можно обратиться напрямую в службу технической поддержки сайта — внимательно изучить правила удаления информации и оформить заявку.

Необходимо понимать: если информация попала в сеть, то *удалить ее со стопроцентной гарантией уже не получится*. Определить все ресурсы, на которых остались следы ваших персональных данных, практически невозможно. Поэтому прежде чем выкладывать свои персональные данные в интернет, хорошенько подумайте: к чему это может привести?

Какая информация может быть удалена из интернета?

Принимая решение об удалении информации, администрация ресурса руководствуется целым рядом соображений:

- информация, размещенная на сайте, *не должна нарушать законодательство РФ*, а значит, удалить противозаконный контент будет достаточно легко. Важно точно разобраться, какой контент противозаконен, и сослаться на соответствующие законодательные акты*;
- информация, размещенная на сайте, *не должна нарушать правила использования ресурса и пользовательское соглашение*. Ознакомиться с ними можно на самом ресурсе в соответствующем разделе. Как правило, ответственные

* Ознакомиться с законодательными актами, регулирующими обращение информации в интернете, можно на сайте Роскомнадзора. URL: http://eais.rkn.gov.ru/.

ресурсы указывают список видов информации, подлежащих удалению, например, номер паспорта, кредитной карты и т.д.;

- еще одна категория данных, подлежащих удалению, — *недостоверные данные, порочащие честь, достоинство или деловую репутацию пользователя* (ГК РФ, Ч. 4, Разд. I, Гл. 8, Ст. 152). Однако в этом случае пользователю придется доказать в суде, что информация действительно является недостоверной и порочащей его честь. Некоторые ресурсы могут пойти вам навстречу и удалить данные без постановления суда, но только при условии, что это никак не ущемит права других пользователей ресурса.

Администрация ресурса также обязана по вашему требованию удалить персональные данные, размещенные на сайте без вашего согласия. В этом случае полезным будет вспомнить, что такое персональные данные. Следует иметь в виду, что, подписывая пользовательское соглашение об использовании социальных сетей, мы автоматически даем согласие на использование и обработку наших данных. По закону его можно отозвать, написав соответствующее заявление в администрацию ресурса, однако это повлечет за собой автоматическое закрытие аккаунта.

Администрация ресурса обязана удалять контент, распространяемый без согласия его автора. Размещая в интернете созданные вами произведения литературы, фотографии, видео- и аудиозаписи, позаботьтесь о защите своих авторских прав, указав рядом с произведением знак копирайта — ©, ваши Ф.И.О., а также год публикации. Только в этом случае вам удастся защитить свои права.

Приложение № 10.3

КАРТОЧКИ С ИСТОРИЯМИ

Карточка № 1

Сводные сестры Золушки не могут выйти замуж

После того как Золушка вышла замуж за Принца, а в интернете была опубликована их счастливая семейная история, ее мачехе и сводным сестрам житья не стало. Никто не хочет с ними знакомиться и дружить: прочитав заметку, все считают их несправедливыми и злыми.

С первого дня мачеха возненавидела свою падчерицу. Она заставляла ее делать всю работу по дому и не давала ни минуты покоя. То и дело слышалось: «А ну, пошевеливайся, лентяйка, принеси-ка воды! Давай, бездельница, подмети пол! Ну, чего ждешь, грязнуля, подкинь дров в камин!». От грязной работы девочка и в самом деле всегда была выпачкана в золе и пыли. Сводные сестры Золушки не отличались характером от своей злой и ворчливой матери. Завидуя красоте девушки, они заставляли ее прислуживать им и все время придирались к ней.

Несмотря на то, что сестры попросили прощения у Золушки, о чем также говорится в истории, их репутация оказалась серьезно испорчена.

...Примерили туфельку и — о, чудо! туфелька пришлась впору. Тут сестры и мачеха поняли, кто была та неизвестная красавица на балу. Они бросились к ней просить прощения. Золушка была не только хороша собой, но и добра: она простила их от всего сердца.

Помогите сводным сестрам Золушки составить письмо в адрес администрации новостного портала с просьбой удалить информацию, порочащую их честь и достоинство.

Карточка № 2

Медведь сел на теремок и не может снять квартиру

После неудачного заселения в теремок медведь опубликовал в интернете объявление о том, что ему срочно нужно новое жилье — он хочет снять просторную квартиру в городе. Однако арендодатели очень переживают за свои дома и не откликаются на его заявку из-за громкого «скандала с теремком», который разгорелся после записи в новостной ленте.

Медведь и полез в теремок. Лез-лез, лез-лез — никак не мог влезть — и говорит:

— А я лучше у вас на крыше буду жить.

— Да ты нас раздавишь!

— Нет, не раздавлю.

— Ну так полезай!

Влез медведь на крышу и только уселся — бах! — затрещал теремок, упал набок и весь развалился.

Медведь утверждает, что он не причинил никому вреда: теремок все равно был ветхий и тесный, а на его месте сразу же возникла элитная новостройка.

Еле-еле успели из него выскочить мышка-норушка, лягушка-квакушка, зайчик-побегайчик, лисичка-сестричка, волчок-серый бочок — все целы и невредимы. Отстроили теремок новый, еще лучше старого!

Помогите медведю составить письмо в адрес администрации новостного портала с просьбой удалить информацию, порочащую его честь и достоинство.

Карточка № 3

Баба-яга не может устроиться на работу в детский сад, потому что ее обвиняют в жестоком обращении с детьми

Баба-яга уже давно живет одна. Ей скучно в лесу, и поэтому она решила устроиться на работу в детский сад — ведь у нее многолетний опыт работы с детьми. Однако в новостной ленте написали страшную историю о том, что она чуть не съела маленькую девочку, и теперь никто не хочет брать ее на работу.

Вот девочка села у окна и стала ткать. А Баба-яга вышла из избушки и говорит своей работнице: «Я сейчас спать лягу, а ты ступай истопи баню и вымой племянницу. Да смотри, хорошенько вымой: проснусь — съем ее!». Девочка услыхала эти слова — сидит ни жива, ни мертва.

Баба-яга недоумевает: ее методы воспитания давно признаны эффективными, к тому же с племянницей она всегда обращалась ласково и приветливо.

Работница баню топит, а Баба-яга проснулась, подошла к окошку и спрашивает: «Ткешь ли ты, племяннушка, ткешь ли, милая?» — «Тку, тетушка, тку, милая!».

Она обратилась в суд с требованием удалить данную информацию, считая подобные заметки в интернете оскорбительными. Помогите Бабе-яге составить письмо в адрес администрации новостного портала с просьбой удалить информацию, порочащую ее деловую репутацию.

ОБРАЗОВАТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

В результате освоения программы у учащихся должны быть сформированы способность и готовность самостоятельно в соответствии с актуальными жизненными задачами защищать персональные данные с помощью технических и программных приемов и средств, устанавливать границы собственной приватности и управлять репутацией в сети.

Учащиеся должны знать о видах персональных данных, последствиях их небрежного использования, способах их попадания в интернет и дальнейшего распространения в сети; уметь пользоваться следующими средствами управления персональными данными и приватностью в интернете:

- методы защиты конфиденциальных персональных данных от несанкционированного доступа;
- специальные безопасные режимы работы в браузерах;
- приемы, позволяющие контролировать распространение персональных данных в интернете, а также удалять следы онлайн-активности с различных устройств и онлайн-ресурсов;
- настройки приватности в социальных сетях и на других онлайн-ресурсах;
- обращение в службу технической поддержки разработчиков устройств, приложений, онлайн-ресурсов; в общественные и государственные организации.

ОЦЕНКА УРОВНЯ ЦИФРОВОЙ ГРАМОТНОСТИ ПО УПРАВЛЕНИЮ ПЕРСОНАЛЬНЫМИ ДАННЫМИ В ИНТЕРНЕТЕ

Данный тест направлен на оценку уровня цифровой грамотности школьников в сфере управления персональными данными в интернете и может быть использован для оценки эффективности освоения программы учащимися. Методика представляет собой набор из 20 тестовых заданий с одним верным вариантом ответа. На выполнение теста отводится 30–40 минут.

Инструкция

Вам будет предложено 20 заданий, касающихся вопросов безопасности обращения с персональными данными в интернете. Среди вариантов ответа есть *только один* правильный. Ваша задача — выбрать и отметить тот вариант, который вы считаете верным. На выполнение всего теста отводится не более 40 минут.

1. **Какая информация может быть отнесена к персональным данным?**

   A. Фамилия, имя, отчество.

   B. Дата и место рождения.

   C. Место учебы.

   D. Политические и религиозные убеждения.

   E. Все предложенные варианты.

2. Какие из приведенных персональных данных позволяют однозначно идентифицировать пользователя в нашей стране?

A. Имя, фамилия, год рождения.

B. Фамилия, год рождения, номер школы.

C. Имя, номер паспорта РФ, город проживания.

D. Имя, фамилия, город проживания.

E. Ни один из предложенных вариантов.

3. Этим летом Маша Иванова вместе с классом ездила в Царское Село. В конце экскурсии классный руководитель сделал групповую фотографию класса на фоне Екатерининского дворца. Фотография получилась удачной, поэтому учитель поместил ее на своей странице в социальной сети с подписью «9 “Б” в Царском Селе» и отметил на ней несколько человек, включая Машу. Какая информация о Маше Ивановой содержится в этой записи?

A. Внешние данные.

B. Место учебы.

C. Место проведения экскурсии.

D. Имена одноклассников Маши Ивановой.

E. Все предложенные варианты.

4. На выходных Вася гостил у своего друга Пети. Пару раз он воспользовался компьютером друга, чтобы оформить покупку новой компьютерной игры в интернет-магазине и почитать новости. Какая персональная информация Васи могла сохраниться на Петином компьютере?

A. История поисковых запросов.

B. История посещений сайтов.

C. Личная переписка в социальной сети.

D. Скачанные файлы.

E. Ни один из предложенных вариантов.

5. Ксюша, находясь в кафе с подругой Светой, воспользовалась ее ноутбуком для входа в браузер. Что нужно сделать Ксюше, чтобы оставить минимум личной информации на Светином ноутбуке?

A. Очистить журнал посещений после выхода из браузера.

B. Не сохранять пароли во время работы в сети.

C. Использовать режим инкогнито во время работы в браузере.

D. Сменить пользователя на ноутбуке.

E. Очистить папку временных файлов после работы за компьютером.

6. Таня познакомилась с Колей на портале популярной онлайн-игры Lineage. Долгое время они играли за одну команду и не раз выручали друг друга в виртуальных боях. Как-то раз Таня собралась в очередной рейд, но в последний момент узнала о контрольной работе по геометрии и поняла, что не сможет принять участие в сражении. Коля предложил Тане дать пароль от ее аккаунта Колиному другу, который бы мог заменить ее на время в игре. Как лучше всего поступить Тане в такой ситуации?

A. Коля поручился за своего друга, поэтому можно спокойно передать ему пароль.

B. Нет ничего страшного в том, чтобы сообщить пароль другому игроку — это всего лишь игра.

C. Колиному другу можно передать пароль — даже если он украдет аккаунт, его можно будет восстановить.

D. Следует отказаться от Колиного предложения, поскольку пользовательское соглашение запрещает игрокам передавать пароль третьим лицам.

E. Тане нужно собрать максимум информации о Колином друге, а потом принять окончательное решение.

7. При регистрации на сайте у вас запросили номер телефона. В каком случае это наиболее безопасно?

A. Вы регистрируетесь на крупном и хорошо известном онлайн-ресурсе, например, на портале Mail.ru.

B. Вы первый раз совершаете покупку в интернет-магазине, на сайте которого размещены положительные отзывы других пользователей.

C. Вы регистрируетесь на игровом портале, который порекомендовали вам ваши друзья и знакомые.

D. Вы хотите скачать новый фильм на файлообменнике, и от вас требуется регистрация во всплывающем окне.

E. Во всех обозначенных выше случаях.

8. Какой из приведенных паролей можно считать самым надежным?

A. SupermanVasya2005.

B. QwErTy123456.

C. A!z8@;).

D. Q1jk45)@da.

E. M@$h@2oo!

9. Какой из способов хранения пароля от аккаунта можно считать самым надежным?

A. В записной книжке в нижнем ящике письменного стола.

B. В текстовом файле в скрытой папке на компьютере.

C. В специальной программе, бесплатно скачанной в интернете.

D. Все перечисленные выше способы можно считать полностью надежными.

E. Все перечисленные выше способы считать полностью надежными нельзя.

10. Однажды вечером Аня обнаружила, что кто-то взломал ее аккаунт, разместил на ее стене неприличные изображения и стал рассылать оскорбления ее друзьям в личной переписке. Аня восстановила доступ к аккаунту и поменяла пароль, но было поздно. Многие удалили ее из друзей и добавили в «черный список», а кто-то даже перестал разговаривать в школе. Что следует сделать Ане для того чтобы восстановить свою репутацию?

A. Удалить все неприятные сообщения со своей страницы.

B. Разместить на странице пост, разъясняющий причины произошедшего, и извиниться перед читателями.

C. Сменить пароли ко всем аккаунтам на других онлайн-ресурсах.

D. Постараться лично поговорить с самыми близкими друзьями и объяснить им ситуацию.

E. Все вышеперечисленные варианты.

11. В социальной сети Вове пришло личное сообщение, в котором сообщалось о попытке взлома его аккаунта с чужого устройства. Вове настоятельно рекомендовалось пройти по ссылке, указанной в сообщении, для смены пароля. Как правильно поступить в такой ситуации?

A. Пройти по ссылке, указанной в письме, и сменить пароль.

B. Проигнорировать письмо и добавить его в спам.

C. Написать в ответ гневное письмо с критикой работы социальной сети.

D. Самостоятельно зайти в свой аккаунт социальной сети и сменить пароль.

E. Ответить на это письмо и уточнить информацию.

12. Мила решила начать вести здоровый образ жизни. Она скачала на смартфон фитнес-трекер, который позволяет регистрировать пройденное расстояние и количество калорий, потраченных во время занятий спортом. Приложение было бесплатным, но требовало обязательного доступа к определенному набору персональных данных и функций смартфона. Какое из этих требований можно считать чрезмерным?

A. Доступ к фотокамере и медиафайлам, хранящимся на устройстве.

B. Информация о местонахождении и перемещении.

C. Возможность совершать покупки внутри приложения.

D. Пол, возраст, вес, рост.

E. Все перечисленные требования разумны.

13. Какая персональная информация, размещенная на онлайн-ресурсе, должна быть удалена из поисковой системы по запросу пользователя?

A. Любое групповое фото, на котором есть изображение данного пользователя.

B. Перепост пользовательского поста, размещенного в открытом доступе на странице данного пользователя в социальной сети.

C. Номер паспорта или любого другого официального документа пользователя.

D. Никакая персональная информация о пользователе не подлежит обязательному удалению.

E. Любая персональная информация должна быть удалена из интернета по запросу пользователя.

14. Как поступить, если злоумышленники взломали ваш аккаунт на онлайн-ресурсе и поменяли пароль и адрес почтового ящика, к которому был привязан аккаунт?

A. Не стоит тратить силы на восстановление аккаунта — всегда можно завести новый.

B. Обратиться к администрации ресурса с просьбой восстановить вам доступ к аккаунту.

C. Обратиться к злоумышленникам с просьбой вернуть аккаунт.

D. Обратиться к знакомому хакеру с просьбой взломать ваш аккаунт еще раз и вернуть его законному владельцу.

E. Это безвыходная ситуация — потерянный аккаунт в принципе невозможно вернуть.

15. Влад — Наташин сосед по парте и очень любопытный юноша. Какое из действий Влада будет являться нарушением Наташиной приватности?

A. Рассказал одноклассникам о том, что у Наташи аллергия на сладкое.

B. Сфотографировал спящую на парте Наташу и выложил это фото в социальную сеть.

C. Взял с парты Наташин смартфон и посмотрел историю звонков.

D. Прочел вслух записку, которую Наташа написала перед уроком Ване.

E. Все вышеперечисленные варианты.

16. Какие виды Наташиных персональных данных Влад может распространять с полной уверенностью в том, что это никак ей не навредит?

A. Номер телефона, Ф.И.О. родителей, домашний адрес.

B. Страна проживания, номер школы, информация о перенесенных заболеваниях.

C. Хобби, номер и адрес школы, логин от страницы в социальной сети.

D. Возраст, рост и вес, оценки в журнале.

E. Никакие из перечисленных видов данных.

17. Какое из утверждений является полностью верным?

A. Каждому человеку необходимо защищать свою персональную информацию и сохранять как можно больше сведений о себе в тайне от других людей.

B. Каждый человек может самостоятельно решать, какая информация и при каких условиях может быть сохранена в секрете или передана другим людям.

C. Бесполезно контролировать свои персональные данные в интернете, поэтому нет смысла об этом беспокоиться.

D. Каждому человеку следует предоставлять как можно больше сведений о себе, поскольку это позволяет пользоваться всеми возможностями интернета.

E. Ни один из перечисленных вариантов.

18. Оля рассталась с Васей и теперь встречается с Антоном. Они часто гуляют, делают совместные фотографии и выкладывают их в сеть. Оля по-прежнему хорошо относится к Васе, но не хочет расстраивать его фотографиями с новым молодым человеком. Как ей лучше поступить?

A. Ограничить для Васи доступ к своим фотографиям.

B. Прекратить выкладывать свои фотографии в социальную сеть.

C. Попросить Васю не заходить на ее страницу.

D. Удалить Васю из друзей.

E. Внести Васю в «черный список».

19. Выберите верное утверждение. Авторские посты, размещаемые пользователями в социальных сетях и блогах...

A. Показывают уникальность человека и всегда позитивно влияют на его репутацию.

B. Никогда не содержат персональной информации, поэтому их публикация не влечет за собой серьезных последствий.

C. Оцениваются читателями по-разному, поэтому невозможно предсказать, как публикация поста отразится на репутации его автора.

D. Всегда содержат излишнюю персональную информацию о человеке, что может навредить не только его репутации, но и личной безопасности.

E. Не содержат ничего хорошего, поскольку свидетельствуют исключительно о желании похвастаться.

20. Каких правил НЕ стоит придерживаться, публикуя информацию в интернете?

A. Писать посты, руководствуясь первым эмоциональным порывом, — с целью донести до читателя бурю своих эмоций.

B. Публиковать сведения и комментарии о важных фактах и событиях только после их проверки в нескольких источниках.

C. Выкладывать в сеть данные о другом человеке только в том случае, если он дал на это свое предварительное согласие.

D. Оценивать публикуемую информацию с точки зрения различных категорий пользователей.

E. Все вышеперечисленные правила верны.

Правильные ответы

1 — E, 2 — C, 3 — E, 4 — B, 5 — C, 6 — D, 7 — A, 8 — D, 9 — E, 10 — E, 11 — D, 12 — A, 13 — C, 14 — B, 15 — E, 16 — E, 17 — B, 18 — A, 19 — C, 20 — A.

Уровень освоения программы оценивается в соответствии со следующей таблицей:

Количество правильных ответов	**Примерная оценка по пятибалльной шкале**
17–20	Отлично
14–16	Хорошо
10–13	Удовлетворительно
Менее 10	Неудовлетворительно

ГЛОССАРИЙ

Автосинхрониза́ция — автоматический процесс приведения данных, которые содержатся на нескольких устройствах, к одинаковому состоянию. Такой процесс может быть как односторонним, так и двусторонним. Во втором случае данные копируются в двух направлениях одновременно. Иными словами, если мы изменили файлы в одном месте, эти изменения будут применимы и к другому месту, и наоборот. Каждый раз, когда происходит автосинхронизация, к примеру, между ПК и мобильным устройством, происходит сравнение данных между собой и выявление их идентичности. Если они различаются, осуществляется автоматическое обновление.

Акка́унт, учетная запись (англ. account) — хранимая в компьютерной системе совокупность данных о пользователе, необходимых для его опознавания (аутентификации) и предоставления доступа к его личным данным и настройкам.

Аутентифика́ция (англ. authentification; от греческого αὐθεντικός [authentikos] — «реальный, подлинный», от αὐθέντης [authentes] — «автор») — процедура проверки подлинности. Может представлять собой проверку подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных пользователей; подтверждение подлинности электронного письма путем проверки цифровой подписи письма и др.

Бра́узер или веб-обозрева́тель (англ. web browser, устар. бро́узер) — прикладное программное обеспечение для просмотра веб-страниц, содержания веб-документов, компьютерных файлов и их каталогов, управления веб-приложениями, а также для решения других задач. В глобальной сети браузеры используются для запроса, обработки, манипулирования и отображения содержания веб-сайтов.

Ватса́п, вотса́п, васса́п (англ. WhatsApp, игра слов от What's Up — «Что происходит?») — бесплатный частный коммерческий мессенджер для смартфонов. Позволяет пересылать текстовые сообщения, изображения, видео- и аудиофайлы через интернет.

Видеохо́стинг — сайт, позволяющий загружать и просматривать видео в браузере, например через специальный проигрыватель.

Википе́дия (англ. Wikipedia) — свободная, общедоступная, мультиязычная, универсальная интернет-энциклопедия, реализованная на принципах ви́ки (веб-сайт, структуру и содержимое которого пользователи могут самостоятельно изменять с помощью инструментов, предоставляемых самим сайтом; форматирование текста и вставка различных объектов в текст производится с использованием специальной вики-разметки). Википедия расположена по адресу: *http://www.wikipedia.org/*.

Вики-проект — веб-сайт, работающий на технологии вики (использующий вики-движок), который развивается за счет коллективного труда сообщества авторов, как правило, неоплачиваемого и добровольного. Вики-проект позволяет

создание неограниченного числа веб-страниц и последующее их редактирование другими пользователями.

Вики-среда́ (соединение слов *wiki* и *среда*) — совокупность вики-проектов, их содержания, участников и технической основы. В широком смысле вики-средой можно назвать все вещи, связанные с технологией вики, в узком — все, связанное с Википедией.

Виртуа́льная реа́льность, искусственная реальность, электронная реальность, компьютерная модель реальности (англ. virtual reality, VR) — созданный техническими средствами мир (объекты и субъекты), передаваемый человеку через его ощущения: зрение, слух, обоняние, осязание и др. Виртуальная реальность имитирует как воздействие, так и реакции на воздействие. Для создания убедительного комплекса ощущений реальности компьютерный синтез свойств и реакций виртуальной реальности производится в реальном времени.

Геолока́ция (англ. geolocation) — определение реального географического местоположения электронного устройства, например, радиопередатчика, сотового телефона или компьютера, подключенного к интернету. Словом «геолокация» может называться как процесс определения местоположения такого объекта, так и само местоположение, установленное таким способом. Часто для целей геолокации используется та или иная система позиционирования, и бывает важнее определить местоположение в виде, легко воспринимаемом человеком (например, почтовый адрес), нежели точные географические координаты.

Еди́ный ре́естр доме́нных име́н, указателей страниц сайтов в сети «интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «интернет», содержащие информацию, распространение которой в Российской Федерации запрещено — автоматизированная информационная система ведения и использования базы данных о сайтах, содержащих запрещенную к распространению в России информацию. Реестр находится в ведении Роскомнадзора в соответствии с постановлением Правительства Российской Федерации от 26 октября 2012 года № 1101 «О единой автоматизированной информационной системе Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "интернет", содержащие информацию, распространение которой в Российской Федерации запрещено».

Идентифика́тор — имя, под которым зарегистрирован пользователь в проверяющей его компьютерной системе.

Инстагра́м (англ. Instagram) — бесплатное приложение для обмена фотографиями и видеозаписями с элементами социальной сети, позволяющее снимать фотографии и видео, применять к ним фильтры, а также распространять их через свой сервис и ряд других социальных сетей.

Инфо́рмер (англ. informer — «осведомитель, доносчик») — автоматически обновляющийся специальный блок, который устанавливается на сайте пользователя для предоставления посетителям дополнительной оперативной информации в какой-либо области.

Кейло́геры (англ. keyloggers) — специальные программы и устройства, позволяющие регистрировать нажатие клавиш на клавиатуре компьютера.

Кибербу́ллинг (англ. cyberbulling) — намеренное и регулярное причинение вреда (запугивание, унижение, травля, физический или психологический террор) одним человеком или группой людей другому человеку с использованием электронных форм контакта.

Комментáрии (см. также — пост) — не существуют отдельно от записей (поста или темы для обсуждения). Главная задача комментария — дать возможность развернуто оценить запись, уточнить непонятные моменты или выразить несогласие с автором. В отдельных случаях комментарии могут нести бóльшую ценность, чем сама запись (пост). Обычно комментариями являются собственные мысли, реже — цитаты из каких-либо источников или изображения. Комментарии зачастую носят характер предположения или личного оценочного суждения и не являются точными сведениями.

Конфиденциáльность (англ. confidence — «доверие») — **1.** Необходимость предотвращения утечки (разглашения) какой-либо информации. **2.** Обязательное для выполнения лицом, получившим доступ к определенным сведениям (сообщениям, данным) независимо от формы их представления, требование не передавать их третьим лицам без согласия лица, самостоятельно создавшего информацию либо получившего на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (Федеральный закон от 27.07.2006

№ 149-ФЗ «Об информации, информационных технологиях и о защите информации»). Полный перечень сведений конфиденциального характера см. в Указе Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями и дополнениями от 23.09.2005, 13.07.2015). В англо-американской традиции различают два основных вида конфиденциальности: добровольную (*privacy*) и принудительную (*secrecy*)*. В первом случае имеются в виду прерогативы личности, во втором — информация для служебного пользования, доступная ограниченному кругу официальных лиц фирмы, корпорации, государственного органа, общественной или политической организации. Хотя *privacy* и *secrecy* схожи по значению, на практике они обычно противоречат друг другу: усиление *secrecy* ведет к нарушению и уменьшению *privacy*.

Кэш (англ. cache; фр. cacher — «прятать») — **1.** Промежуточный буфер с быстрым доступом, содержащий ту информацию, которая будет запрошена с наибольшей долей вероятности. Доступ к данным в кэше осуществляется быстрее, чем выборка исходных данных из более медленной памяти или удаленного источника, однако их объем существенно ограничен по сравнению с хранилищем исходных данных. **2.** Кэширование интернет-страниц — процесс сохранения часто запрашиваемых документов на (промежуточных) прокси-серверах или электронном устройстве пользователя с целью предотвращения их постоянной загрузки с сервера-источника и уменьшения трафика.

---

* Подробнее: *Shils E.* The Torment of Secrecy: The Background & Consequences Of American Security Policies. — Chicago, 1956.

Логи́н (англ. login; login name; username; user — «пользователь») — имя (идентификатор) учетной записи пользователя в компьютерной системе.

Ме́ссенджер, система обмена мгновенными сообщениями (англ. instant messaging, IM) — службы мгновенных сообщений, программы-онлайн-консультанты (OnlineSaler) и программы-клиенты для обмена сообщениями в реальном времени через интернет. Могут передавать текстовые сообщения, звуковые файлы, изображения, видео, а также производить такие действия, как совместное рисование или игры. Многие из таких программ-клиентов могут применяться для организации групповых текстовых чатов или видеоконференций.

Настро́йки прива́тности — система специальных параметров, позволяющих пользователю онлайн-ресурса настраивать уровень внешнего доступа к различным видам персональной информации.

Неприкоснове́нность ча́стной жи́зни (в юридической науке) — ценность, обеспечиваемая правом на неприкосновенность частной жизни и включающая: запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия; право контролировать информацию о себе; право на защиту чести и доброго имени; право на защиту персональных данных; право на тайну связи (иногда оформлено как отдельное право); право на неприкосновенность жилища (иногда оформлено как отдельное право); врачебную тайну, тайну усыновления, тайну исповеди и другие виды профессиональной тайны. В России неприкосновенность частной жизни про-

возглашается ст. 23, 24 Конституции РФ. К нормативным актам, регулирующим защиту права на неприкосновенность частной жизни, также относятся Федеральный закон «О персональных данных», Гражданский кодекс, а также ряд международных договоров: Всеобщая декларация прав человека, Европейская конвенция о защите прав человека и основных свобод, Международный пакт о гражданских и политических правах. Неприкосновенность частной жизни поставлена под охрану ст. 137 Уголовного кодекса Российской Федерации («Неприкосновенность частной жизни»).

Опера́тор персона́льных да́нных — государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и/или осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Па́блик, публичная страница (англ. public) — сообщество в социальной сети, в которое могут вступить зарегистрированные в ней пользователи. В отличие от группы в социальной сети, в пабликах отсутствует возможность создания тем и общения участников между собой. Как правило, паблики используются в коммерческих целях рекламы компании, продукции; прямых продаж; заработка на рекламе; развлечения; привлечения на внешние сайты.

Паро́ль (фр. parole — «слово») — условное слово или набор знаков, предназначенный для подтверждения личности или полномочий. Пароли часто используются для защиты информации от несанкционированного доступа. В большинстве вычислительных систем комбинация «имя пользователя — пароль» используется для идентификации пользователя.

Персона́льные да́нные (согласно Федеральному Закону РФ № 152) — любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу — субъекту персональных данных (ст. 3 Федерального закона РФ от 27.07.2006 № 152).

Пин-код (англ. Personal Identification Number — «личный опознавательный номер») — аналог пароля (см. Пароль). В ходе авторизации операции используется одновременно как пароль доступа держателя карты к терминалу (банкомату) и как секретный ключ для цифровой подписи запроса. PIN-код предусматривается для кредитных и других карт (например, сим-карт); с его помощью производится авторизация держателя карты. PIN-код должен знать только держатель карты. Обычно предусмотрено ограничение попыток правильного ввода (в основном не больше 3 раз), после чего карта блокируется для использования.

Поиско́вый запро́с — последовательность символов, которую пользователь вводит в поисковую строку, чтобы найти интересующую его информацию. Формат поискового запроса зависит как от устройства поисковой системы, так и от типа информации для поиска. Чаще всего поисковый запрос задается в виде набора слов или фразы. Но бывают и совсем иные виды запросов. Так, при поиске изображений по содержанию запросом может являться изображение, а результатом поиска — страницы в интернете, на которых это изображение встречается (*reverse image search*). Существует несколько категорий запросов: *информационные* — когда пользователь хочет найти информацию (например, Колорадо или грузовые автомобили); *навигационные* — когда пользователь хочет найти определенный

сайт или компанию (например, ВКонтакте или Аэрофлот); *транзакционные* — когда пользователь хочет совершить определенное действие (например, купить автомобиль или установить Windows).

Пост (англ. post) — запись, отдельное сообщение на веб-форуме. Для того чтобы оставить («опубликовать») сообщение на веб-форуме, необходимо заполнить соответствующую форму на сайте. В сообщениях на веб-форумах, кроме содержания, обычно указывается имя автора (ник), дата и некоторые другие данные, относящиеся к сообщению или автору.

Пра́во на забве́ние (англ. right to be forgotten — «право быть забытым») — право ограничивать доступ к неприятной или устаревшей информации о себе в глобальной сети. В настоящее время в России информация удаляется не поисковыми системами, а самими операторами персональных данных по требованию Роскомнадзора.

Прива́тность (англ. privacy — «уединение», «уединенность») — **1.** Право человека на личное пространство, свободное от вмешательства других людей и организаций (*Clarke*, 1996). Выделяется 4 типа: физическая; личности, или поведенческая; персональной коммуникации, или коммуникационная; персональной информации, или информационная. **2.** Регуляторный динамический процесс, детерминирующий и непрерывно корректирующий границы личности с точки зрения ее взаимоотношений с окружающим миром (*Altman*, 1975). **3.** Право индивида решать, насколько быть открытым или закрытым по отношению к внешнему миру, какая информация и при каких условиях может быть сохранена как тайна или, наоборот, передана другим людям (*Westin*, 1967).

Сет (англ. set — «комплект») — комплект предметов экипировки игрового персонажа. Как правило, в сет может входить от двух до шести предметов обмундирования (шлем, перчатки, ботинки, штаны и т.д.), при одновременном использовании которых персонаж получает дополнительный игровой бонус (неуязвимость и пр.).

Скайп (англ. Skype) — бесплатное программное обеспечение с закрытым кодом, обеспечивающее текстовую, голосовую и видеосвязь через интернет между компьютерами (IP-телефония) и опционально использующее платные услуги для звонков на мобильные и стационарные телефоны.

Смартфо́н (англ. smartphone — «умный телефон») — мобильный телефон, дополненный функциональностью карманного персонального компьютера.

Сни́мок экра́на, скриншот, скрин (англ. screenshot) — изображение, полученное устройством и показывающее в точности то, что видит пользователь на экране монитора или другого визуального устройства вывода. Обычно это цифровое изображение получается операционной системой или другой программой по команде пользователя. Намного реже снимки экрана получают с помощью внешнего устройства, такого как фото/видеокамера, или путем перехвата видеосигнала от компьютера к монитору.

Спам (англ. spam) — **1.** Рассылка коммерческой и иной рекламы или подобных коммерческих видов сообщений лицам, не выражавшим желания их получать. **2.** Название распространяемых материалов. Распространителей спама называют спамерами.

Та́мблер (англ. Tumblr) — сервис микроблогов, включающий в себя множество картинок, статей, видео- и gif-изображений по разным тематикам и позволяющий пользователям публиковать посты в их тамблелог (англ. tumblelog). Пользователь может подписываться (англ. follow — «следовать») на блоги других пользователей, после чего их записи будут появляться на его ленте новостей (англ. dashboard — «приборная панель»). Сервис характеризует себя как «простейший способ вести блог» (англ. The easiest way to blog).

Тви́ттер (англ. to twit — «чирикать, щебетать, болтать») — социальная сеть для публикации коротких (до 140 символов) сообщений при помощи веб-интерфейса, SMS, средств мгновенного обмена сообщениями или сторонних программ-клиентов для пользователей интернета любого возраста.

Трансграни́чная переда́ча персона́льных да́нных — передача персональных данных оператором через государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Тре́керы (англ. track — «след, отслеживание») — общее название устройств и программ, с помощью которых можно отследить разные показатели организма, например пульс, правильность осанки, качество питания, ритмы сна и т.д.

Фи́тнес-тре́кер (см. Трекеры) — браслет или клипса со встроенным датчиком, способные отслеживать множество факторов, касающихся здоровья и тренировок: продолжительность и качество сна (функция «умный будильник»), количество

пройденных шагов, качество питания, показатели пульса, сожженные калории, настроение, уровень насыщения крови кислородом, калорийность поступающей в организм пищи (как инновационная разработка — трекер «HealBe GoBe»).

Фи́шинг (англ. phishing, от fishing — «рыбная ловля, выуживание») — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне не отличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определенному сайту, что позволяет мошенникам получить доступ к его аккаунтам и банковским счетам. Фишинг — одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности (в частности, многие не знают о том, что сервисы не рассылают писем с просьбами сообщить свои учетные данные, пароль и прочее).

Форскво́р (англ. foursquare — «квадрат, квадратный») — социальная сеть с функцией геопозиционирования, предназначенная, в основном, для работы с мобильными устройствами. Данный сервис доступен пользователям не только с устройствами, которые оборудованы GPS-навигацией, например, пользователям смартфонов, но и просто для работы с любым

сотовым телефоном. Пользователи отмечаются в различных заведениях с помощью мобильной версии веб-сайта, SMS-сообщения или же специального приложения, разработанного под определенную операционную систему мобильного устройства. Каждая такая отметка позволяет пользователю зарабатывать foursquare-баллы, а в некоторых случаях — и «бейджи».

Цифрова́я компете́нтность — основанная на непрерывном овладении системой соответствующих знаний, умений, мотивации и ответственности способность индивида уверенно, эффективно, критично и безопасно выбирать и применять инфокоммуникационные технологии в разных сферах жизнедеятельности (работа с контентом, коммуникации, потребление, техносфера), а также его готовность к такой деятельности.

Цифрово́й след, цифрово́й отпеча́ток — вся совокупность персональной информации о пользователе, которая хранится в интернете.

Че́рный спи́сок — 1. Функция, предусматривающая возможность блокировки активности пользователя на онлайн-ресурсе в целях пресечения поведения, запрещенного правилами сервиса, публикации запрещенного контента, спама и вирусов. **2.** Функция в социальной сети, позволяющая заблокировать недоброжелателям доступ к профилю пользователя в целях его защиты от нежелательного общения, рекламных рассылок и спама.

Электро́нная по́дпись (ЭП), электро́нная цифрова́я по́дпись (ЭЦП) — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позво-

ляющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки — подтвердить факт подписания электронного документа (неотказуемость).

ЛИТЕРАТУРА

Асмолов А.Г. Оптика просвещения: социокультурные перспективы. — М.: Просвещение, 2012. — 447 с.

Божович Л.И. Проблемы формирования личности: Избр. психол. тр. / Под ред. Д.И. Фельдштейна. — 3-е изд. — М.: МПСИ; Воронеж: МОДЭК, 2001. — 349 с.

Выготский Л.С. Психология. — М.: ЭКСМО-Пресс, 2000. — 1008 с.

Дети России онлайн. Результаты международного проекта EU Kids Online II в России / Г.У. Солдатова, Е.И. Рассказова, Е.Ю. Зотова, М.И. Лебешева, П.М. Роггендорф. — М., 2012. URL: http://detionline.com/assets/files/helpline/Final_Report_05-29-11.pdf.

Емелин В.А. Утрата приватности: идентичность в условиях технологического контроля // Национальный психологический журнал. — 2014. — № 2 (14). — С. 19–26.

Кастельс М. Информационная эпоха: экономика, общество и культура / Пер. с англ. под науч. ред. О.И. Шкаратана. — М.: ГУ ВШЕ, 2000. — 315 с.

Ктениду М.Д. Трансляция чувства приватности в отношениях родителей с подростками: дис. ... канд. пед. наук. — Краснодар, 2010. — 189 с.

Леонтьев А.Н. Избранные психологические произведения: в 2 т. Т. 1. / под ред. В.В. Давыдова, В.П. Зинченко, А.А. Леонтьева, А.В. Петровского. — М.: Педагогика, 1983. — 391 с.

Нартова-Бочавер С.К. Теория приватности как направление зарубежной психологии // Психол. журн. — 2006. — № 5. — С. 28–39.

Официальный портал Роскомнадзора РФ. URL: http://pd.rkn.gov.ru/press-service/subject1/news4207/.

Официальный портал службы государственной статистики РФ. URL: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/population/demography/#.

Сайт Федеральной службы государственной статистики. URL: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/population/demography/# .

Солдатова Г.У., Олькина О.И. Отношение к приватности и защита персональных данных: вопросы безопасности российских детей и подростков // Национальный психологический журнал. — 2015. — № 3 (19). — С. 56–66.

Солдатова Г.У., Олькина О.И. Минусы открытости. Российские школьники: приватные сведения и безопасность в сети // Дети в информационном обществе. — 2015. — № 20. — С. 26–47.

Федеральный закон «О персональных данных»: научно-практический комментарий / Под ред. А.А. Приезжевой. — М.: Библиотечка Российской газеты. — 2015. — № 11. — 176 с.

Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г.У. Солдатова, Т.А. Нестик, Е.И. Рассказова, Е.Ю. Зотова. — М.: Фонд Развития Интернет, 2013. — 144 с.

Эльконин Д.Б. Психическое развитие в детских возрастах. — Москва: МПСИ, 2001. — 416 с.

Altman I. The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding. Monterey, CA., 1975.

Children's Online Privacy Protection Act (COPPA) // Federal Reserve system official website, USA. URL: http://www.federalreserve.gov/boarddocs/supmanual/cch/200601/coppa.pdf

Children's Online Privacy Protection Rule (COPPA) // Federal Trade Commission official website, USA. URL: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

Clarke R. What's 'Privacy'? URL: http://www.rogerclarke.com/DV/Privacy.html#Defn.

Kuzma J.M. Children and geotagged images: quantitative analysis for security risk assessment // International Journal of Electronic Security and Digital Forensics. — 2012. — Vol. 4 (1). — P. 54–64.

Nolan J., Raynes-Goldie K., McBride M. The Stranger Danger: Exploring Surveillance, Autonomy, and Privacy in Children's Use of Social Media // Canadian Children Journal. — 2011. — Vol. 2 (36). — P. 24–32.

Parents, Teens, and Online Privacy / M. Madden, S. Cortesi, U. Gasser, A. Lenhart, M. Duggan // Pew Research Center. 2012. URL: http://www.pewinternet.org/2012/11/20/parents-teens-and-online-privacy/

Pastalan L.A. Privacy as a behavioral concept // Social Forces. — 1970. — Vol. 45 (2). — P. 93–97.

PIA Trilateral Report Executive Summary // Information Commisioners officers' official website, UK. URL: https://ico.org.uk/media/for-organisations/documents/1042837/trilateral-report-executive-summary.pdf

Rainie L., Anderson J. Privacy in 2025: Experts' Predictions // Pew Research Center. URL: http://www.pewinternet.org/2014/12/18/privacy-in-2025-experts-predictions/

The EMC Privacy Index Global & In-Depth Country Results // EMC Corporation. URL: http://russia.emc.com/collateral/brochure/privacy-index-global-in-depth-results.pdf

Westin A. Privacy and freedom. — N.-Y., 1967.

Wolfe M. Childhood and Privacy. — N.-Y., 1978.

ПОЗИТИВНЫЙ КОНТЕНТ

Всероссийский конкурс сайтов «Позитивный контент» (www.positivecontent.ru) проводится ежегодно с 2009 г. (регистрация участников и прием заявок — до 1 ноября). Его задача — поиск и поддержка самых качественных и безопасных образовательных интернет-ресурсов, вовлекающих детскую и молодежную аудиторию Рунета в активную жизнь — как в Сети, так и за ее пределами, привлечение внимания к необходимости компетентного использования интернет-технологий и мотивация аудитории на создание сайтов с позитивным контентом.

Из небольшого отраслевого проекта конкурс «Позитивный контент» вырос во всероссийское движение, в рамках которого проходят образовательные мероприятия, выпускаются просветительские брошюры, а также ведется список «Позитивных сайтов» — ресурсов, отвечающих всем правилам IT-безопасности. Одним из таких ресурсов признан **сайт учителя информатики Андрея Сиденко** *(www.agsidenko.ru)*. Сайт содержит коллекцию полезных уроков по программированию. Он стал первым в истории «Позитивного контента» сайтом, который был признан Роскомнадзором практикующим безопасную обработку личной информации детей и подростков.

ИЗУЧИ ИНТЕРНЕТ — УПРАВЛЯЙ ИМ!

«Изучи интернет — управляй им!» — это социально-образовательный проект, направленный на повышение цифровой грамотности детей и подростков, который был создан Координационным центром при поддержке Ростелекома (игра-интернет.рф). Проект состоит из образовательного модуля, где в игровой форме представлена информация об устройстве интернета, функционировании основных IT-сервисов и безопасном использовании сети, и тренировочного приложения, позволяющего совершенствовать полученные навыки.

Ежегодно в рамках проекта проходит *Всероссийский онлайн-чемпионат,* в котором школьники могут продемонстрировать свое знание устройства интернета, побороться за верхние строчки рейтинга, получить титул чемпиона и ценные призы. Пользователями образовательного модуля уже являются более 40 тысяч школьников по всей стране, а количество участников онлайн-чемпионата в 2016 г. составило около 15 тыс. чел. Отметим, что в 2016 г. все вопросы и задания Чемпионата были посвящены теме безопасности в интернете — защите от сетевых угроз и борьбе с киберпреступниками, конфиденциальности данных, безопасности в социальных сетях.

Учебное издание

Г.У. Солдатова, А.А. Приезжева,
О.И. Олькина, В.Н. Шляпников

ПРАКТИЧЕСКАЯ ПСИХОЛОГИЯ БЕЗОПАСНОСТИ: УПРАВЛЕНИЕ ПЕРСОНАЛЬНЫМИ ДАННЫМИ В ИНТЕРНЕТЕ

Редактор *Д. Комарова*
Корректор *Е. Мохова*
Дизайн обложки *А. Гущина*
Оригинал-макет *С. Иванова*

Издательство «Генезис»
129301, Москва, ул. Ярославская, д. 14, корп. 1

Оптовая закупка книг издательства
(495) 682-54-42, info@genesis.ru

Розничная продажа
(495) 682-54-42, (495) 682-60-51
Москва, ул. Ярославская, д. 14, корп. 1
Книга почтой
125464, г. Москва, а/я 32
sale@genesis.ru

Интернет-магазин
www.genesisbook.ru, www.knigi-psychologia.com

Подписано в печать 05.12.2016. Формат 60×84/16
Бумага офсетная. Печать офсетная. Усл.-печ. л. 13,1
Тираж 2000 экз. Заказ №

Отпечатано в полном соответствии
с качеством предоставленных материалов в

Как защитить гаджеты от вредоносных программ

⇒ Установите на гаджеты специальные почтовые фильтры и антивирусные программы. Они могут предотвратить, как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.

⇒ Используйте только лицензионные программы. Чаще всего вирусами бывают заражены пиратские копии программ.

⇒ Используйте проверенные сайты.

⇒ Систематически проверяйте свои домашние компьютеры на наличие вирусов.

⇒ Делайте резервную копию важных данных.

⇒ Периодически меняйте пароли от электронной почты, социальных сетей, форумов и пр.

Будьте бдительны и соблюдайте основные правила Интернет-безопасности!

Управление Роскомнадзора по Приморскому краю

Телефон : (423) 239-08-11

ул. Беломорская, д. 18,
г. Владивосток, 690041

e-mail: rsockanc25@rkn.gov.ru

Роскомнадзор

Управление Роскомнадзора по Приморскому краю

Правила общения в сети Интернет

Правило 1

Старайтесь не выкладывать в Интернет личную информацию (фотографии, видео, ФИО, дату рождения, адрес дома, номер школы, телефоны и иные данные) или существенно сократите объем данных, которые публикуете в Интернете.

Правило 2

Не выкладывайте личную информацию (совместные фотографии, видео, иные данные) о ваших друзьях в Интернет без их разрешения. Прежде чем разместить информацию о друзьях в Сети, узнайте, не возражают ли они, чтобы вы выложили данные.

Правило 3

Не отправляйте свои персональные данные, а также свои видео и фото людям, с которыми вы познакомились в Интернете, тем более если вы не знаете их в реальной жизни. Выходите из своих аккаунтов, если пользуетесь общественными компьютерами в школе, кафе или библиотеке.

Правило 4

При общении с другими пользователями старайтесь быть вежливыми, деликатными, тактичными и дружелюбными. Не пишите грубостей, оскорблений, матерных слов – читать такие высказывания так же неприятно, как и слышать.

Правило 5

Старайтесь не реагировать на обидные комментарии, хамство и грубость других пользователей. Всегда пытайтесь уладить конфликты с пользователями мирным путем, переведите все в шутку или прекратите общение с агрессивными пользователями. Ни в коем случае не отвечайте на агрессию тем же способом.

Правило 6

Не используйте Сеть Интернет для распространения сплетен, угроз или хулиганства. Если решить проблему мирным путем не удалось, напишите жалобу администратору сайта, потребуйте заблокировать обидчика.

Правило 7

Если администратор сайта отказался вам помочь, прекратите пользоваться таким ресурсом и удалите оттуда свои данные.

Правило 8

Если к вам пришло незнакомое приложение, подумайте, стоит ли его открывать? Возможно лучше сразу его удалить.

Правило 9

Не встречайтесь в реальной жизни с онлайн-знакомыми без разрешения родителей или в отсутствие взрослого человека. Если вы хотите встретиться с новым интернет-другом, постарайтесь пойти на встречу в сопровождении взрослого, которому вы доверяете.

Правило 10

Не оставляйте без присмотра компьютер с важными сведениями на экране.

Есть в большой Сети злодей,

Злой и страшный Бармалей!

Поджидает он детей,

Способом обманным,

Он желает, вход найти

К ПЕРСОНАЛЬНЫИ ДАННЫМ!

Данные свои храни,
Никому не говори,
Бережно к ним относись,
В ИНТЕРНЕТЕ не делись!

Будь на страже своих персональных данных

Портал http://персональныеданные.дети

Управление Роскомнадзора
по Приморскому краю
Телефон : (423) 239-08-11

ул. Беломорская, д. 18,
г. Владивосток, 690041
e-mail: rsockanc25@rkn.gov.ru

Правила безопасности в сети интернет для тебя и твоих друзей

Что такое Интернет?
Злой, ужасный человек?
Или добрый милый мишка?
Может спорт это и книжка?
На вопрос об Интернет,

Мы откроем Вам секрет.
Это вовсе не злодей,
Собирает сто друзей,
Ищет нужные вещички,
И уроки, и странички,
В Интернете все легко,
Клик и все уже нашлось.

Можно книгу отыскать,
Можно сказку прочитать,
Посмотреть любое диво,
Что красиво и игриво,

А еще там все ответы,
Обо всем на белом свете…
НО!

Нельзя Вам забывать,
Кроме пользы, Важно знать!
Безопасность в Интернете,
Надо детям соблюдать!

далее правила

1

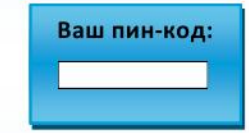
Не рассказывай секреты,
О себе ты в Интернете,
В переписках: где и с кем,
Сообщать не надо Всем!

Ограничь объем информации о себе в Интернете. Удали лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.

2

Если Вы нашли страничку,
Где к Вам просится безличка –
это злое приложение,

Хочет вирус навязать,
Просит Вас пин - код отдать?
Или просит Ваше имя, адрес,
карту, телефон,



Никогда нельзя ребята,
Таким сайтам доверять!
Уходи оттуда просто,
Лучше взрослого спроси,
А уж если все несносно,
Антивирус запусти!

3

А еще мы в Интернете,
Можем друга завести,
Незнакомец в Интернете-
это может быть обман,
Потому что в самом деле,
Может быть он хулиган.
Если ты не знаешь друга,
С кем общаешься в Сети,
Лучше удалить такого,
В черный список занести!

4

Не встречайся с людьми, которых не знаешь в реальной жизни. Если кто-то приглашает тебя встретиться или оскорбляет тебя – не отвечай и срочно расскажи об этом родителям или кому-нибудь из взрослых близких людей!

Помни! В мире Интернета,
Виртуального
пространства,
Все реально, как и в жизни
Наполняется коварством.

5

Если ты попал в
беду,
И затеял чехарду,
В Интернете видно
сразу
Кто ты, где ты, слезы
градом,
Троллят, издеваются?
Тебе это не нравится!

Не отчаивайся друг,
Ведь подмога тут как тут,
Сразу взрослым сообщай,
Все странички удаляй,
Никого не обзывай,
И в ответ не отвечай!

**Все решится без труда,
Улыбнись, и будь на страже,
Своих данных личных, Важных!
Персональные они,
В твоей жизни так Важны!**

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО ПРИМОРСКОМУ КРАЮ

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ НЕСОВЕРШЕННОЛЕТНИХ

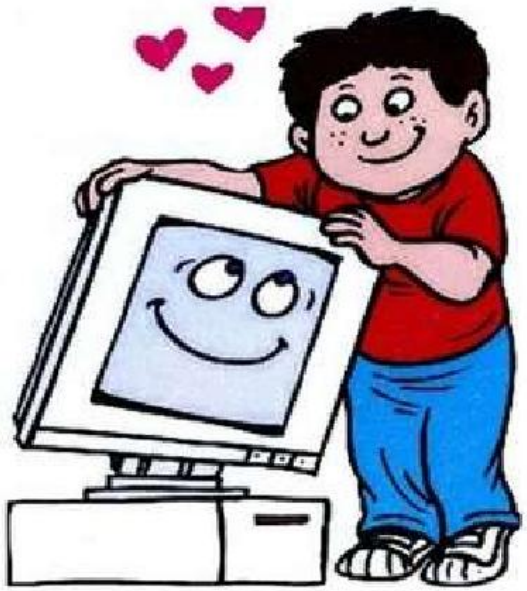
ОСНОВЫ БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ

1. Будьте осторожны с незнакомыми сайтами.
2. Если в сети необходимо пройти регистрацию, постарайтесь, чтобы в ней не было указано никакой личной информации.

3. Не сообщайте другим людям свой пароль.
4. Старайтесь использовать для паролей набор цифр и букв, чтобы посторонним было трудно его запомнить.

5. Если к Вам по почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть его, обязательно проверьте на вирусы.
6. Если пришло незнакомое вложение, подумайте, стоит ли его открывать? Возможно, лучше сразу его удалить.

7. При общении в Интернете не указывайте свои личные данные, используйте псевдоним (ник).
8. Без контроля взрослых не встречайтесь с людьми, с которыми познакомились в сети Интернет.
9. Не всей информации, которая размещена в Интернете, можно верить.



10. Не оставляйте без присмотра компьютер с важными сведениям на экране.
11. Не сохраняйте личные сведения на общедоступном компьютере.
12. Выходите из своих аккаунтов, если пользуетесь общественными компьютерами в школе, кафе или библиотеке.

Памятка

«ОСНОВЫ БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ»

Роскомнадзор

Правило № 1 – «Спрашивай взрослых и установи фильтр»

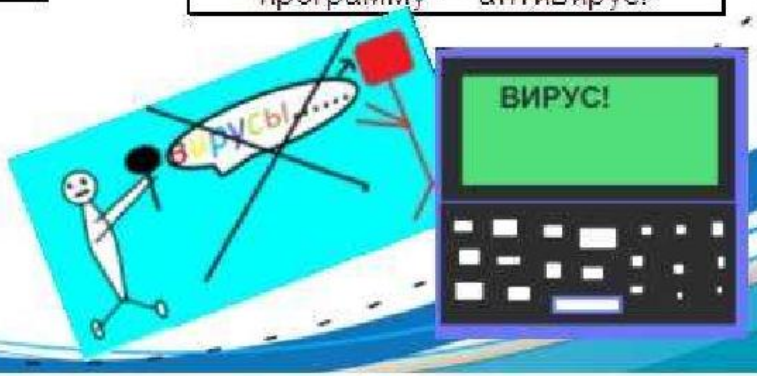
Если что-то непонятно
Страшно или неприятно,
Быстро к взрослым поспеши,
Расскажи и покажи.
Как и всюду на планете,
Есть опасность в Интернете.
Мы опасность исключаем,
Если фильтры подключаем.

Всегда спрашивай родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.

Правило № 2 – «Безопасность компьютера в Интернете»

Не хочу попасть в беду —
Антивирус заведу!
Всем, кто ходит в Интернет,
Пригодится наш совет.

Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу — антивирус!



Правило № 3 – «Осторожно! Мошенники!»

Иногда тебе в Сети...
Вдруг встречаются вруны.
Ты мошенникам не верь,
Информацию проверь!

Если хочешь скачать картинку или мелодию, но тебя просят отправить СМС — не спеши!

Не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.

Не соглашайся на требования мошенников!

Информационно-образовательный сайт «ПЕРСОНАЛЬНЫЕ ДАННЫЕ.ДЕТИ»

ПЕРСОНАЖИ

ИГРЫ

КОНКУРСЫ

ТЕСТЫ

Портал персональные данные дети

СПАСИБО ЗА ВНИМАНИЕ