

Безопасный Интернет

Управление Федеральной службы по надзору в сфере связи,
информационных технологий и массовых коммуникаций
по Алтайскому краю и Республике Алтай

Что такое персональные данные?

Персональные данные (ПД) – это набор данных, позволяющих идентифицировать Вас среди других.

В том числе:

1. *фамилия, имя, отчество;*
2. *дата рождения;*
3. *адрес местожительства;*
4. *паспортные данные*
5. *социальное, имущественное, семейное положение;*
6. *сведения об образовании;*
7. *фотографии;*
8. *и другие.*



Я ознакомился с **правилами**, политикой **конфиденциальности** и принимаю их условия.

Специальные персональные данные

К специальным персональным данным относятся:

- ▶ *расовая или национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья и пр.*

Следует заметить, что приведенный перечень персональных данных не является исчерпывающим и может включать в себя еще множество иных идентификационных данных.

Биометрические персональные данные

Биометрические персональные данные представляют собой сведения о наших биологических особенностях. Эти данные уникальны, принадлежат только одному человеку и никогда не повторяются.

Биометрические данные заложены в нас от рождения самой природой, они никем не присваиваются, это просто закодированная информация о человеке, которую люди научились считывать. К таким данным относятся:

- ▶ *отпечаток пальца, рисунок радужной оболочки глаза, код ДНК, слепок голоса и пр.*

Набор цифр как персональные данные

- ▶ Существуют персональные данные, которые представляют собой набор цифр. Благодаря такому набору цифр нас можно определить как конкретного человека, установить нашу личность.
- ▶ **Таковыми персональными данными являются: номер и серия паспорта, страховой номер индивидуального лицевого счета (СНИЛС), индивидуальный номер налогоплательщика (ИНН), номер банковского счета, номер банковской карты.**
- ▶ Такие «кодовые данные» представляют собой некий набор зашифрованной информации о человеке. Шифрование этих данных может производиться государством. Например, когда ребенку исполняется 14 лет, ему выдают паспорт в ФМС. Такой паспорт содержит серию и номер, а также иную информацию. Шифрование может производиться банковской организацией, например, номер банковской карты тоже индивидуальный, он не повторяется и принадлежит исключительно держателю банковской карты.
- ▶ **пр.**

Большие данные

Большие данные – это все таки информация. Настолько большая, что ей сложно оперировать с помощью обычных программных средств.

В широком смысле – это сбор, хранение, анализ, поиск, передача, визуализация, обновление и безопасность данных. В узком смысле – анализ и предсказания по большим наборам данных.

Некоторые ее примеры:

База данных операторов мобильной связи

Геолокационная информация всех фотографий, выложенных в Instagram

База данных пользовательских аккаунтов Facebook

Данные с сейсмологических станций по всей Земле

Зачем защищать персональные данные ?

- 👉 Вы хотите платить «чужие» кредиты»?
- 👉 Вы хотите читать о себе в сети ложную информацию?
- 👉 Вы хотите, что бы ваша электронная переписка стала достоянием гласности?
- 👉 Вы хотите, чтобы Ваш банковский счет стал общим?
- 👉 Вы хотите, чтобы о Ваших болезнях и недугах стало известно всем?

НЕТ?

ТОГДА ЗАЩИТИТЕ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Угрозы безопасности персональных данных



Кража имущества

Когда нет физических угроз, то и физическая защита не нужна, а вот информационная — нужна всегда.



Ваши фото и видео скопируют без разрешения



Фейковый аккаунт



Навязчивая реклама и звонки



Могут собрать и продать информацию о Вас



Вы можете стать объектом слежки

Как защитить свои данные в сети?



Не указывайте лишнюю информацию при регистрации на сервисах Интернет и в социальных сетях



Включите двухфакторную авторизацию на всех сайтах и сервисах (с подтверждением входа по смс или e-mail)



Ограничьте доступ к своему профилю в соцсетях



Не публикуйте в «онлайн» фотографии документов, билетов и платежных чеков

Как защитить свои данные в сети?



Не запускайте подозрительные вложения, присланные по электронной почте и через интернет - messengers



Никогда не повторяйте ввод одинаковых паролей на разных ресурсах



Установите на компьютер (смартфон) защитное ПО и следите за регулярностью обновления антивирусных баз



Старайтесь не работать с открытыми точками Wi-Fi



Не ставьте геолокацию под своими постами

Кто хранит мои персональные данные



Основные опасности Интернета

1. *Вредоносные программы* - (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным.

- ▶ Они также могут снижать скорость обмена данными и даже использовать ваш компьютер для распространения вируса, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети и даже следить за всем что вы вводите с клавиатуры.



Основные правила поведения:

1. Установите на компьютеры специальные антивирусные программы (Антивирус Касперского, Dr.Web, avast!) для предотвращения заражения компьютера и потери данных.
2. Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.
3. Используйте только сложные пароли, разные для разных учетных записей и сервисов.
4. Старайтесь периодически менять пароли, особенно после их использования не на вашем личном ПК .

Примеры «плохих» и «хороших» паролей:

Нельзя использовать:

| | |
|--|---|
|  Bobik | Персональные данные, которые легко о вас узнать |
|  password | Слова «пароль», «pass», «password» и т.д. |
|  18723627 | Только цифры |
|  qwerty | Буквы «йцукен», «qwerty», «abcdef» и т.д. |
|  noklab | Обратный порядок букв в словах |

Можно использовать:

| | |
|--|--|
|  MagazinMVideo | Буквы как в верхнем, так и нижнем регистре |
|  MagazinNomer1 | Буквы и цифры |
|  MagazinM1M.Video | Буквы, цифры и спец-символы (№, ^, &, @) |

Главные правила «Хорошего» пароля:

1. Длина пароля не менее 8 символов
2. Наличие букв в различных транслитерациях (например: русские, английские)
3. Наличие прописных и строчных букв
4. Наличие цифр и специальных символов

Как придумать правильный пароль:

- Используйте любое русское слово, набранное в английской раскладке, заменяя некоторые буквы цифрами
- Закройте глаза и нажимайте на клавиатуру время от времени придерживая Shift. Откройте глаза и запомните то, что получилось
- Вспомните фразу или цитату, например «Терпение и труд все перетрут», соедините первые буквы слов или слоги

ч-е-л-о-в-е-к
↓
4 t k 0 d t r

f Q 6 S s d 9 # L c

T-i-T-r-V-s-p-r-t-r
↓
T 1 i T r # V s p 8 r t r

Кибербуллинг - это нападение с целью нанести психологический вред;

- преследование сообщениями, содержащими оскорбления, агрессию, запугивания;

- распространение видеороликов с записями реальных сцен насилия, без согласия жертв такого насилия.

► **киберпреследование** - скрытое выслеживание жертвы с целью организации нападения, избиения, и т.д.

Троллинг - вызывающее поведение, оскорбления и провокации в Интернете.



Грумлинг - установление дружеских отношений с целью личной встречи, вступления в сексуальные отношения, шантажа. Такие знакомства чаще всего происходят в чате, на форумах или в социальной сети.



Кибермошенничество - получение денег или имущества путем обмана или злоупотребления доверием.

- ▶ Если планируете совершить покупку через интернет-сайт: ознакомьтесь с отзывами покупателей, убедитесь в его безопасности – проверьте реквизиты и название магазина.



Фишинг

Фишинг - один из видов интернет-мошенничества, целью которого является получение доступа данным пользователей - логинам, паролям, данным лицевых счетов и банковских карт.

- В основном, используется метод проведения массовых рассылок от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих.



[COMPOSE](#)[4-100000000121] Ошибка доставки сообщений Inbox x

Inbox (7)

Starred

Sent Mail

Drafts

More ▾

Ekaterina ▾ Gmail Team <ru.gm.contact@gmail.com>
to ru.gm.contact ▾

Nov 16 (4 days ago) ☆



Russian ▾

> English ▾

[Translate message](#)[Turn off for: Russian x](#)

Google accounts

Уважаемый пользователь!

Сообщения, отправленные Вам с 17.11.15, не были доставлены в связи с перегрузкой почтовых серверов. Чтобы получить письма, перейдите на страницу расположенную ниже:

[Получить недоставленные сообщения](#)

Спасибо за понимание. Обработка доставки может занять до 3х часов.

С уважением, служба поддержки почтовой системы Google

[Click here to Reply or Forward](#)

No recent chats
[Start a new one](#)

Основные правила поведения:

1. **Ограничьте** объем информации о себе, находящейся в Интернете. **Удалите** лишние фотографии, видео, адреса, номера телефонов, дату рождения, сведения о родных и близких и иную личную информацию.
2. **Не отправляйте** видео и фотографии людям, с которыми вы познакомились в Интернете и **не знаете** их в реальной жизни.
3. Отправляя кому-либо свои персональные данные или конфиденциальную информацию, **убедитесь** в том, что адресат — действительно тот, за кого себя выдает.
4. Если в сети Интернет кто-то просит предоставить ваши персональные данные, например, место жительства или номер школы, класса иные данные, **посоветуйтесь с родителями** или взрослым человеком, которому вы доверяете.
5. Заведите себе **два адреса электронной почты** — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для открытой деятельности (форумов, чатов и так далее).

Настройки приватности на примере ВКонтакте:

Моя страница

Кто видит основную информацию моей страницы  Только друзья

Кто видит фотографии, на которых меня отметили  Только друзья

Кто видит список моих сохранённых фотографий  Только я

Кто видит список моих групп Все пользователи

Связь со мной

Кто может писать мне личные сообщения Все пользователи

Кто может мне звонить Все пользователи

Записи на странице

Кто видит чужие записи на моей странице  Только друзья

Кто может оставлять записи на моей странице  Только я

Кто видит комментарии к записям Все пользователи

Кто может комментировать мои записи Все пользователи

Кто может отмечать меня на фотографиях  Только друзья

Основные правила:

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



Что делать, если Вас взломали?

► **Как определить, что Вас взломали!**

- От Вашего имени были совершены действия, которые Вы не делали *(написаны сообщения, добавлены друзья, оставлены комментарии, поставлены отметки и др.)*
- *Вы не можете зайти в свой аккаунт с помощью своего логина и пароля;*

► **Что делать?**

- Незамедлительно поменяйте пароль;
- Проверьте компьютер на наличие вирусных угроз;
- Напишите администратору сайта *(о невозможности восстановить доступ к аккаунту, о необходимости заблокировать аккаунт и др.);*
- В случае, если мошенники использовали полученные в результате взлома Ваши персональные данные без Вашего согласия и такими действиями Вам причинен материальный или моральный вред , Вам следует обращаться в правоохранительные органы, т.к. такие противоправные действия подпадают под составы уголовно-наказуемых деяний.

Информация, которая подлежит блокировке

- ▶ Информация о способах совершения самоубийства, призывах к нему;
- ▶ Информация о несовершеннолетних, пострадавших от противоправных действий;
- ▶ Информация об азартных играх;
- ▶ Информация, содержащая предложения о продаже дистанционным способом, алкогольной продукции, спиртосодержащей продукции, этилового спирта;
- ▶ Информация о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;
- ▶ Материалы с порнографическими изображениями несовершеннолетних.

ВОПРОСЫ, КОТОРЫЕ СЛЕДУЕТ ЗАДАТЬ САМОМУ СЕБЕ



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.

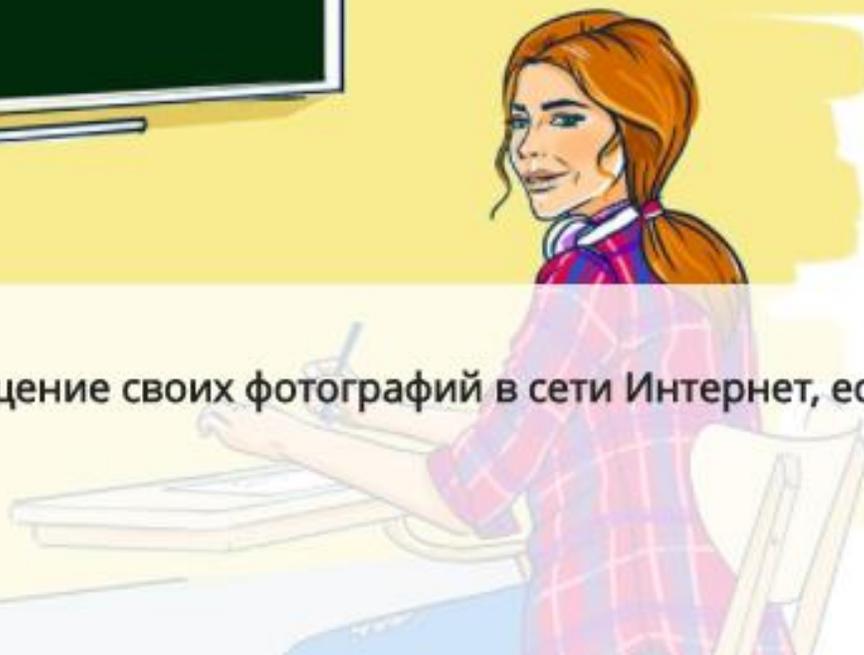


Перечень данных, который можно отнести к персональным, четко не определен в законах. Поэтому набор данных, позволяющий определить или идентифицировать тебя среди множества других людей является персональными





Что такое персональные
данные?



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

- Да
- Нет



При публикации фотографий в Сети, вы даете другим возможность на их загрузку, изменение или даже использование их в рекламе! Всегда проверяйте, что вы установили настройки приватности.





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.

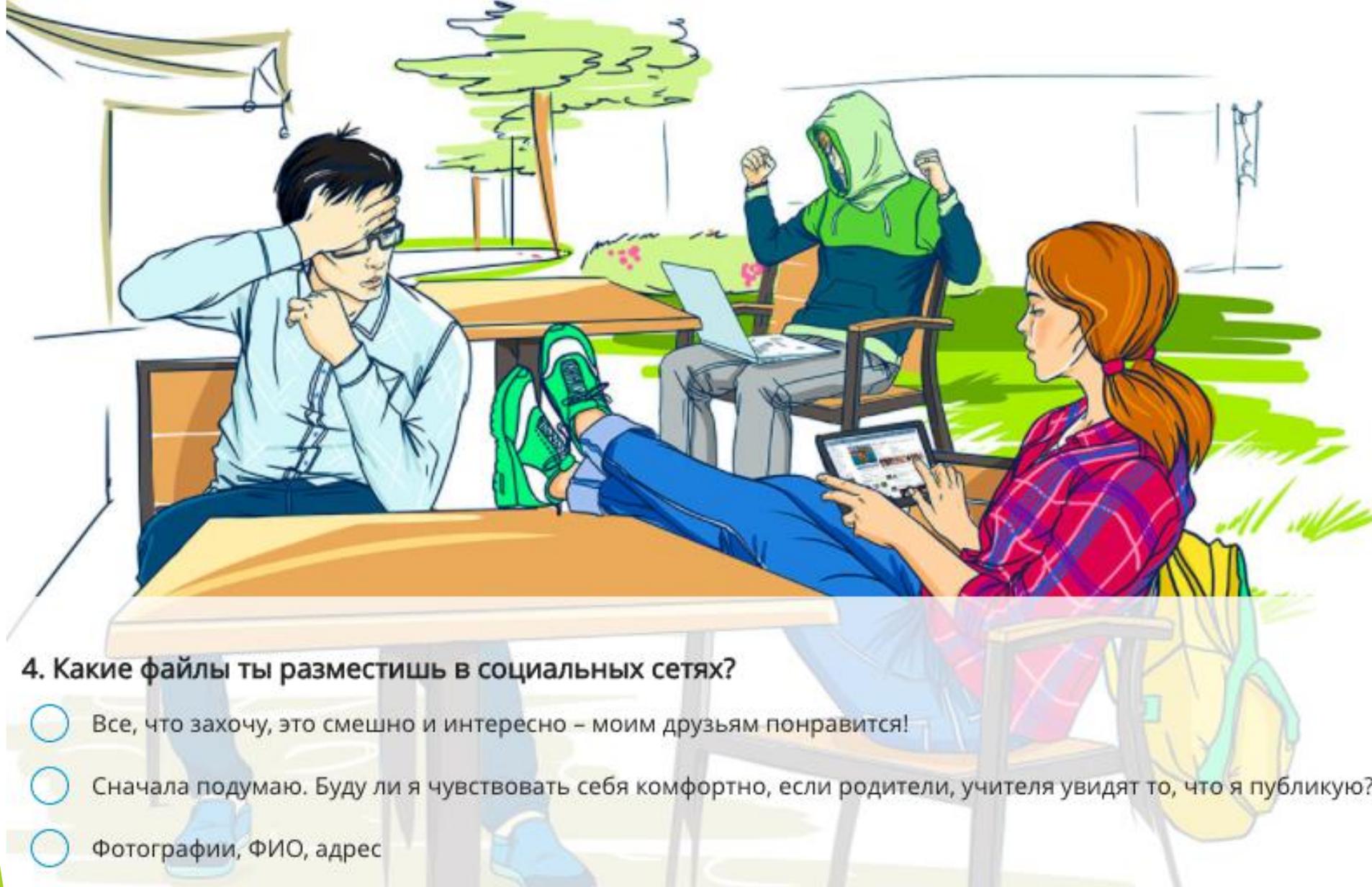
Да

Нет



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



Важно сначала подумать, прежде чем публиковать что-то. Вся информация из твоего профиля - комментарии, фотографии - могут увидеть тысячи людей и эта информация никогда не будет полностью стерта. Информация в сети помогает другим людям составить впечатление о тебе, и как ты ведешь себя в реальной жизни.





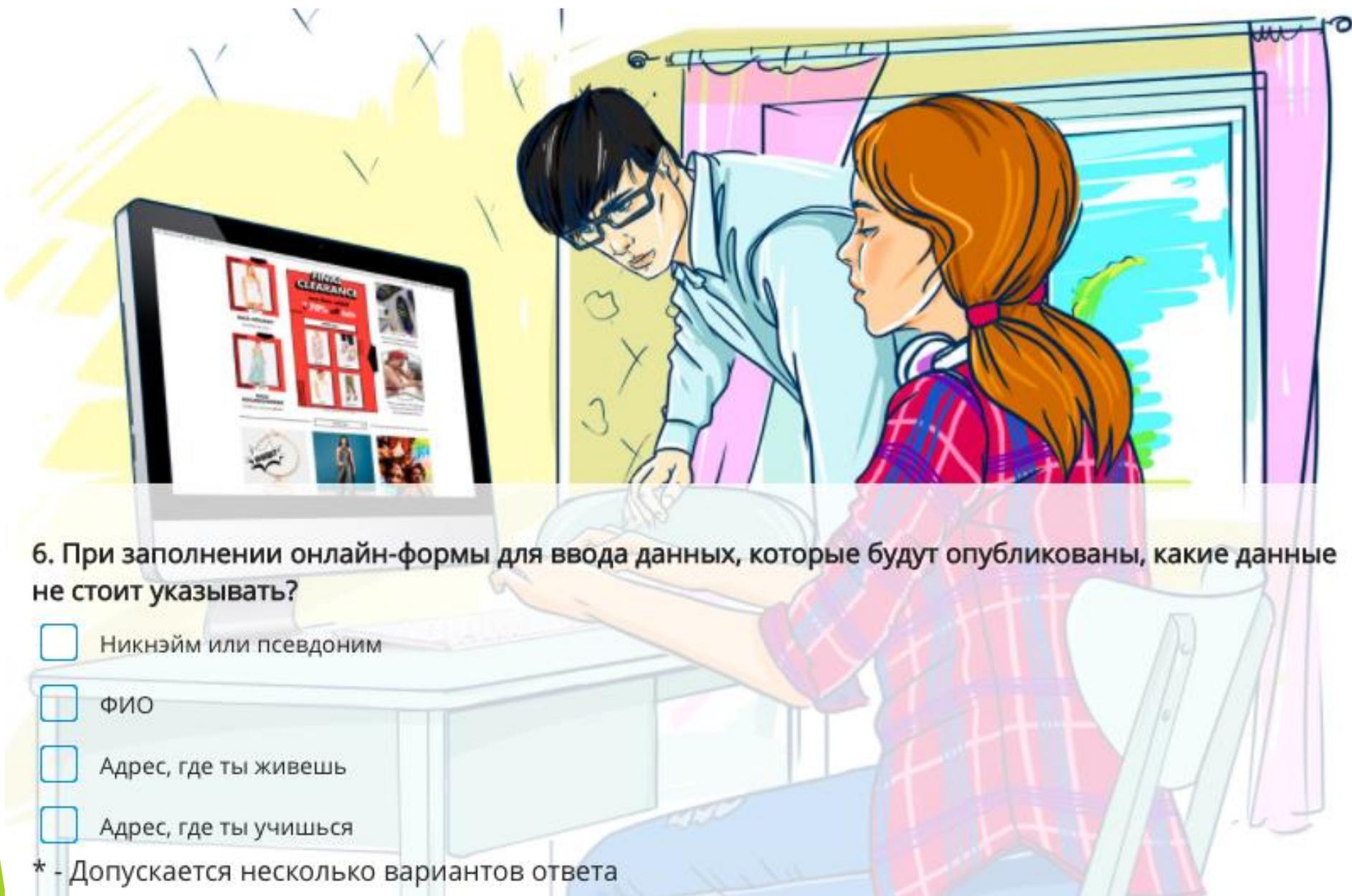
5. Может ли твой друг заходить в твой аккаунт и отправлять от твоего имени сообщения?

- 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.



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.





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

- Никнейм или псевдоним
- ФИО
- Адрес, где ты живешь
- Адрес, где ты учишься

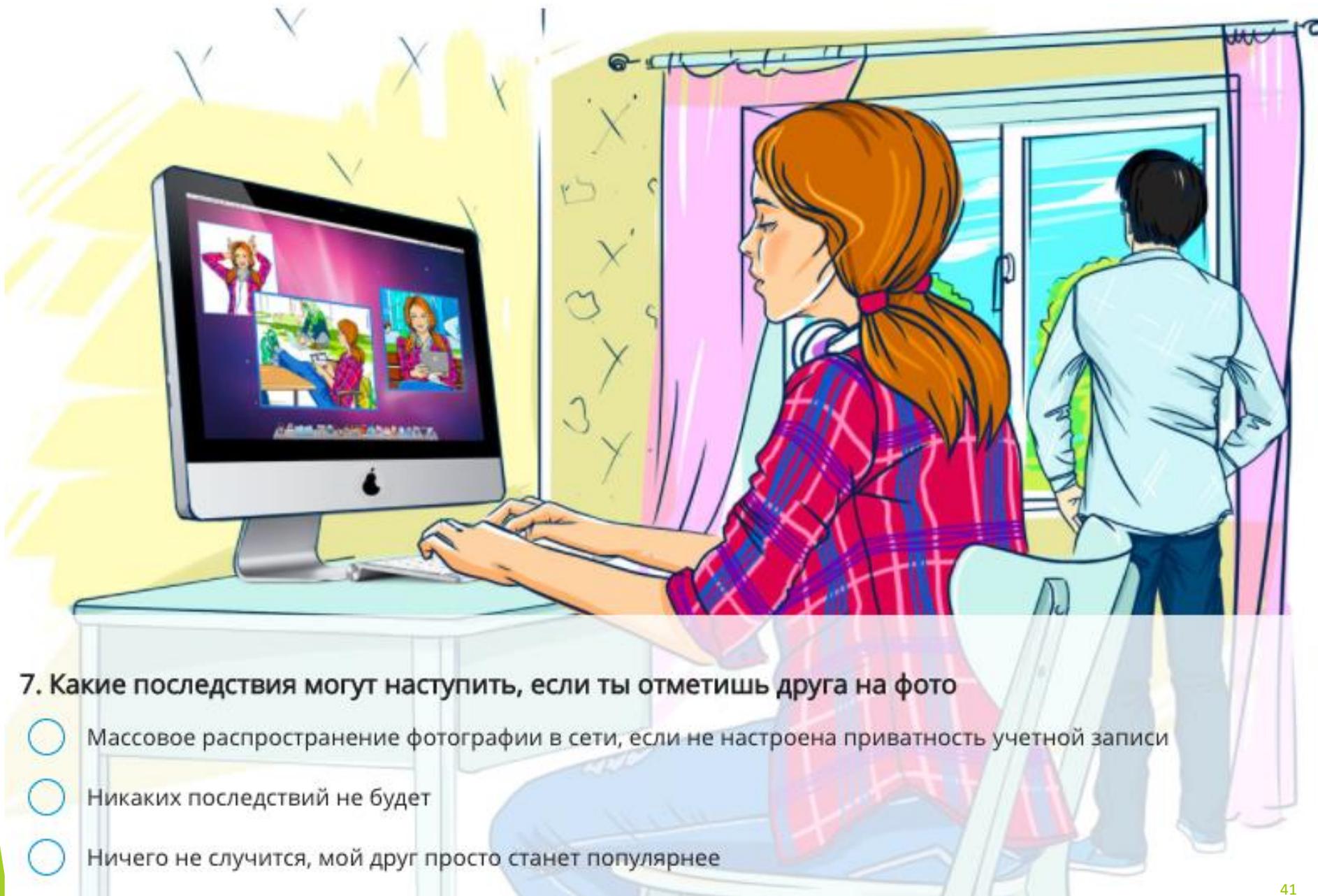
* - Допускается несколько вариантов ответа



ФИО и адрес места жительства позволяет идентифицировать вашу виртуальную личность в реальной жизни.

ДАЛЬШЕ





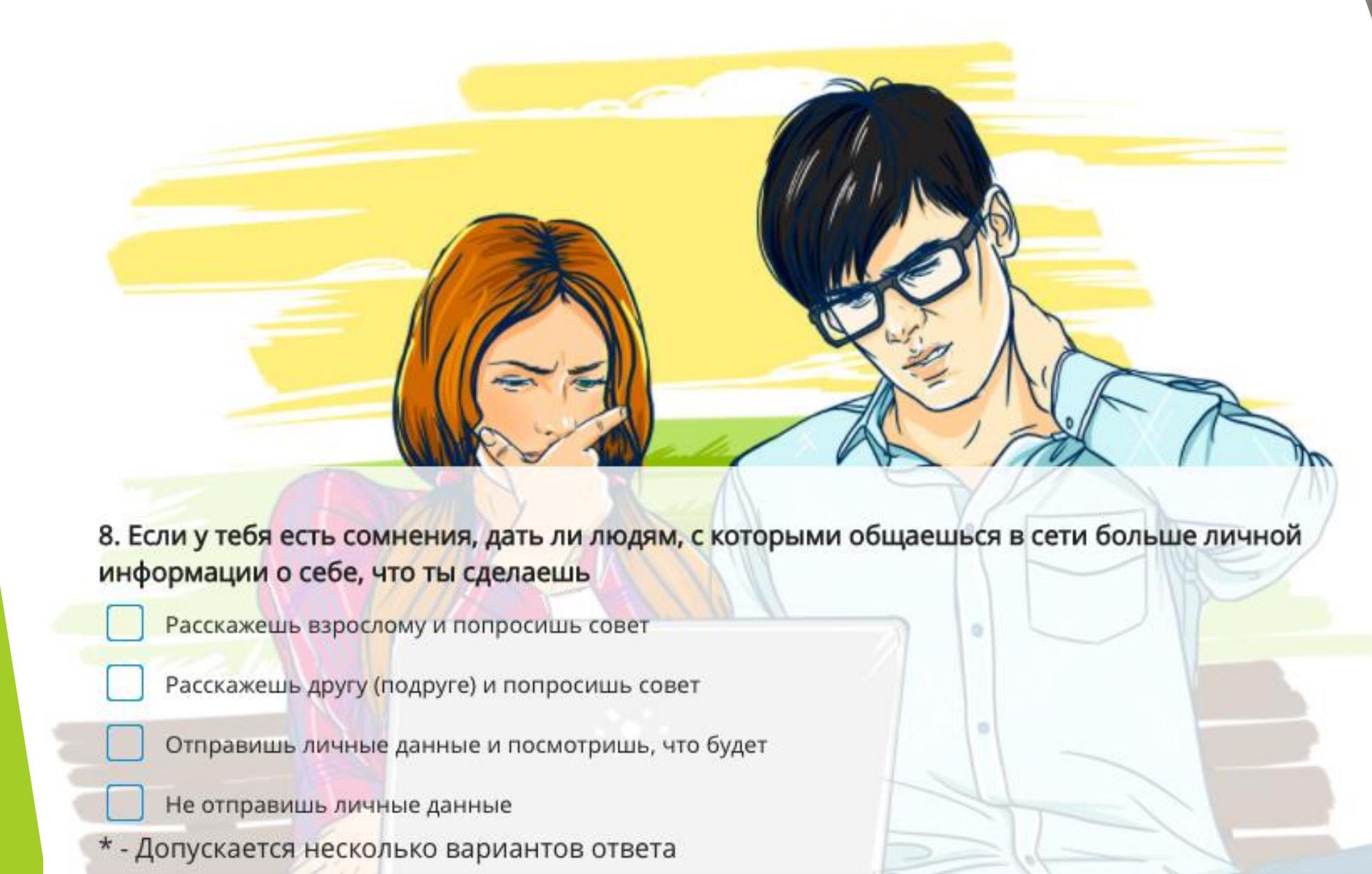
7. Какие последствия могут наступить, если ты отметишь друга на фото

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



Вы никогда не можете знать точно, кто имеет доступ к информации, которую вы публикуете на сайте. Не стоит этого делать без разрешения друга, возможно, он не хочет, чтобы информация о нем стала доступной для других.





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



В любом случае, не стоит отдавать незнакомцам свои персональные данные. Вы не можете быть уверены, как их будут использовать.





СПАСИБО ЗА ВНИМАНИЕ!

*Управление Федеральной службы по надзору в сфере связи,
информационных технологий и массовых коммуникаций по
Алтайскому краю и Республике Алтай*

адрес: г. Барнаул, ул. Интернациональная, д. 72.
e-mail: rsockanc22@rkn.gov.ru
тел. (3852) 55-66-13 – приемная
(3852) 55-66-29, 55-66-31, 55-66-32 – отдел по защите
прав субъектов персональных данных.