Агенты безопасности

№ 1 2022

ТЕМА НОМЕРА

Социальные сети

А ТАКЖЕ ДРУГИЕ

СЕКРЕТНЫЕ МАТЕРИАЛЫ
Управление «К» информирует и предостерегает

ЧТО СКАЖЕТ ПСИХОЛОГ
Опасное селфи. Лайк или жизнь

КОГО ВОЗЬМУТ В БУДУЩЕЕ
Кто приносит самую большую прибыль

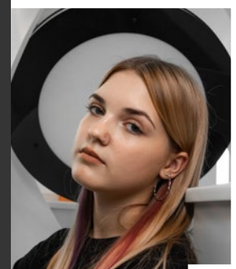
ЮНКОРЫ МЕДИАШКОЛЫ. МАРШРУТ ПОСТРОЕН
Один день в Москве

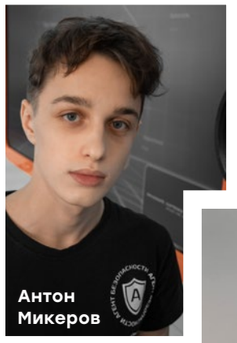
СОДЕРЖАНИЕ

ФОСАГРО · ДРОЗД ЧЕРЕПОВЕЦ · ИНТЕРАКТИВНО-ПОЗНАВАТЕЛЬНЫЙ ЦЕНТР ЗЕЛЕНАЯ ПЛАНЕТА

Агенты безопасности – то, что тебе нужно

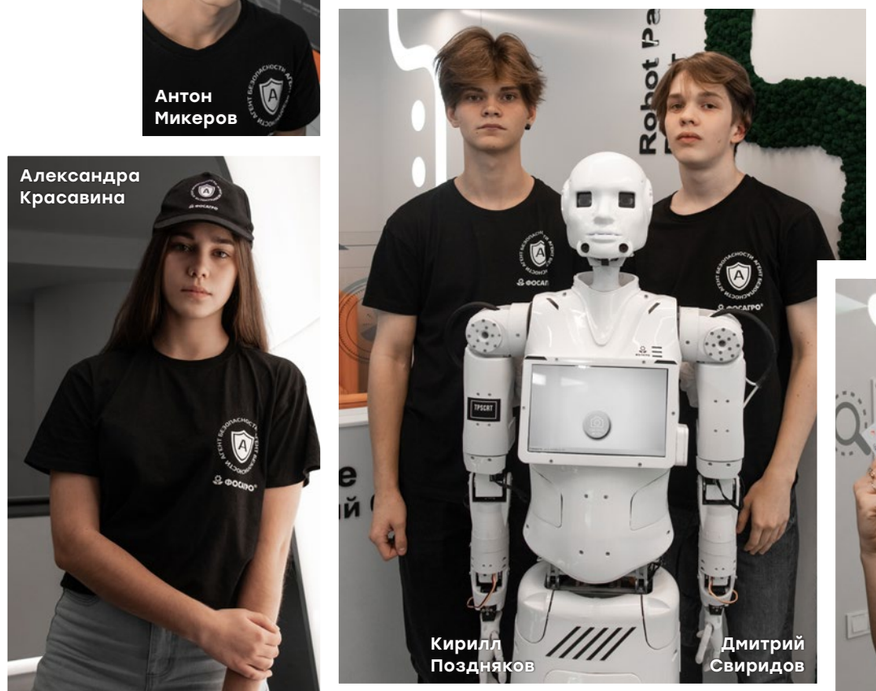
Привет!
Мы – участники проекта «Агенты безопасности», который реализуется в интерактивно-познавательном центре «Зеленая планета».
У тебя в руках первый номер нашего журнала о кибербезопасности.
Для чего мы его сделали? Чтобы рассказать о нашем уникальном проекте и поделиться лайфхаками от крутых экспертов, с которыми мы здесь познакомились.
Ты тоже можешь стать героем одного из номеров журнала. Присоединяйся к нашей команде!


Виктория Родичева

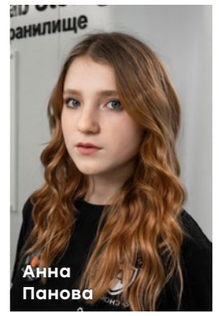

Антон Микеров


Олеся Баринова


Влад Попов

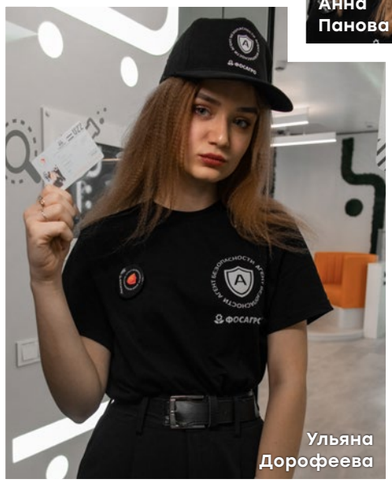

Кирилл Поздняков · Дмитрий Свиридов

ЗДЕСЬ МОЖЕШЬ БЫТЬ ТЫ


Анна Панова


Софья Бычкова

Александра Красавина


Ульяна Дорофеева

О том, зачем нужен проект, что его участники узнают на занятиях, рассказывает руководитель проекта, директор профориентационно-выставочного центра ЧОУ ДПО «Учебный центр ФосАгро» **Юлия Бондаренко**.

О проекте

Сознательный выбор в пользу безопасной жизни

Проект «Агенты безопасности» стартовал в июне 2021 года и задуман для ребят 12–18 лет. Мы запустили его для того, чтобы познакомить подростков со спецслужбами и профессиями в области защиты населения в городе, на предприятии, в быту. А главное — научить, как противостоять различным угрозам, которые нас подстерегают в повседневной жизни.

Конечно, сами бы мы с такой сложной темой не справились. Поэтому объединились с теми, кто обеспечивает нашу безопасность в жизни, в школе, на работе: с Дирекцией по экономической безопасности нашего предприятия АО «Апатит», УМВД по Вологодской области и УМВД г. Череповца.

Первым делом наши юные агенты знакомятся с организацией работы службы безопасности (СБ) предприятия. Для этого выходят на контрольно-пропускной пункт (узнают, как работают тепловизор и алкотестер), а также на пункт видеонаблюдения. Кстати, служба режима АО «Апатит» для контроля за тем, что происходит на территории предприятия, использует квадрокоптеры: во время полета их камеры транслируют изображение на мониторы СБ и ведут видеосъемку.

Кроме того, агенты имеют уникальную возможность:

- провести дактилоскопию и увидеть секретное содержимое специального чемоданчика криминалиста;
- попробовать составить фоторобот в лаборатории портретной экспертизы;
- на месте увидеть, как трудятся пожарные и кинологи с собаками, которых учат выявлять наркотики и взрывчатые вещества;
- примерить спецснаряжение и даже получить мастер-класс по приемам самообороны;
- побывать на практических занятиях по кибербезопасности, которые ведут специалисты по информационной безопасности АО «Апатит»;
- проверить свою физическую форму и сдать нормы ГТО — в этом помогут тренеры АНО «ДРОЗД».

ХОЧЕШЬ стать тем, кто обеспечивает безопасность города, региона, страны?

Погрузись в эту профессию!

ИНТЕРЕСНО, как работают криминалисты?

Приглашаем попробовать задействовать технологию и логику!

А МОЖЕТ, хочешь узнать, как воспитывают служебных собак кинологической службы?

Это и многое другое ты узнаешь вместе с нами!

Вступай в ряды агентов безопасности! Выполняй задания! Получай звезды и обменивай их на призы, которые получишь за то, что уделяешь внимание своей жизни!

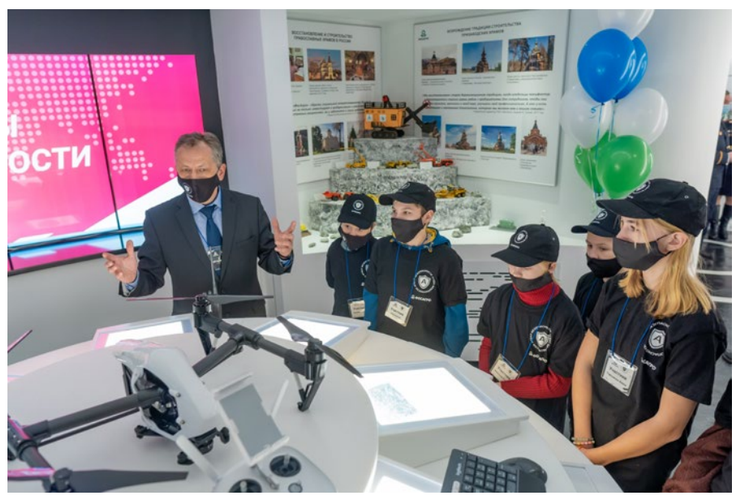
Уникальность проекта в том, что он помогает ребятам определиться с профессией, расширить кругозор, а также обеспечивает сознательный выбор в пользу безопасного жизненного пути.

Стать его участником могут школьники и студенты. За полтора года, что он реализуется, 4 тысячи мальчишек и девчонок прошли квесты, побывали на экскурсиях и занятиях… Словом, узнали все о безопасности.

Мы такого не ожидали, но сейчас проект уже вышел за пределы Череповца: в ряды юных агентов вступили ребята из Вологды, Волхова и Балакова. Для новичков мы специально разработали атрибутику с особой эмблемой.

Каждый подросток, вступая в ряды агентов безопасности, получает в подарок фирменный комплект: футболку, кепку, ручку блокнот и… именную карту. На нее агенту присваиваем звезды за успешное выполнение заданий. Ну а самых активных награждаем на Фестивале безопасности (проходит в декабре), где подводим итоги года.

Аналогов нашему проекту в России нет. Неслучайно в мае 2022 года он стал победителем IV Всероссийского конкурса «Корпоративный музей» (номинация «Лучшее мероприятие»).



ФОСАГРО · ИНТЕРАКТИВНО-ПОЗНАВАТЕЛЬНЫЙ ЦЕНТР ЗЕЛЕНАЯ ПЛАНЕТА

Из отзывов

6 «А», школа 14, г. Череповец

Все очень понравилось! Организация, интересный материал, практическая часть — выше всяких похвал! 😍👏👏👏

Спасибо большое!!! Очень приятно 😊😘

А. Бутакова, г. Санкт-Петербург

Как психолог могу сказать, что экспозиция, посвященная зависимостям, кибербезопасности и буллингу, сделана изумительно! 👍😃😊

Благодарим за отзыв. Нам очень важно мнение профессионала! 😊😊

Т. Кудряшова

Примеряли форму,😉 тушили пожар,💨🔥 изучали следы преступлений, ловили преступников… 🤓 Очень понравилось.👍

Отлично! А на занятии по кибербезопасности вы были? Если еще нет, то приглашаем! 😊🙏🙏

Зам. начальника ОУУП и ПДН УМВД России по г. Череповцу, подполковник полиции С. Иванова

Экспозиция «Лаборатория безопасности» и все мероприятия, которые проводятся в ее рамках, в том числе проект «Агенты безопасности», получили высокую оценку руководства УМВД по Вологодской области. 👏😎😉

Ого! Это действительно значимая оценка для нас. Служим Отечеству! 😃🤝

ИТОГИ ГОДА 2022

СОЗДАНО СООБЩЕСТВО «Агенты безопасности» в соцсети «ВКонтакте».

В нем собраны актуальные новости проекта, онлайн-задания и афиши мероприятий.

ОРГАНИЗОВАНЫ ЭКСКУРСИИ

в пожарную часть ООО «Агрохимбезопасность», лабораторию экспертов-криминалистов, Центр кинологической службы и музей УМВД г. Череповца, а также на территорию ГИБДД.

СОВМЕСТНО С ПАРТНЕРАМИ ПРОЕКТА проведено

БОЛЕЕ 350 МЕРОПРИЯТИЙ

КОЛИЧЕСТВО УЧАСТНИКОВ ПРЕВЫСИЛО

БОЛЕЕ 4 500 ЧЕЛОВЕК

Это подростки, родители, учителя, а также дети, состоящие на учете в полиции.

РАЗРАБОТАНЫ УНИКАЛЬНЫЕ ПРОГРАММЫ, ЗАНЯТИЯ И БЕСЕДЫ

Среди них: интерактивные беседа «Все о психоактивных веществах и не только» и квест в реальности «Лаборатория безопасности», «Мозговой штурм», практические занятия по «Кибербезопасности», от «Экспертов криминалистов» и мастер-класс от ГИБДД.

ПРОЕКТ «АБ» активно тиражируется в Музейно-выставочном центре «Пятнадцатый элемент» (г. Волхов) **и Музее Балаковского филиала АО «Апатит»** (г. Балаково).

КВЕСТ-ИГРА И БЛОГИНГ

Ключевое мероприятие — интерактивный квест «Агенты безопасности». Это своего рода комплекс-погружение в проект. Так, за два часа пребывания в «Зеленой планете» его участники узнают о режиме работы охраны предприятия, как обеспечивается безопасность на территории производственных комплексов. А также знакомятся с работой пожарной части «Агрохимбезопасность», экспертов-криминалистов, ГИБДД и т. д.

«ФЕСТИВАЛЬ БЕЗОПАСНОСТИ»

«Фестиваль безопасности» — главное мероприятие-праздник, на котором были подведены итоги первого года реализации проекта. Он прошел в декабре 2021 года в г. Череповце. Почетными гостями фестиваля стали начальник Управления МВД Российской Федерации по Вологодской области, генерал-майор полиции Виктор Пестерев и генеральный директор АО «Апатит» Александр Гильгенберг. В торжественной обстановке они вручили юным агентам безопасности дипломы за прохождение квест-игры.


Почетные гости открывают Лабораторию безопасности

«МЕДИАШКОЛА»

Популярным направлением стал проект «Медиашкола». Это курс занятий от проекта «АБ» и ИПЦ «Зеленая планета», который помогает ребятам стать ближе к блогингу. Здесь учат азам видео- и фотоконтента, помогают изучить работу журналиста и приобрести опыт написания сценариев.
Занятия проводят профессионалы в области медиасферы г. Череповца. Учебу в Медиашколе уже прошли 45 человек.
Кстати, среди агентов безопасности и выпускников первого потока Медиашколы есть ребята, которым посчастливилось этим летом побывать со специальной миссией в г. Москве. Они открыли для себя Центральный музей МВД России, взяли интервью у ветерана милиции, а также посетили «Лабораторию Касперского» — сняли специальный репортаж. (Об этом – на с. 30).

Несмотря на свою новизну, «АБ» стремительно набирает обороты и становится популярным. И нам очень радостно, что ты тоже с нами!

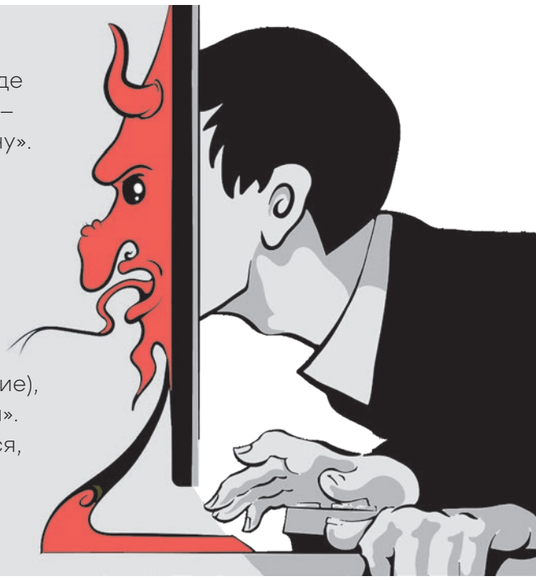
Управление «К» информирует и предостерегает

Как только появилась киберпреступность, в МВД России было создано Управление «К». Деятельность этого спецподразделения направлена на противодействие незаконным деяниям в сфере компьютерной информации. Чтобы обезопасить себя и своих близких от преступников, достаточно соблюдать несложные правила.
Наш эксперт – сотрудник отдела «К» Управления МВД России по Вологодской области (из-за специфики службы его имя не раскрываем).

Хулиганы в Интернете

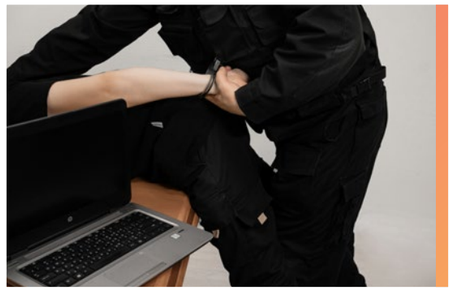
Их цель — испугать тебя, огорчить или заставить грубить в ответ.
Среди них есть интернет-вредители с преступными намерениями в отношении тебя лично или просто злые люди, которые сначала выходят за грань воспитанности, а затем и за грань закона.
Самый распространенный вид хулиганства в Сети — **троллинг**.
Это форма провокации или издевательства при общении в Интернете. Проявляется в возбуждении ссор, призыве к неблаговидным действиям, в сознательном обмане, клевете. Обычно такие хулиганы заинтересованы в узнаваемости и эпатаже.
Анонимность в Сети позволяет троллям представлять себя совершенно другими и быть уверенными в безнаказанности. Поэтому они пишут и делают то, что никогда бы не рискнули сотворить в присутствии оппонента. По причине своей недосягаемости им кажется забавным травить, оскорблять и провоцировать других. Причем, как показывает практика, больше половины сетевых грубиянов — дети, скучающие в Интернете или не ладящие со сверстниками.
Запомни простое правило: «кормить» троллей бессмысленно. Если ты заметил, что кто-то в Сети так себя ведет, можешь легко победить его: не обращай внимания. Ведь единственное, что ему нужно, — твоя реакция.
Гораздо опаснее — когда тебя начинают обижать твои знакомые. Особенно в ситуации коллективной травли. Но не стоит расстраиваться и замыкаться: многие из тех, кто в нее включается, лично против тебя ничего не имеют. По принципу «стадного инстинкта» они просто пошли на поводу у группы людей.
Но вот тебя начинают атаковать: требуют фото или персональные данные, угрожают, организуют коллективное преследование?
Это уже **кибербуллинг** — агрессивное преследование в сети Интернет, в том числе коллективное.
(От английского слова bull — бык: агрессивно нападать, задирать, провоцировать, донимать, терроризировать). В отличие от конфликта при травле жертва не в состоянии защитить себя.
В результате теряет уверенность, вплоть до психических отклонений и жестокой агрессии к хулиганам и даже ухода из жизни.
Здесь очень важно понимать, что это дело рук злоумышленников. Причем они травят безосновательно, поэтому нет причин для расстройства, снижения самооценки.
Как действовать в такой ситуации?
Не переживай в тайне от родителей. Обязательно сообщи им, родственникам или учителям и вместе примите решение обратиться в полицию. Храни информацию, подтверждающую факты нападений в Сети. Если для травли используют твои прошлые ошибки, проще сразу признаться в этом старшим, чем загонять проблему внутрь. Кроме того, не спеши выбрасывать свой негатив в киберпространство — создавай собственную онлайн-репутацию. И еще: сам никогда не допускай такого в коллективе и не принимай участие в травле других. Твое достойное поведение — главная защита и гарант спокойствия тебя и твоих близких!

Троллинг – в переводе с английского trolling – «ловля рыбы на блесну». То есть цель тролля – подбросить, скажем, в чате школы, класса или в чате по интересам, такую «наживку» (обидное слово, насмешка, оскорбление), чтобы ты ее «заглотил». А именно: расстроился, начал писать ругательства в ответ.



Злоумышленники в Сети

За последнее время преступления с использованием мессенджеров составляют большую часть от общей доли преступности. Это очень опасный уровень интернет-угроз, где цель — ты сам. Именно тебя виртуальный злодей хочет вовлечь в преступную деятельность.
Категорий этих мошенников достаточно много. Рекламируя солидный заработок по распространению наркотиков, запрашивая у тебя личные фото за большие деньги или требуя сфотографировать банковскую карту родителей, они нарушают закон. Все это — реально наказуемые деяния, и Интернет — лишь виртуальная рука, протягиваемая к тебе преступниками.
Большая часть детей, которые стали объектом такого виртуального насилия, не достигли 16 лет.
К сожалению, и среди тех, кто оступился и совершил преступление, есть несовершеннолетние.
Да, родители встают на их защиту, но в Интернете всегда остаются

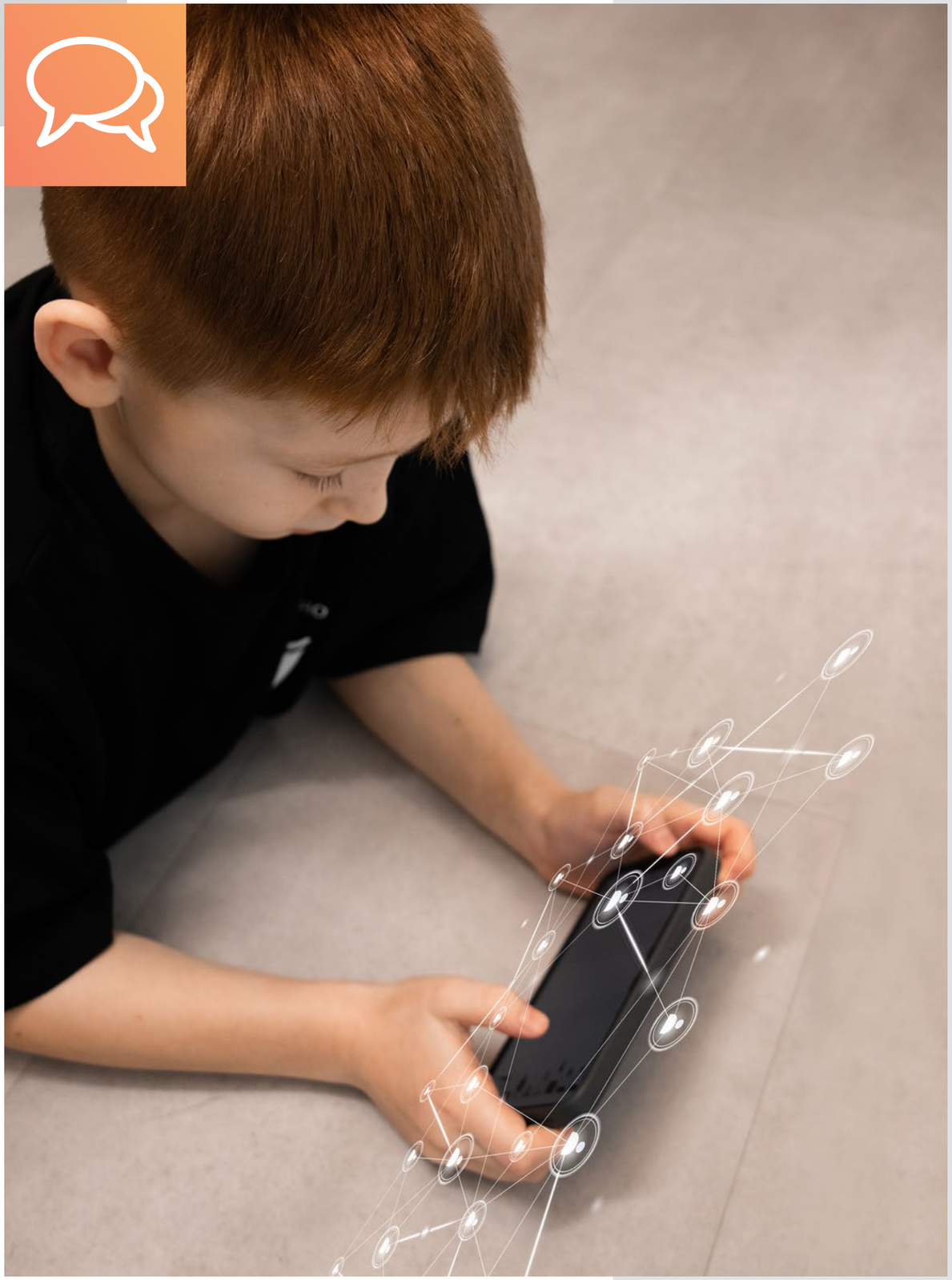


цифровые следы, по которым мы находим злоумышленника. Поэтому заниматься этим не советую.
Обращаю твое внимание на то, что в Российской Федерации установлен общий 16-летний возраст уголовной ответственности, а за отдельные преступления — с 14 лет.
Получить судимость в эти годы — собственными руками подписать приговор своему будущему.
Понятно, что в домашних условиях, с учетом возраста, любопытства и чувства безопасности, тебе легко вступать в разговоры на любые запретные темы. В том числе развращающего характера. Скажем, эфебофил (взрослый, который испытывает сексуальное влечение к детям), представляясь фотографом, вступает с тобой в переписку и, засыпая комплиментами, просит скинуть несколько твоих снимков. В том числе в обнаженном виде.
Прежде всего ты должен сообщить об этом родителям.
Набирает обороты одна из страшных угроз — **вовлечение в распространение наркотиков через соцсети**. Если ты увидел, скажем, объявление о том, что требуется курьер-разносчик писем с высокой зарплатой, знай: скорее всего, речь идет именно об этом.
К сожалению, подростки и даже их родители не до конца осознают всю полноту ответственности, которая может последовать.
А безнаказанными такие деяния не остаются! На первом этапе некоторые закладчики воспринимают происходящее как увлекательный квест.
Кстати, сами обычно наркотики не употребляют, многие даже из вполне благополучных семей.
А вот срок, который грозит им по статье за сбыт и распространение наркотиков, — 8–15 лет.
К слову, наркотики остаются в организме долго, и простой анализ покажет: употребляет их подросток или нет. Причем такая беда может коснуться и тебя лично. Поэтому, если знаешь о таких противоправных деяниях, которые совершают твои знакомые, расскажи об этом взрослым и вместе сообщите в полицию.

Еще злоумышленников можно встретить, когда что-либо **покупаешь в Сети**. Чтобы не попасться, запомни четыре правила. Во-первых, никогда не сообщай никому реквизиты пластиковых карт. (Особенно защищенными должны быть PIN-коды и CVV-коды на обороте карты).
Во-вторых, не переходи по ссылкам от незнакомых пользователей.
В-третьих, оформляй доставку только на официальном сайте.
В-четвертых, обсуждай сделку лишь во встроенном мессенджере этого сайта: чтобы обезопасить продажи, эти сервисы взаимодействуют с правоохранительными органами.
Ну и главное — родители должны быть в курсе всех твоих действий с онлайн-платежами. Они смогут быстро отменить ошибочный платеж, а в случае мошенничества — обратиться в полицию.
Приведу пример. Несовершенно-летняя девушка, проживающая в одном из районов Вологодской области, решила купить на известной торговой площадке в Интернете смартфон. Его стоимость была ниже, чем в обычном магазине.
Для этого она вступила в переписку в мессенджере внутри мобильного приложения этой площадки. После чего ей предложили продолжить общение в мессенджере WhatsApp и оплатить товар через переход по ссылке. Последовав совету, покупатель ввела данные банковской карты, с которой списали денежные средства. Причем...

дважды. В результате потерпевшая осталась и без телефона, и без денег. Но мы нашли мошенника. Он сознался в содеянном.
Этим количество угроз в Сети не ограничивается. Еще есть фишинг *(цель — получить доступ к конфиденциальным данным пользователей — ред.)*, распространение вредоносного программного обеспечения, кража личных данных, вымогательство

и масса других опасностей, которые угрожают тебе и которым также противодействует подразделение «К» УМВД.
(Об этом читай в материалах рубрики «Социальные сети» — ред.)
Подводя итог, попрошу тебя быть бдительным в Сети точно так же, как и в реальной жизни. Запомни: незнакомец — каждый, кого ты не знаешь лично. Поэтому не доверяй интернет-знакомствам и не жди, что преступник сразу покажет лицо. Подсказкой должно стать содержание первой же просьбы, предложения. Что-то насторожило? Прекрати общение — никаких дискуссий. Сними скриншот (снимок экрана компьютера или телефона, планшета, сделанный с помощью стандартных средств или специальной программы). Наконец, заблокируй собеседника и сообщи родителям об этом факте.



О правилах кибербезопасности и не только рассуждает наш эксперт **Сергей Тюкин**, заместитель начальника управления информационной безопасности Дирекции по экономической безопасности АО «Апатит» (выпускник первого потока по специальности «Информационная безопасность» Череповецкого государственного университета). Стаж работы в IT-сфере более 15 лет.

Социальные сети: зло или благо?

Сегодня трудно представить себе подростка да и взрослого, который бы не пользовался этим интернет-ресурсом. Он стал неотъемлемой частью нашей жизни. Ведь, по некоторым данным, основная часть общения переместилась в цифровое пространство. Итак, социальные сети… Что это: зло или благо?

Как появились социальные сети

Из соцсетей первым появился «Фейсбук» * — пользователи оценили. А далее, что называется, спрос родил предложение: по всему миру началось продвижение других площадок. В том числе «ВКонтакте». К слову, по интерфейсу *(оформление — ред.)* эта соцсеть первоначально очень напоминала ныне запрещенный «Фейсбук» *. Немного особняком еще недавно стояли мессенджеры, которые использовались для переписки. Сейчас обе эти группы сближаются и современные мессенджеры — тот же «Телеграм» — по сути, стали соцсетями. В них много характерных, к примеру, для «ВК», элементов: создание групп, каналов. В отличие от обычных сайтов, где контент *(содержимое — ред.)* наполняет администратор, в социальных сетях его создают сами пользователи.

** Признан экстремистской организацией и запрещен на территории РФ.*

В чем их особенность

Лично я пользуюсь этими площадками. Жаль, их не было, когда я учился в школе: они только зарождались во время моего студенчества. Главное — знать меру, чтобы цифровой мир, что называется, не заменил реальный, «не засосал» целиком, не сделал подростка зависимым. Поэтому, скорее, соцсети нужно воспринимать как дополнение к живым коммуникациям и возможность общаться с теми, кто далеко.

Основная особенность компьютерного мира — в том, что подросток не всегда знает, с кем общается. Ведь за фотографией-аватаркой может стоять кто угодно. Сегодня виртуальные знакомства набирают обороты, в друзья все чаще «стучатся» незнакомые люди. Есть случаи, когда соцсети используют педофилы. Они прикидываются ровесниками и напрашиваются на встречи. Нередко все заканчивается крайне плачевно…

Аккаунт, риски и безопасность

Аккаунт – это твой профиль, доступ к которому осуществляется по персональному логину и паролю. Поэтому все пользователи должны заботиться о том, чтобы их аккаунт не взломали. Ведь с этим связана масса рисков. Если злоумышленники — а это очень «изобретательные» личности — получат доступ к твоей страничке, то найдут массу способов, как получить от этого выгоду.

Самое простое — писать твоим друзьям и пытаться выпросить деньги. Далее, часто через соцсети пользователи передают сканы документов, которые уходят в Интернет. Хакер может покопаться во всем, что у вас есть, и найти, скажем, скан паспорта. А, имея его, через онлайн-приложение он легко

способен стать клиентом банка и получить деньги.

Продолжая общение от имени друга, попытается заразить чужие компьютеры, отправляя под видом интересной игры вредоносные файлы. Тот, к кому пришел такой файл, запускает его — после этого компьютер заражен. Начинает медленнее работать, греться; быстрее выходит из строя; мышь может самопроизвольно двигаться; появляются непонятные окна.

А еще пароли от привычных сайтов перестают подходить; с банковской карты пропадают деньги...

Если компьютер заразился вирусом, последний может похитить пароль: при его вводе он запомнит и отправит хакеру. Не стоит сохранять пароли в браузере — вирус также с легкостью выкрадет их. Притом все сразу.

Со мной однажды был такой случай. Институтский одногруппник написал: «Привет! Вступи, пожалуйста, в группу. Хочу ее раскрутить». Мне показалось это подозрительным, да и сама группа не внушила доверие и, вообще, относилась к другому городу. Поэтому я задал проверочный вопрос, на который «одногруппник», хоть и с небольшой паузой, но ответил правильно.

ЗЛОУМЫШЛЕННИК С ПОМОЩЬЮ ВРЕДОНОСНОЙ ПРОГРАММЫ МОЖЕТ ДЕЛАТЬ ВСЕ, ЧТО УГОДНО.

Во-первых, поискать данные банковских карт, доступ к интернет-банкам, чтобы вживую получить деньги.

Во-вторых, начать майнинг *(добыча — ред.)* криптовалюты.

В-третьих, использовать компьютер для сетевой атаки на сайты, чтобы вывести их из строя путем большого количества запросов.

В-четвертых, рассылать с компьютера спам *(вредоносные письма без согласия получателя — ред.)*. Поскольку таких отправителей часто блокируют, хакер вынужден искать другую жертву.

В-пятых, зашифровать компьютер и попросить за расшифровку выкуп, порой даже угрожая распространить компромат, обнаруженный на компьютере.

Кроме этого, злоумышленник может использовать чужой аккаунт для раскрутки групп в соцсети.

Я вступил в группу. Как потом оказалось, парня, действительно, взломали, а ответ на мой достаточно простой проверочный вопрос нашли, «порывшись» у меня на страничке.

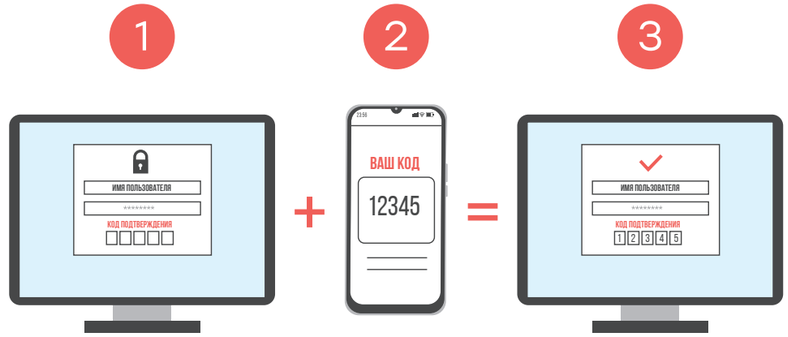
Другими словами, свой аккаунт необходимо защищать! И это относится к любым важным ресурсам Интернета.

Как похищают пароль

Злоумышленники похищают пароль прежде всего **через вредоносную программу**. Поэтому необходимо иметь антивирус и крайне осторожно относиться ко всему, что тебе присылают. Независимо откуда, каким образом и кто. Причем даже друзья: их могут взломать и от их имени отправлять вредоносные ссылки и файлы.

Далее — с помощью **фишинга**. Так сейчас называют атаки, основанные на подмене настоящих ресурсов очень похожими копиями. Это могут быть электронные письма или сайты, напоминающие соцсеть, а на самом деле созданные злоумышленником (скопированные шаблон и адрес чуть отличаются).

Когда ты вводишь свой аккаунт, фишинговый сайт его сохранит и, скорее всего, отправит на истинный сайт. Поэтому можешь и не заметить, что твои данные украли. Словом, и здесь нужно быть внимательным ко всему, что ты получаешь.



Лучшая защита – это двухфакторная аутентификация *(проверка подлинности — ред.)*. Особенность ее в том, что эта проверка подлинности использует два не связанных между собой способа: помимо пароля пользователя спрашивает что-то еще. Чаще всего — это код с СМС после верного ввода пароля.

Бывает сложнее: нужно установить специальное приложение, которое при каждом входе присылает уникальный код, или он может прийти в личных сообщениях в соцсети от специального робота. (Это бывает, когда ты хочешь зайти в свой профиль на новом устройстве). Процесс входа выглядит так. Вводишь свои логин и пароль — на телефон приходит СМС, push-уведомление *(всплывающее сообщение на экране компьютера, телефона — ред.)* от специального приложения или сообщение в соцсети с одноразовым кодом. Его нужно ввести в специальное поле. Этот простой шаг поможет тебе решить большое количество проблем. Дополнительный плюс — если тебе внезапно приходит такой код, это верный признак, что кто-то уже подобрал твой пароль и пытается преодолеть второй фактор. Стоит срочно принять меры!

Я лично пользуюсь этой настройкой для защиты аккаунтов в соцсетях и других важных сервисах: электронной почте, «Госуслугах» и т. п. Ее достаточно один раз установить, а именно: поставить галочку. Хотя и здесь необходим надежный пароль. Причем не словарный, не ассоциированный с твоей личностью.

Есть атаки вида перебор паролей, когда программа быстро подбирает разные, и, как только натыкается на верный, аккаунт взломан… Опять же если у пользователя нет двухфакторной аутентификации. При этом для всех ресурсов с ценной для тебя информацией используй отличающиеся пароли. Для незначительных допустим один, но сложный. А в идеале — везде применять разные (уникальные) пароли.

Таким образом, социальные сети — это ни хорошо и ни плохо — а данность современного общества. Поэтому тебе важно знать о возможных угрозах и следовать рекомендациям, о которых я рассказал. И этого будет достаточно в 99,9 % случаев.

Как запомнить сложный «ключ»

Это отдельное искусство. Во-первых, есть специальные программы для хранения паролей, где те содержатся в зашифрованном виде. Лично я использую их. Причем, сами пароли я даже в глаза не видел: каждый раз создается новый, состоящий из 20-ти случайных символов. Нужно только запомнить один сложный пароль для расшифровки общей базы паролей. Вот так массу секретов мы заменим одним, который проще запомнить. Разумеется, тебе необходимо обеспечить надежность хранения зашифрованного файла и следить, чтобы его не выкрали.

Второй вариант — придумать семейство паролей и логику их создания, изменения. К примеру, за основу брать фразы из песен (разумеется, не популярных и не тех которые ты постоянно напеваешь) или из стихов, а может, имена и фамилии любимых футболистов. После этого их нужно модифицировать, чтобы в составе паролей появились маленькие и большие буквы, цифры и спецсимволы.

Персональные данные — твое полное досье

В век стремительного развития цифровых технологий наши персональные данные все чаще становятся доступными для других. Неудивительно, что из всей этой информации в архивах социальных сетей, по сути, собраны целые досье на пользователей. Но если взрослые «фильтруют», какую личную информацию можно обнародовать, а какую не стоит, то подростки, не задумываясь, делятся в Сети всем подряд. Причем ее видят не только их друзья...

С точки зрения закона

Начнем с того, что 27 июля 2006 года был принят Федеральный закон от № 152-ФЗ «О персональных данных». Он направлен на «обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиту прав на неприкосновенность частной жизни, личную и семейную тайну». С точки зрения этого нормативно-правового акта к персональным денным относится любая информация, по которой можно установить личность конкретного человека. Это прежде всего фамилия, имя, отчество, паспортные данные, адрес, фото, а также номер телефона, электронная почта и т. п. Что касается подростков, то к их персональным данным относится информация из:

- свидетельства о рождении или паспорта (если ребенок старше 14 лет);
- личного дела школьника;
- классного журнала;
- медицинской карты;
- из документа о регистрации места жительства;
- фото ребенка.

...И не только

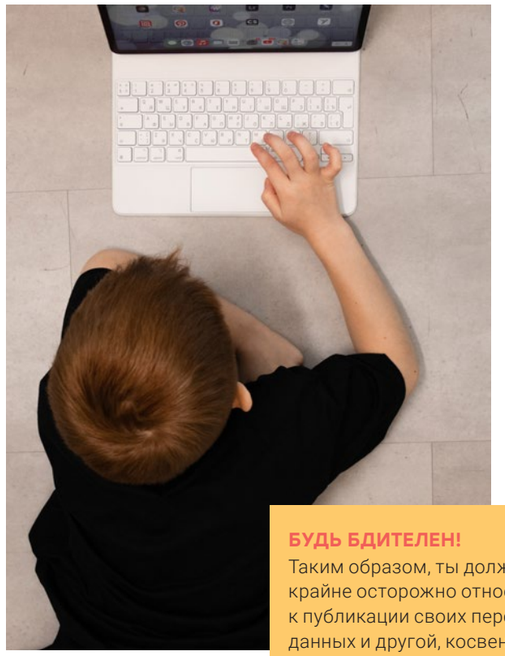
Но повредить тебе может размещение в соцсетях не только персональных данных. Взять, допустим, банальное фото, которое сделано рядом с твоим домом. Или снимок с видом из окна, особенно если оно выходит на какую-то достопримечательность. И тем более фото с табличкой с названием улицы и номером дома. Как ты понял, по этой косвенной информации злоумышленник без труда может вычислить, где ты живешь.
А иногда, особенно во время каникул, в погоне за лайками под своим постом подростки делятся планами на отдых, сопровождая их снимками ж/д- или авиабилетов. Таким образом, по сути, подсказывают, когда их не будет дома... И даже если дату отлета на билете кто-то из них позаботился закрыть, на нем есть штрих-код, по которому можно получить всю информацию: кто, когда и куда уезжает-улетает.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

(Из Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».)



Почему это может быть опасно?

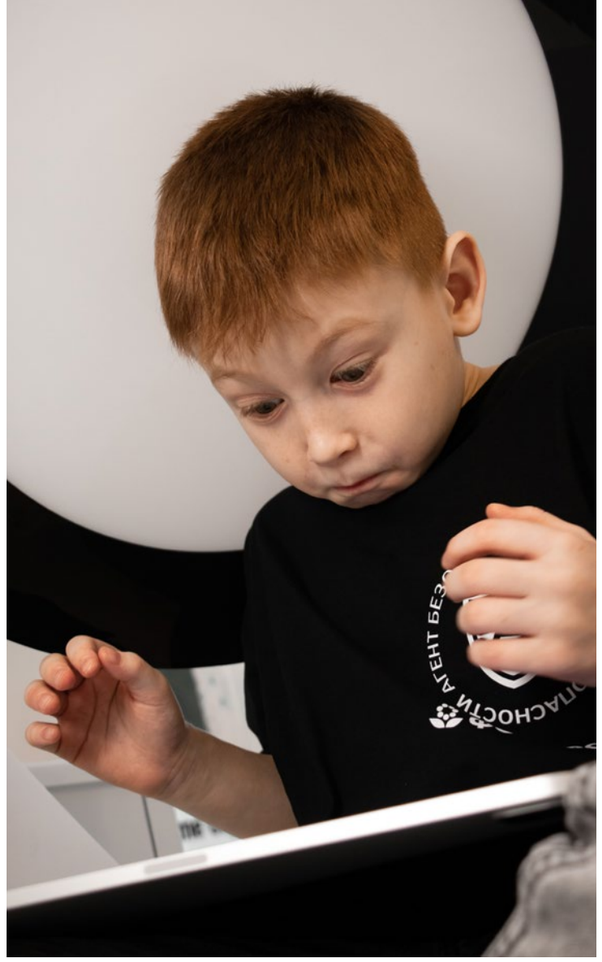
Есть люди, которые ищут такую информацию в Сети: они зарабатывают на этом. Хочешь поделиться о том, как ты с родителями замечательно отдохнул, и набрать побольше лайков под своим постом, лучше это сделать, когда вернешься домой. Дело в том, что последствия размещения информации в соцсетях выходят за пределы Интернета. Причем это не какая-то виртуальная атака, а, к примеру, живое ограбление. Допустим, если ты опубликовал свой адрес, злоумышленник без особого труда может «вычислить», что у твоих родителей дорогая машина, элитная квартира, и попытаться проникнуть в нее. Вообще не стоит публиковать ничего, что говорит о статусе семьи: фото с деньгами или новость о том, что папу назначили директором... Особенно важно избегать размещения информации о продолжительном отсутствии дома. Так, по статистике, опубликованной РИА «Новости» 1 июля 2022 года, квартиры более 20 % отпускников были ограблены, пока они отдыхали... Один из ярких примеров — ограбление дома актрисы Хилари Дафф в Беверли-Хилз. Угадай, откуда воры узнали об отсутствии хозяйки? Она сама опубликовала свое фото в отпуске в Канаде. Результат — из дома пропали все драгоценности, стоимость которых оценивается в сотни тысяч долларов.

БУДЬ БДИТЕЛЕН!

Таким образом, ты должен крайне осторожно относиться к публикации своих персональных данных и другой, косвенной информации, по которой можно идентифицировать твою личность. Да, что-то при желании можешь разместить, чтобы видели все. Другую информацию мы делаем доступной, скажем, только друзьям. И, наконец, определенные сведения ни под каким предлогом нельзя размещать в Сети. Это данные документов и все, что может о тебе рассказать. В том числе подобную информацию не стоит публиковать и для друзей: их могут взломать и под их учетной записью украсть у тебя информацию, чтобы воспользоваться ей в корыстных целях.
Запомни главное правило: каждый раз, делая пост, подумай: нет ли в нем информации, которая может помочь злоумышленнику навредить тебе и твоим близким.

Правда VS фейк

Как научиться проверять информацию



Все вокруг тебя можно назвать информацией. Ее очень много, она разная и при этом влияет на твои решения. Скажем, что ответить на вчерашний «выпад» одноклассника, как отреагировать на новости в Сети или какую книгу подарить любимому учителю на день рождения... Но главное – информация не существует без источника. Проблема в том, что в последнее время появляется все больше фейков, которых порой сложно отличить от правды.

Фейковые новости. Для чего их используют

Если говорить о фейках, то лично я по долгу службы чаще имею дело с фейковыми новостями, которые, по своей сути, искажают факты. Для чего они могут быть использованы? Прежде всего, с целью влияния на людей, в том числе на массы, управления их сознанием, поведением, принятием решений.

Хотя бывают и более приземленные мотивы. А именно: связанные с привлечением внимания и мошенничеством. Скажем, новости о сборе денег для определенного лица, проекта и т. д.

Есть много разных сценариев, используемых для завладения чужими средствами. Один из наиболее популярных связан с криптовалютой *(цифровая валюта, надежность которой построена на шифровании, а при проверке транзакций которой не участвуют банки. Она позволяет любому пользователю, в любом месте отправлять и получать платежи — ред.)*.

Как это работает

В социальной сети, чаще всего в «Твиттере», создается фейковый аккаунт, подделанный под аккаунты известной личности.

Под такие же аккаунты делаются и боты *(в данном случае — аккаунты в соцсети, которыми управляют программы-виртуальные роботы, выполняя за людей определенные задачи, — ред.)*. Они в большом количестве подписываются под созданный фейковый аккаунт, чтобы пользователи видели, что подписок много.

Далее, делается пост, к примеру, «Я раздаю криптовалюту, переведите мне 0,1 биткоина *(самая популярная криптовалюта — ред.)* — верну в два раза больше». Под ним боты сразу же пишут комментарий типа: «О, действительно, я перевел — все получилось!», «Мне вернулось, я заработал!» Люди заходят на такие аккаунты, смотрят, переводят деньги и, естественно, ничего не получают. А тем временем фейковая новость раскручивается, попадает в топы просмотров. Жертвы мошенников, конечно, могут написать комментарий, но те могут его удалить или он где-то затеряется. К сожалению, подобная схема развода на деньги процветает.

Другой сценарий использования фейков, даже куда в более глобальном масштабе, – влияние их на цены акций компаний. Допустим, когда выходит фейковая новость о том, что на одном из предприятий произошла авария с разрушением оборудования и потерпевшими. Как результат — цены акций могут упасть, а злоумышленники — приобрести их по более низкой цене, чтобы потом, когда она «поползет» вверх (мы же помним, что никакой аварии не было), выгодно продать их и, как следствие, на этом заработать.

А торговля акциями — игра с нулевой суммой: если злоумышленники заработали, значит, кто-то потерял деньги.

Так, однажды в телеграм-канале появилась новость от какого-то анонима о том, что одна из российских компаний решила отказаться выплачивать дивиденды. В подтверждение был приложен скриншот новости с сайта РБК. Причем ранее было известно о планах дивиденды выплатить. Как оказалось позднее, этот скриншот кто-то сделал в фотошопе. Таким образом, один канал пустил пулю, с него скопировали другие, и... понеслось. Курс акций начал «скакать» и, наверняка, на этом кто-то нажился. Ирония судьбы, но спустя полтора месяца эта компания все же отменила дивиденды и акции упали еще ниже. Но это — чистое совпадение и, вообще, уже совсем другая история...

Фейк (англ. fake – подделка) – фальшивка, обман, выдаваемые за достоверность с целью ввести в заблуждение. Он может быть чем угодно. Бывает фейковый аккаунт, но преимущественно это слово плотно вошло в нашу жизнь в связке со понятием «новость». Фейковые новости – намеренная дезинформация в социальных сетях и СМИ.

Отличай правду от фейка

Что касается правил, никаких суперсекретов здесь нет. Предлагаю придерживаться несложных принципов безопасного Интернета. Для этого просто ответь на следующие вопросы:

1. **Известен ли владелец источника информации?**
Не доверяй новостям в анонимных каналах, а также тем, которые ведут «любимые профессора из МГУ», «угарные преподы» и прочие безымянные или диванные эксперты.

2. **Что об этом событии пишет первоисточник?**
Если в новости есть ссылка на источник, постарайся найти новость на нем. При этом, к примеру, решение Центрального банка стоит проверить именно на официальном сайте ЦБ РФ и т. п.

3. **Если источник указан, надежен ли он?**
Наряду с авторитетными новостными сайтами (изданиями) есть «желтые» таблоиды *(небольшие газеты — ред.)*. Будь бдителен!

4. **Есть ли подтверждение или опровержение новости от официальных лиц (ведомств)?**
Обязательно проверь и это.

5. **Что пишут о новости другие серьезные ресурсы?**
Поищи новость на авторитетном, а не на анонимном ресурсе. Желательно найти не менее двух источников.

6. **Содержит ли новость призыв перепостить или переслать ее?**
Обычно цель автора — не проинформировать, а многократно размножить сообщение. Поэтому не предпринимай поспешных действий. В соответствии с российским законодательством, если ты сделал репост, это расценивается как твоя личная точка зрения. А значит, ты несешь ответственность за размещенную у себя информацию.

7. **Каким языком написано сообщение?**
Фейки чаще обращаются к эмоциям, вызывают чувства страха, паники, неуверенности и даже агрессии.

8. **Есть ли в твоем городе улицы, предприятия, организации, люди, о которых говорится в сообщении?**
Нередко фальшивки содержат обобщенную информацию, подходящую, казалось бы, для любого населенного пункта.

9. **Оригинальный ли снимок сопровождает новость?**
Как правило, размещенное фото не имеет никакого отношения к посту, поэтому может на других сайтах сопровождать абсолютно посторонние события.

Теперь ты знаешь, как отличить правду от фейка. Просто соблюдай эти несложные правила, и у тебя не будет никаких проблем!

Мошенничество в Интернете

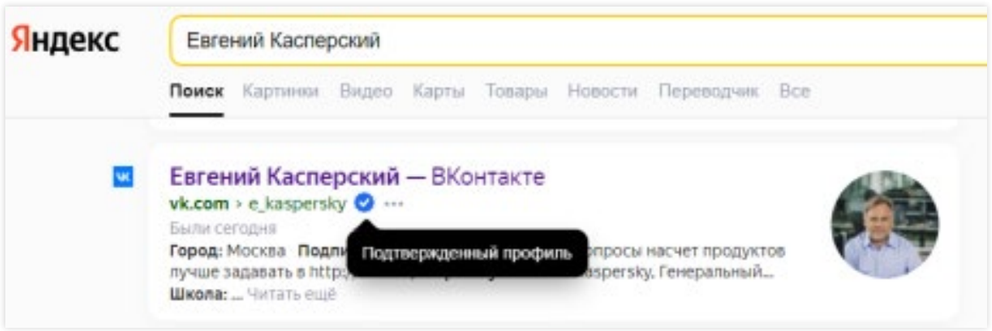
Чтобы не стать жертвой обмана

Сейчас все чаще можно слышать о мошенничестве в Интернете. Причем на удочку злоумышленников попадаются как подростки, так и взрослые. О чем это говорит? Прежде всего, об излишней доверчивости и отсутствии бдительности. Ведь, по сути, любой человек, с которым ты познакомился в Сети и вступил в переписку, может оказаться вымышленным персонажем.

Фейковый аккаунт

Задача мошенников — выйти на контакт с потенциальной жертвой. И самый простой путь, естественно, — через соцсети. Здесь возможны несколько вариантов.
Во-первых, когда хакеры создают выдуманные аккаунты, с которых начинают взаимодействовать с теми, кто представляет для них интерес. Управлять таким профилем могут как вручную, так и автоматически (с помощью программ) — тогда такие аккаунты называются «ботами».
Часто фейковые аккаунты достаточно легко определить: на них размещено чужое фото, а чаще — абстрактные изображения. Причем злоумышленники не сильно заморачиваются: даже на простой обман легко попадаются те, кто не задумывается о безопасности… Поэтому прежде всего обрати внимание на аватарку, количество друзей (если их подозрительно мало — это фейковый аккаунт), стену (как правило, она пустая или, наоборот, на ней куча репостов, но ничего личного). Что касается профиля, или визитной карточки, по которой можно идентифицировать человека, то он, разумеется, не заполнен.

Более того, сейчас практически у всех соцсетей есть возможность верификации *(проверка, подтверждение — ред.)* аккаунтов — в профиле известных лиц и известных агентств стоит галочка. Так, что сама интернет-площадка может убедиться в подлинности того, кто ведет тот или иной канал. Выглядит это везде примерно одинаково: синяя галочка или белая галочка на синем фоне. (Пример см. ниже).
К слову, даже «Яндекс» умеет отображать эту галочку в поисковой выдаче.



Что делать

Когда тебе пишет хозяин такого аккаунта, лучше сразу его заблокируй, поскольку это всегда злоумышленник. Если человек заявляет, что вы знакомы, не стесняйся и задай ему уточняющий вопрос. К примеру, когда и где конкретно вы могли видеться — так поймешь, с кем имеешь дело.
Если тебе отвечают, что «просто заинтересовала твоя страница, хочу смотреть, читать…», таких точно не надо добавлять в друзья! Можно оставить в подписчиках *(те, кто подписался на обновления личных аккаунтов в запрещенном сегодня в РФ «Фейсбуке» или «ВКонтакте», в «Одноклассниках», но не вошел в число друзей — ред.)*, они будут видеть общедоступную информацию. А в друзья, конечно, нужно добавлять тех, про кого ты понимаешь, кто они и зачем стоит общаться с ними. Кстати, и для друзей можно сделать разные группы и настроить для них «области видимости». Допустим, для близких друзей можешь дать доступ к большему количеству фото, а для остальных — только к избранным.
К сожалению, в последнее время количество друзей и количество лайков стало некой мерой значимости социального одобрения в подростковой среде и не только. Но все-таки лучше не рисковать и попытаться воздержаться от зависимости в эмоциональной поддержке виртуальным сообществом.

Аккаунт-клон

Второй вариант — создание аккаунта-клона реально существующего человека. То есть взята чужая фотография, имя, данные из профиля и даже список друзей — к ним начинает «стучаться» в друзья злоумышленник, который сделал этот клон.
Если напрашивается тот, кто у тебя уже есть в списке контактов, спроси, почему у него появился второй аккаунт. И делать это лучше по телефону: жулик легко придумает причину, а проверить ее через соцсеть может быть не так-то просто.

Мошенничество в сфере компьютерной информации наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо арестом на срок до четырех месяцев.

Из статьи 159.6. УК РФ. Мошенничество в сфере компьютерной информации.

Взлом аккаунтов

В-третьих, мошенники могут взломать аккаунт твоего знакомого и с его учетной записи начать с тобой общаться. На что стоит обратить внимание, когда тебе пишут друзья? Допустим, если просят перевести деньги или запустить игровой файл, то чаще всего это говорит о том, что их взломали. Набери номер телефона такого друга и спроси, действительно ли он в чем-то нуждается. Так в том числе ты подскажешь о случившемся, а он быстрее сможет что-то предпринять. К тому же меньше людей станет жертвой обмана, развода.

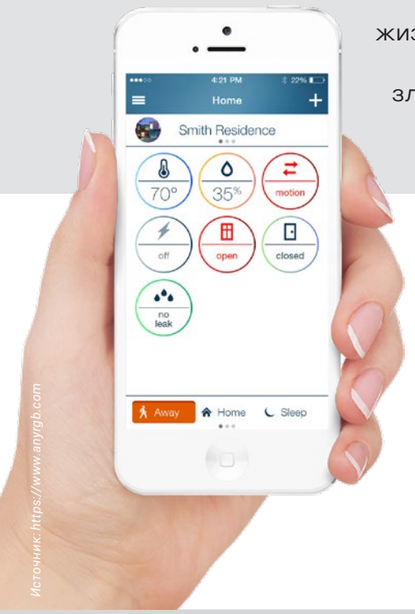
«Серега, ты…» или «Сергей, Вы…»

Зная манеру общения человека, достаточно легко можно вычислить, с кем на самом деле ты общаешься. Если, скажем, к тебе всегда обращались: «Серега», а сейчас называют «Сергей», или вдруг начали обращаться на «Вы» вместо привычного «ты», либо всегда писали грамотно, а тут начали делать ошибку на ошибке, — это должно насторожить. Лучше всего позвонить и спросить, все ли хорошо.
Отдельная темя — файлы, которые тебе присылают. Все обязательно проверяй антивирусом. Если «кидают» какую-то «классную полезную программу», не стоит ее запускать. Бесплатную ты легко и сам скачаешь с официального сайта, а платную — надо покупать. Ну а взломанную программу категорически не рекомендую использовать: тебе же дороже выйдет. Дело в том, что тот, кто производил взлом, запросто мог внедрить в нее вредоносное программное обеспечение. Поэтому или приобрети, или ищи аналоги.
Ссылки также проверяем. Если они ведут на внешний ресурс, лучше всего опять же перейти на них через поисковик — это к случаю, когда твоих друзей могут взломать злоумышленники и начать общаться от их имени.
Итак, делаем вывод. На обращения сомнительных личностей не отвечай, забанивай *(блокируй — ред.)* их. Можно нажать кнопку «пожаловаться». Если склоняешься к тому, что это реальный человек и он может быть тебе интересен, подумай, чем именно, и прими решение: добавить в друзья или оставить в подписчиках — по принципу достаточного основания, согласно которому все должно иметь причину. Что касается друзей, будь внимателен и следи за тем, не изменился ли стиль вашего общения. А на просьбы всегда лучше реагировать, проверяя ситуацию вживую. Например, с помощью звонка по телефону. Ну и, наконец, контролируй ссылки и файлы, которые получаешь. Присылаемые тебе программы не запускай.

Мобильные приложения

Где таится угроза и как себя обезопасить

Мобильные приложения (МП) прочно заняли свое место в твоей жизни. Но есть среди них такие, которые могут собирать твои личные данные, прослушивать разговоры, воровать деньги и отправлять злоумышленникам... Проблема в том, что многие пользователи, сами того не понимая, скачивают опасные приложения на телефон. Разберемся, где таится угроза и как себя обезопасить.



Источник: https://www.anygb.com

Мобильное приложение – это программное приложение для работы на телефоне, планшете, часах и других мобильных устройствах. Его назначение может быть самым разнообразным: развлечения, сервисы, магазины, онлайн-помощники и т. д. Многие МП при покупке устройства уже установлены производителем.

Типы мобильных приложений

Среди них есть те, которые предназначены для развлечений, общения, покупок. Также бывают финансовые, справочные и офисные МП.

К развлекательным можно отнести игры, онлайн-кинотеатры, электронные книги и т. п.

О приложениях для общения мы упоминали в предыдущих статьях: это социальные сети, мессендежеры, а также приложения для работы с электронной почтой, для проведения онлайн-конференций и др.

Большинство магазинов приложений *(интернет-магазины, где клиенты могут приобретать и загружать программные приложения, — ред.)* сейчас имеют свое МП, в котором предусмотрен и твой личный кабинет с дисконтной картой, историей заказов и каталогом товаров. К слову, последние ты можешь забронировать или даже заказать с доставкой (зависит от магазина). В эту же категорию попадают и приложения маркетплейсов *(торговые площадки, которые продают товары и услуги разных продавцов через Интернет, — ред.)* «Ozon», «Wildberries», «Яндекс. Маркет» и т. п.

К финансовым МП относятся приложения банков, страховых компаний и платежных систем.

К справочным — энциклопедии, словари и базы данных с возможностью поиска.

Офисные приложения включают в себя записные книжки, таск-менеджеры *(программы для управления проектами — ред.)*, в которых удобно записывать свои задачи, планы, цели, также программы для работы с текстом, графикой и видео.

МП и телефон

Для решения всех этих задач уже есть обычные веб-сайты. Но из-за скромных размеров мобильников пользоваться ими не так удобно. Вот поэтому МП и получили такое распространение. Таким образом, по сути, МП — это адаптированная форма предоставления уже известных тебе сервисов.

Взять те же «Вотсап», «Телеграм» и «ВКонтакте» – на мобильном телефоне ты почти всегда используешь эти приложения.

Можно, конечно, эти и прочие МП открыть через браузер *(приложение для загрузки и просмотра страниц, скачивания файлов, управления приложениями — ред.)*, как это делаешь на компьютере, но это будет крайне сомнительное удовольствие.

В результате развитие современных телефонов пошло так, что, купив новый мобильный, ты получаешь сразу массу установленных приложений. Какими-то из них будешь пользоваться, а какие-то, возможно, тебе и не понадобятся. Хотя удалить сможешь не все: некоторые жестко «зашиты».

Магазин приложений

Но никто тебя не ограничивает набором приложений, который «идет» вместе с телефоном. Ты запросто можешь установить сам все, что тебе нужно, через магазин приложений (он есть для всех современных телефонов). Для iPhone — это AppStore, для Android — Google Play. У определенных моделей, скажем, Huawei, имеются свои магазины МП. Из таких стандартных магазинов, как правило, устанавливать МП безопасно. Правда, здесь есть одно «но» — к нему вернемся позже. Сегодня ввиду сложившейся геополитической ситуации уже появился русскоязычный магазин МП. К слову, он будет установлен принудительно на всех мобильных телефонах — без него в России продавать телефоны запретят.

Основной источник заражения

— это приложения, скачанные не через магазин, а через браузер. Зачастую хакеры подделывают вредоносные программы под наиболее популярные приложения. Например, не так давно российские антивирусные эксперты обнаружили более тысячи вредоносов, притворявшихся популярным приложением для знакомств. Поэтому нельзя устанавливать МП по какой-то ссылке. Речь идет как о тех, что тебе прислали, так и о тех, которые ты сам нашел.

В принципе, есть техническая возможность скачать из Интернета файл-приложение и установить его. Между тем так делать нельзя. Ведь ты никогда не знаешь, что внутри его. К тому же у честного разработчика МП нет причин распространять свое приложение именно через такие файлы, вместо публикации его в магазине приложений.

Объясню почему.

Во-первых, разработчикам МП самим выгодно распространять их именно через магазин приложений: так владельцы телефонов легко могут найти приложение, поставить ему оценку или написать лестный комментарий. Во-вторых, все МП проходят проверку со стороны Google *(крупнейшая поисковая система — ред.)* для телефонов систем Android либо Apple *(производитель компьютеров, аудиоплееров, смартфонов, программного обеспечения и цифрового контента — ред.)* для смартфонов iPhone.

Таким образом владельцы обеих компаний (Google и Apple) выявляют нештатный функционал: будь то кража твоих данных, навязчивая реклама или самые настоящие вирусы для телефона.

Риск должен быть оправдан

Несмотря на то, что МП в магазинах приложений проходят проверку, вредоносные приложения в них могут просочиться — такие случаи нечасто, но встречаются. Поэтому не стоит, не глядя, устанавливать все подряд. Руководствуйся правилом: чем популярнее приложение, тем меньше вероятность того, что там будет что-то плохое. Если, скажем, ты откроешь «ВК», у которого миллион установок, в нем практически наверняка не обнаружишь ничего вредоносного. А вот у МП, которое скачали 10 человек, вероятность риска значительно больше. Даже если оно находится в официальном магазине мобильных приложений.

Что еще важно помнить при установке МП? На экране всегда появляется список функций, к которым оно просит доступ: к изображению с камеры телефона, к осуществлению звонков, чтению СМС, геолокации, внутренней памяти и т. д. Тебе при этом важно соотнести то, что ты загружаешь, с тем, что запрашивает МП.

Если, скажем, устанавливаешь игру, а она просит доступ к твоей геолокации, будет справедливым вопрос: зачем. Прежде всего, такой критичный подход станет однозначным поводом не дать излишнего доступа потенциальным злоумышленникам к твоим данным.

К тому же – серьезной причиной отказаться от установки такого МП. Злоумышленники могут собирать личную информацию, чтобы использовать ее в разных целях. Как в легальных: допустим, чтобы сделать на человека таргетированную рекламу *(онлайн-реклама, направленная на поиск целевой аудитории, которая может интересоваться рекламируемым товаром или услугой, — ред.)*. Так и в нелегальных: произвести на тебя компьютерную атаку, украсть твои данные и попытаться продать или потребовать с тебя выкуп.

Есть и более безобидные варианты «нехороших» приложений: они могут накручивать счетчики голосований или посещения сайтов. Такие случаи встречаются, но эти приложения обычно достаточно быстро выявляются и удаляются из магазинов приложений до того, как их установит большое количество людей.

ИЗ ИСТОРИИ

Отправной точкой для создания МП считается появление в 1990-е гг. на мобильном телефоне экрана. Это были уже встроенные производителем небольшие аркадные игры (компьютерные, с примитивным игровым процессом – ред.), редакторы рингтонов (мелодии для звонков – ред.), календари, калькуляторы и др.

Лишнее ни к чему

Поэтому перед установкой МП, во-первых, хорошо подумай, нужно ли тебе это приложение. Во-вторых, изучи карточку приложения, количество скачиваний, лайков, отзывов. В-третьих, – если решил установить — посмотри, какие оно запрашивает права. В-четвертых, после установки не забывай его обновлять: в приложениях встречаются уязвимости, которые могут использовать злоумышленники. А слабые места по недосмотру разработчиков оказываются во всех подобных продуктах. Обнаружив их, разработчик, чтобы закрыть проблему, выпускает обновление. И, в-пятых, если приложением не пользуешься, не забывай удалять: лишнее — ни к чему.

Что касается прав, которые запрашивает МП, их перечень всегда можешь найти в настройках телефона. Этот пункт обычно называется «Права приложения». Здесь увидишь, какое МП и к чему имеет доступ. Более того, можешь сам отрегулировать эти доступы. Скажем, запретить их к геолокации или камере телефона.

Таким образом, советую тебе периодически проводить ревизию твоих приложений. Неиспользуемые — удалять, а нужные — обновлять и оставлять им только необходимые разрешения.

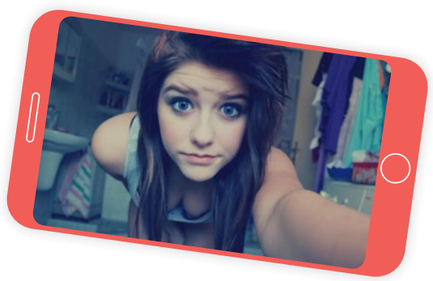
Опасное селфи

Лайк или жизнь?

Источник: https://pixy.org/

Ты делаешь селфи каждый день и размещаешь в соцсетях? Ждешь оценку и переживаешь при неудачном снимке?
Захватившее весь мир увлечение давно перекочевало в криминальные хроники: только в России при попытке сделать эффектный кадр ежегодно гибнут десятки подростков...

Наш эксперт – заведующий детским отделением Вологодского областного психоневрологического диспансера № 1 **Юрий Афанасьев** дает этому профессиональную оценку и предостерегает от беды.



Мерило любви

Селфи в переводе с английского (self — сам, себя) — фотосъемка самого себя с помощью современных гаджетов. Цель — выложить в соцсети и показать, как ты выглядишь, где находишься. Причем никто в этом опасности не видит. Но особенность современного цифрового и главное — информационного мира в том, что многие явления могут уходит в деструктивное, разрушительное русло.
Пример из практики. Иду мимо отделения, вижу: сидит девчонка 12–13 лет и бубнит себе под нос: «Сорок... Сорок... Меня никто не любит...» Спрашиваю: «Что сорок?» «У меня под сегодняшним селфи только сорок лайков, — отвечает бедняжка. — А вчера было 210. Значит, я неудачно сделала селфи».
Здесь мы имеем дело с двумя явлениями: публичность интернет-пространства и поощрение, которое в нем получаем. По сути говоря, речь идет о самопрезентации, или «себяшке».

Для кого? Для чего?

Во время занятий я задаю детям вопрос: «А для кого ты делаешь селфи?» И все заявляют: «Для себя». Но если так, зачем выкладывать в публичное пространство? На мое предложение подумать, они сначала впадают в ступор...
Поэтому ты должен понять, что, во-первых, делаешь это для кого-то, во-вторых — для поощрения (социального или психологического).
В чем оно выражается?
В лайках и репостах.
Словом, есть мотив *(побуждение к действию — ред.)* и, как правило, его психологическая награда.
Мотивом может стать раскрутка себя, популяризация любимого дела и даже удовлетворение нарцисстических особенностей *(завышенное мнение о себе — ред.)*.
Что касается награды, здесь кроется опасность: в виде лайка ты начинаешь получать некий суррогат внимания, одобрения. То есть механизм компенсации этой потребности. Где его взять? Самое простое — уход в Интернет или подростковую группу. Причем большинство создают собственную страничку или аккаунт *(учетная запись пользователя — ред.)* в соцсети или на канале YouTube для самопродвижения.

Опасность Интернета

Ты должен знать не только, как правильно делать селфи, но и что ты транслируешь? Ведь одни подростки настроены на создание позитивного контента, другие — треш-контента *(в переводе с английского trash content — мусор, отходы — ред.)*. Именно на чем-то плохом, выходящем за нормы привычного, к сожалению, чаще всего можно набрать лайки и репосты. Проще говоря, снимая цветочки, много не заработаешь, в отличие от прыжков, залезания на вышки, общения с опасными животными и т. п. Здесь накладывается одна из опасностей — коммерционализация Интернета *(деятельность, направленная на извлечение прибыли, — ред.)*.
Как известно, существует тренд так называемых детских блогеров. Каждый считает, что может создать свой контент, особенно в приложении TikTok, на сервисе YouTube; собрать свою многомиллионную аудиторию и зарабатывать на этом деньги.
Так психология ложится на финансовый мотив.
Но снимать длительный позитивный научный контент не интересно. Дети уходят в треш-блогерство. А это как раз и есть опасные для жизни занятия.

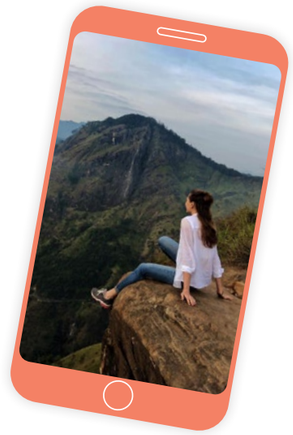
> Представление о собственном «я» – психологическое понятие.
> Оно подразумевает, что мы видим себя не теми, кто мы есть, а теми, кем нас, на наш взгляд, видят другие.

Руферы и зацеперы

Первые из них снимались на крышах высоких зданий и вышках. Вторые — на крышах и на подножках вагонов электричек, поездов, между вагонами.
Те и другие нередко погибали. По сути, это были представители субкультур, которые провоцировали подростков к совершению опасных движений, действий.
Новички, создавая подобный контент, пытались переплюнуть своих предшественников. Так, в 2015 году в Вологде 17-летний подросток, моделируя во время съемки падение, сорвался с 9-го этажа. В 2021-м и тоже в Вологде погиб 13-летний парень. Причина — сильнейший удар током на крыше поезда на станции «Вологда-2». Кроме 70 % ожогов тела, при падении на землю он получил множественные переломы.
Государство жестко отреагировало на подобные инциденты. Вышло постановление Правительства РФ от 8 октября 2020 г. № 1633 «Об утверждении требований по обеспечению транспортной безопасности…». В нем впервые были выработаны критерии противоправных действий — стало возможным привлекать экстремалов к ответственности. Причем не только за участие в селфи, но и за их распространение в соцсетях.

Треш-стримы, хэппи слэпинг…

Еще лет пять-шесть назад треш-контент в Интернете без ужаса смотреть было невозможно. Жестокость детей зашкаливала. Чего стоит увлечение хэппи слэпингом (в переводе с англ. — счастливое издевательство)! Оно же — групповое нападение и избиение на мобильный телефон! Затем пошли треш-стримы — онлайн трансляции, участники которых готовы за пожертвование унижать, избивать, спаивать специально приглашенных.
Проблема приобрела массовый характер. Неслучайно были приняты законы, определяющие, что включает в себя противоправный контент. Кроме тех направлений, которые я назвал, он также предусматривает размещение на страницах в соцсетях фото с треш-контентом.
Это расценивается как пропаганда опасных форм поведения для жизни. Кроме того, МВД России разработало специальную памятку «Делай безопасные селфи. Крутое селфи может стоить тебе жизни».
В свою очередь, МЧС рекомендует придерживаться пяти принципов безопасного селфи. Один из них — убедись, что находишься на безопасном расстоянии от движущегося транспорта, хищников и проводов под напряжением.



Челлендж

К селфи присоединилась монетизация. Самая экстремальная для жизни такая акция — челлендж (от англ. challenge — бросить вызов). Это интернет-ролик, где блогер за бонусы выполняет задание и размещает его в Сети, а затем предлагает детям повторить и продолжить. И они ведутся на это… Соответственно, челлендж может быть как позитивный (к примеру, сбор денег на операцию), так и деструктивный — опасный для жизни.
Но привлечь внимание может и неосознанный треш. Например, фото на фоне змеи или проезжающего поезда… Не понимая степени опасности, ты захочешь поэкспериментировать, подойти поближе. А чем грозит, скажем, съемка на фоне движущихся железнодорожных вагонов? «Пролетающая» на высокой скорости электричка волной воздуха может затянуть под них. А снимки в распахнутом окне? Стоящий на подоконнике не чувствует, что сзади него, — оступившись, рискует выпасть на улицу.

Твоя безопасность и будущее – в твоих руках!

На встречах с подростками специалисты нашего Центра информационной безопасности в сети Интернет «Защита», который я возглавляю, не запрещают — рассказывают. Во-первых, что такое селфи опасно для здоровья. Во-вторых, что теперь это расценивается как противоправный контент. И, если ты его размещаешь на своей странице, это может привести к имиджевым потерям: проблемам при поступлении в вуз, трудоустройстве и т. п.
Словом, ты должен понимать, чем это опасно и для чего это делаешь (желательно с родителями, которые также должны просматривать твои аккаунты).
Наконец, что тебе дороже: лайки или жизнь? Лайки ты не почувствуешь, а сломанную руку с госпитализацией — еще как!
Помни: твоя значимость определяется не количеством лайков, а полезными поступками. В реальной жизни есть те, кто тебя любит, принимает и поддерживает. Интернет — лишь дополнительный ресурс для общения. А значит, твоя безопасность и твое будущее — в твоих руках!

Кто приносит самую большую прибыль

В шестом классе он увидел по телевизору компьютер и влюбился в него. А когда узнал, что в школе появился компьютерный класс, куда пускали только десятиклассников, не стал ждать целых три года. Семиклассником уже практически обслуживал весь кабинет. А с восьмого стал основным техником. Неудивительно, что будущую профессию юноша связал с хобби: поступил в колледж (сейчас Кировский филиал Мурманского арктического госуниверситета), где с первого курса ремонтировал компьютеры, сети, потом стал писать программы… Наконец, в 2006 году закончил Петрозаводский госуниверситет по специальности «Электропривод и автоматика промышленных установок и технологических комплексов».

Знакомьтесь: **Сергей Диденко**, директор по информационным технологиям АО «Апатит».

Сергей, Ваша профессия связана с IT-сферой, которая сегодня переживает бурное развитие. Без программистов невозможно себе представить ни одну отрасль экономики...

Это, действительно, так. Хотя в 2017 году председатель правления «Сбербанка России» Герман Греф заявил, что айтишники не востребованы и не стоит всем гнаться за этой профессией. Сравнил их с инженерами, юристами и экономистами, чьи профессии были «модными», но не обеспечивали успешного трудоустройства. Правда, жизнь доказала другое: многие перевели свой бизнес в Интернет, появились новые задачи и направления развития IT. Если говорить о профессиях будущего ФосАгро, я убежден, что в нашей сфере прежде всего сохранятся те, которые пользуются спросом сегодня. Это программисты, сетевые администраторы, администраторы баз данных и др. И не важно, будет ПК стоять на столе, парить в воздухе или… зашит в мозг в виде капсулы.

Какие из них, на Ваш взгляд, наиболее перспективны?

С появлением новых направлений появились профессии, которые сейчас крайне востребованы, а тем более будут таковыми в ближайшие десятилетия. Прежде всего это специалисты по разработке и обучению нейронных сетей, аналитики данных — управляют данными и выполняют их анализ. Мир стал цифровым. Так, каждый человек в среднем генерирует *(собирает и передает — ред.)* в день около 500 Мегабайт информации. Ее огромные потоки накапливаются, растут. Рассмотрим на примере производственного процесса. Допустим, в какой-то момент он стал идти с отклонениями от норм технологического режима, а разобраться в причине никто не может. В то же время, если проанализировать, скажем, не 10 параметров, которые фиксирует оборудование, а сотню или тысячу, то может оказаться, что сказывается какой-нибудь, на первый взгляд, вторичный фактор типа атмосферного давления или влажности воздуха…

А если рассмотреть более упрощенно?

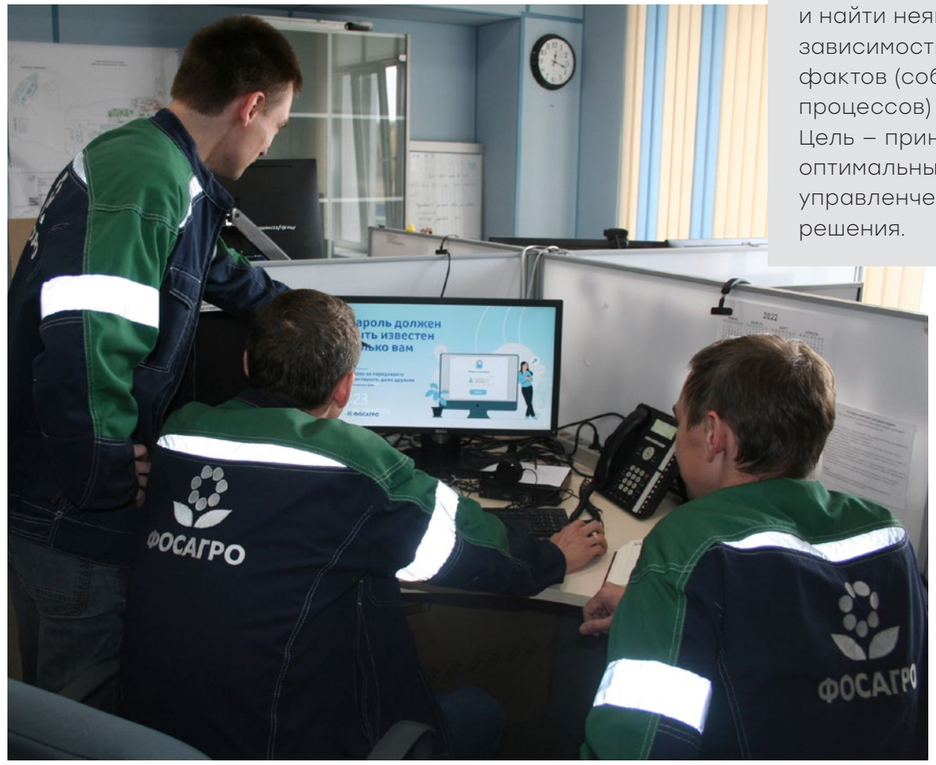
Как думаете, отчего, к примеру, зависит количество посетителей магазина. С одной стороны, это правильная клиентская сегментация рынка, хорошее расположение, большой ассортимент, низкие цены на товары. Но при анализе необходимо также учитывать изменение покупательской способности, расстояние от магазина до дома покупателя, погодные и климатические условия, даты праздников (в том числе и личных), рабочие графики взрослых покупателей и еще сотни параметров. Понятно, что, не обладая специальными знаниями как в области анализа данных, так и самого бизнеса провести качественный анализ невозможно. При стремительном развитии этого направления количество подготовленных специалистов крайне ограничено. Достаточно сказать, что заработная плата выпускника вуза по этому направлению на рабочем месте может «стартовать» от 150–200 тыс. рублей. Верхней границы в зарплатной «вилке» таких специалистов практически нет. В том числе они работают и у нас, в «Инжиниринговом центре ФосАгро».

Расскажите о требованиях, которые работодатель предъявляет к аналитику Big Data?

Это должен быть не просто технарь, преуспевающий в точных науках, а специалист с особым мышлением. Поэтому в числе основных базовых требований — аналитический склад ума и хороший математический аппарат *(знание набора формул, условий, соотношений, с помощью которых решается задача, — ред.)*, глубокое понимание методов обработки и анализа данных.

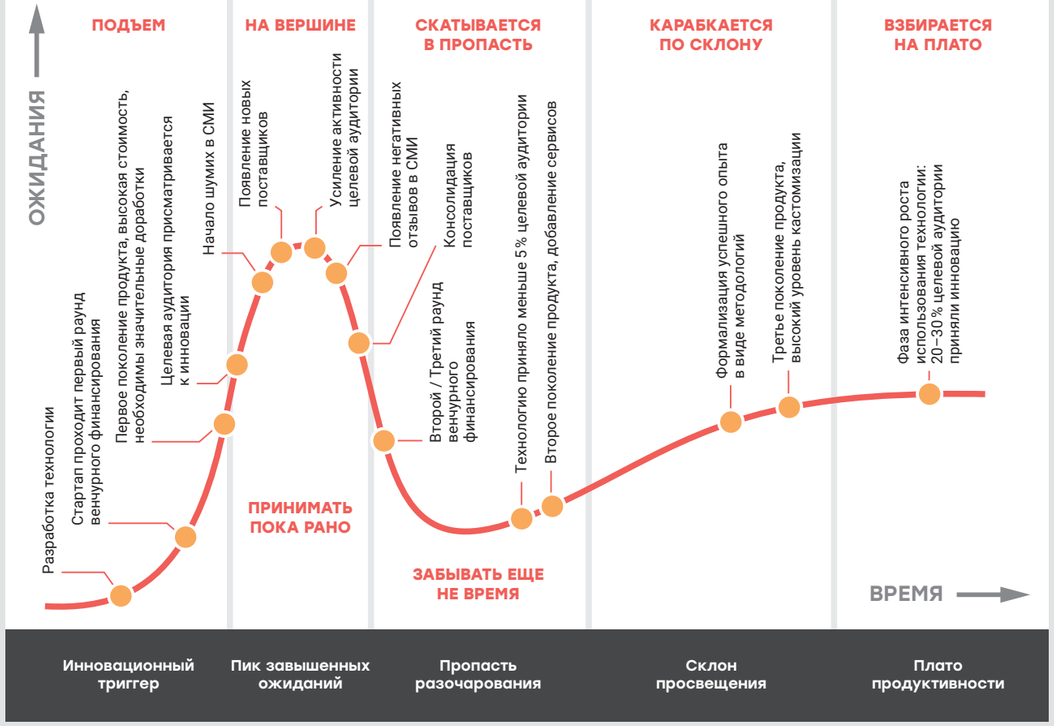
А в чем состоит принцип его работы?

Скажем, у тебя есть набор механизмов, которые дают



Аналитик Big Data – специалист по обработке объемных массивов данных. Его задача – извлечь из данных, которыми он располагает, самое ценное и найти неявные зависимости одних фактов (событий, процессов) от других. Цель – принять оптимальные управленческие решения.

возможность из имеющихся данных построить необходимые отчеты. Те позволяют или предсказать, как пойдет определенный процесс дальше, или проанализировать и найти некие зависимости фактов для приятия решений. Наконец, ты можешь оптимизировать какой-то процесс, который другой человек порой не способен даже увидеть. Так, один из свежих проектов, в реализации которого в 2022 году участвуют наши специалисты, связан с шаровыми мельницами на Апатито-нефелиновой обогатительной фабрике-3 (Кировский филиал АО «Апатит»). Поясню: мельница представляет собой крупное цилиндрическое устройство для измельчения руды. Внутрь загружаются дробленая руда и помольные металлические шары. На оборудовании мельницы установлены датчики вибродиагностики — они снимают информацию о вибрации с нескольких точек. По этим данным можно предположить, насколько качественно загружена мельница. А также когда, с учетом ее технических показателей, она выйдет из строя и какой именно механизм. Чтобы узнать это, специалисты разрабатывают математическую модель процесса, анализируют накопленную информацию с датчиков, разрабатывают и обучают нейронную сеть находить скрытые зависимости между малозаметными изменениями в сотнях параметров и результатах производства. Только после получения достаточно высоких оценок качества предсказания (точность более 90–95 %) «нейронку» перенастраивают для анализа текущих показателей. Система начинает на лету анализировать данные с датчиков и предупреждать персонал о том, что может произойти через несколько часов или даже дней. Производственники заранее знают не только, что конкретно выйдет из строя, но и каким запасом времени они располагают для подготовки ремонта. Вот так аналитики данных и инженеры по разработке нейронных сетей помогают предсказывать будущее… Причем работа эта — не только полезная, но еще и очень интересная.



Источник: https://blog.bitobe.ru/article/krivaya-gartnera/?ysclid=la8jd3x4v5100585800

А как все начиналось в этой профессии?

Мы перешли от эпохи автоматизации процессов обработки информации к эпохе получения за счет ее глубокого анализа дополнительной пользы. Поскольку для массового рынка. Так незаметно и очень быстро мы перешли в эпоху цифровизации.

Кстати, при цифровизации Компании «ФосАгро» подбор аналитиков данных был первой и довольно сложной задачей. А сейчас эта профессия — одна из тех, которые начинают приносить достаточно весомую пользу.

В условиях, когда мир меняется с сумасшедшей скоростью и становится все более жестким, требования к бизнесу и производству очень высокие… Новые инновационные технологии достаточно быстро выходят на рынок. Если, к примеру, автомобиль как инновация или то же самое электричество входили в нашу жизнь десятилетиями, то смартфоны захватили мир за 5–7 лет. Стремительно проникли в нее соцсети, «интернет вещей», умные устройства, облачные сервисы.

В этой связи представляет интерес график появления новых технологий от исследовательской компании Гартнер, которая специализируется на IT-рынках. В чем его суть?

График называется Gartner Hype Cycle. На нем видно, какие технологии сейчас появляются на рынке, какие опробованы и востребованы, а какие уже приносят пользу.

Давайте посмотрим, что происходит. Появляется новая технология, она быстро приходит на рынок, о ней много пишут. Богатые компании вкладывают серьезные средства в ее доработку и внедрение. Через некоторое время заказчики новой технологии оценивают результат и видят: не все удалось реализовать, практический или экономический эффект недостаточны. Налицо спад интереса к ней. И только после доработки и адаптации происходит полноценный продуктивный выход на рынок…

Весь этот цикл инновационная технология проходит в среднем за 5–10 лет. Но некоторым времени требуется больше. К примеру, автономный беспилотный транспорт. Сложно представить себе, как сильно изменится мир, где машины станут ездить без водителя. Это будет напоминать общество после изобретения машины. Как в начале прошлого века исчезла профессия кучера, так исчезнут и таксисты. Их услуги станут дешевле и доступнее — значит, больше людей смогут быстро перемещаться по городу. Изменятся транспортные схемы городов, появятся специальные стоянки, автоматизированные зарядные станции, роботизированные автомойки… Все это могло бы произойти уже сейчас: техническая часть беспилотных машин давно разработана, протестирована и практически готова.

Как и программное обеспечение. Машины самостоятельно проехали уже миллионы километров по обычным дорогам, магистралям и дворам. Но возникли проблемы юридического плана. Кто будет отвечать, если произойдет авария? Обычно в ДТП виновным признают владельца транспортного средства или водителя. Но здесь человек не может повлиять на происходящее. Может вину надо будет возложить на разработчика машины? В общем, вопросов пока много, поэтому диаграмма отводит на полноценное внедрение данной технологии еще как минимум 10 лет…

Ваш совет тем, кто решил выбрать профессию аналитика данных: как стать профессионалом?

Главное — любить дело, которое выбрал. А еще постоянно развиваться, обучаться и иметь огромный объем практики.

Причем ты должен полюбить не только информационные технологии. Важно получать удовольствие от познания нового, от космического объема информации, от постоянного общения.

Идти в IT-сферу за большими зарплатами бессмысленно. Высокий уровень дохода — это следствие перечисленного выше, а не данность. Но пройти путь от «джуна» *(джуниор — начинающий программист — ред.)* до «сеньора» *(программист, который может все, — ред.)* — не только сложно, но и очень интересно. Ведь IT достаточно быстро развиваются, и ты должен уметь и хотеть меняться вместе с ними. В этом, вероятно, и кроется основной секрет профессионализма: меняйся сам и меняй мир к лучшему! Удачи!

Кривая Гартнера (англ. Gartner Hype Cycle) – графическое отображение цикла зрелости технологий, представляющего собой поэтапный процесс, через который проходит любая инновационная бизнес-модель или технология от стадии хайпа до продуктивного использования. Методология Hype Cycle применяется при определении и ведении так называемого профиля инноваций, то есть помогает провести оценку потенциальных возможностей новых технологий для бизнеса.

Источник: https://blog.bitobe.ru/article/krivaya-gartnera/?ysclid=la8jd3x4v5100585800

55.7522
37.6156

Один день в Москве

В июне 2022 года шесть лучших участников проекта «Агенты безопасности», выпускников Медиашколы и Школы журналистики Культурно-досугового центра ФосАгро при поддержке Дирекции по экономической безопасности АО «Апатит» и УМВД России по г. Череповцу совершили увлекательное путешествие в столицу нашей Родины – город Москву. Цель – погружение в тематику безопасности на примере работы подразделений МВД и «Лаборатории Касперского» и отработка полученных навыков фото- и видеосъемки.
Вот что рассказали об этом сами ребята.

Агенты безопасности во время посещения Лаборатории Касперского

Поездка запомнилась на всю жизнь

Ульяна Дорофеева, выпускница Школы журналистики Культурно-досугового центра ФосАгро

Москва встретила агентов чудесной погодой! Насыщенная программа включала в себя экскурсию в Центральный музей МВД, Российский совет ветеранов органов внутренних дел и внутренних войск МВД России и «Лабораторию Касперского».

В начале нашего путешествия мы под руководством Ю. Г. Бондаренко, директора профориентационно-выставочного центра ЧОУ ДПО «Учебный центр ФосАгро» отправились в Центральный музей МВД России. Здесь нас уже ждали и рассказали много нового об истории создания и становления органов внутренних дел в разные периоды жизни страны. Ребята с большим интересом рассматривали экспозиции и задавали экскурсоводу вопросы. В том числе про «лихие 90-е».
В Российском совете ветеранов органов внутренних дел и внутренних войск МВД мы встретились с генералом-лейтенантом милиции В. Н. Булгаковым. Встреча проходила в приятной, располагающей к общению атмосфере. Перед нами стояла задача проинтервьюировать Владимира Никитовича о его деятельности по обеспечению безопасности в сфере борьбы с хищением социалистической собственности, а также безопасности современного предприятия. И с этой задачей мы справились. Кто-то из ребят задавал нашему собеседнику вопросы, а кто-то занимался видеосъемкой.
Следующей нашей остановкой стал центральный офис Компании «Лаборатория Касперского».
Ее сотрудник провел для нас интересную экскурсию по корпоративному музею, познакомил с деятельностью офисов и работой специалистов. Мы также узнали об основных направлениях в сфере безопасного использования интернет-ресурсов и трендах будущего в профессиях по кибербезопасности.
И вот, когда программа поездки была успешно выполнена, агенты безопасности отправились на прогулку по ВДНХ. На фоне ее достопримечательностей сняли кадры для будущего видеоролика, пофотографировались для себя и морально подготовились к дороге домой. Ужинали уже в поезде, обсуждая эту насыщенную, теплую и запомнившуюся на всю жизнь поездку.

Место, где хранят историю МВД

Даниил Илюхин,
участник проекта «Агенты безопасности»

Наверное, полиция – это первое, что приходит в голову, когда речь заходит о безопасности. Ведь именно на сотрудниках правоохранительных органов лежит ответственность за обеспечение порядка внутри государства. В России эту задачу выполняет МВД РФ. Наша команда, как никто другой, заинтересована в подробном изучении вопросов безопасности, именно поэтому мы посетили Центральный музей МВД России, где нам рассказали об истории наших правоохранительных органов.

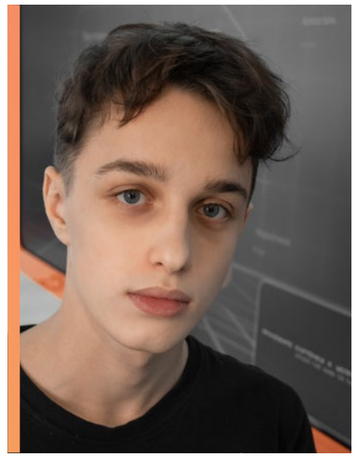
Центральный музей МВД — это по-настоящему удивительное место. Он находится в старинном особняке на Селезневской улице, а был открыт 4 ноября 1981 года. Кажется, здесь собрано абсолютно все, что связано с милицией *(с 2011 года переименована в полицию — ред.)*.
Первым делом мы попали в зал оружия, где увидели легендарный ППШ *(пистолет-пулемет Шпагина — ред.)* и Маузер *(самозарядный пистолет — ред.)*. Главная изюминка экспозиции — наградные пистолеты. Ими поощряли лучших из лучших: за заслуги перед государством в области обеспечения правопорядка, а также за воинские подвиги и заслуги.
Тематика и экспонаты следующих залов тесно связаны с разного вида преступлениями и следственной практикой. Так, здесь нас, в частности, познакомили с историями из служебной жизни оперативников. В этой части музея отдельно хочется отметить особую детальность. К примеру, в разделе о серийных убийцах (маньяки) собраны фотографии жертв, воспроизведены места преступлений.
Особняком стоят исторические экспозиции, посвященные и царской полиции, и советской милиции. К слову, всегда очень интересно обратиться к прошлому и увидеть, что было раньше и как кардинально все поменялось.
Кроме этого, в музее есть зал с экспонатами из разных стран мира, в том числе с униформой полицейских; зал подарков и сувениров, а также экспозиция, посвященная спортивному обществу «Динамо» *(основано руководством ОГПУ — ред.)* и т. д.
Команда «Агентов безопасности» осталась в восторге от экскурсии. Очень понравилось разнообразие экспонатов и тем. Обязательно побывайте в этом музее, чтобы увидеть все своими глазами!

Бескрайнее сердце генерала

Антон Микеров,
выпускник Медиашколы

Одним из ключевых моментов нашей поездки стала встреча с Владимиром Никитовичем Булгаковым. Для меня лично это было самое волнительное событие из всей программы пребывания в столице.

В. Н. Булгаков – генерал-лейтенант милиции. Родился в 1941 г. Имеет высшее юридическое образование. В органах внутренних дел – с 1966 г. Начальник УБХСС Главного управления внутренних дел Красноярского края. 1983–1991 гг. – в аппарате Министерства внутренних дел. 1991–1999 гг. – начальник Главного управления внутренних дел Правительства Саратовской области.



Конечно, мы готовились к этой встрече: продумывали вопросы, расписывали сценарий, распределяли работу операторов. Однако, как это порой бывает, когда к чему-то серьезно готовишься, то все идет немного не по плану. Все началось с того, что нашу группу из семи человек высадили на неизвестной для нас улице — предстояло двигаться пешком по навигатору. Приятный голос Алисы из телефона подсказывал маршрут, но мы… прошли мимо заветного здания. Время поджимало, и в скорости мы не уступали, пожалуй, даже олимпийским бегунам.

Наконец, та самая табличка с золотыми буквами «Совет ветеранов МВД России» оказалась прямо перед моим носом. Кабинет генерала-лейтенанта находился на втором этаже. Поднимаясь по резной лестнице наверх, я заметил на себе чей-то тяжелый взгляд. Обернувшись, увидел огромные портреты, с которых на нас глядели люди в генеральских погонах. Мне показалось, они видели нас насквозь.
По сценарию мы должны были зайти в кабинет, подготовить камеры, настроить микрофон и, не торопясь, начать интервью. Но Булгаков все

Агенты безопасности в Центральном музее УМВД

не могли даже догадываться.
Не успели мы осмотреться, как он начал свой рассказ. Как правило, люди с огромным жизненным опытом, начиная говорить о чем-либо, путаются в терабайтах своих мыслей и быстро уходят от темы. Но история нашего собеседника от этого не становилась менее интересной. Наоборот, мы узнали гораздо больше, чем могли бы.
Родился Владимир Никитович в Красноярском крае, в обычной семье. Мать — доктор, отец — водитель. На тот момент будущий генерал-лейтенант МВД не знал, кем именно хочет быть. Он просто стремился учиться всему и помогать Родине восстанавливаться после тяжелой войны.
Получив высшее юридическое образование и отслужив три года в армии, Булгаков пошел в органы: «Мне предложили поработать в ОБХСС, я согласился. А что это, я тогда и не знал…

взял в свои руки. Встав из-за стола, какие я видел только по телевизору, седой, невысокий мужчина поздоровался с нами и предложил присесть.
На первый взгляд, это был обычный дедушка лет 70–75, одетый в клетчатую рубашку и брюки. Может прозвучать довольно странно, но я никогда не видел генералов. В голове была только одна мысль: неужели он настоящий?
Хоть это и был с виду обычный человек, но было в нем что-то загадочное, как будто он знал и видел что-то такое, о чем мы

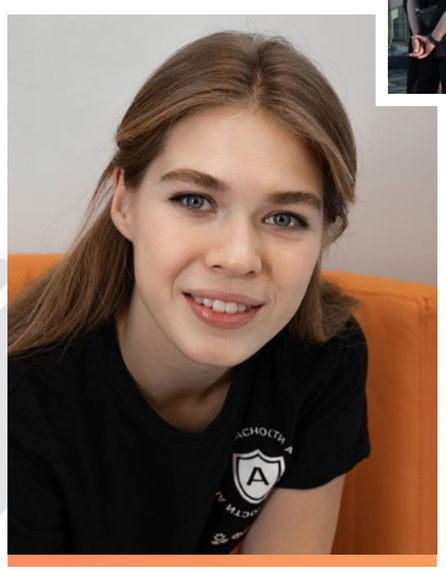
Будущая профессия позволила мне попробовать себя в разных сферах. Работал даже начальником в Компании «Енисейзолото», охранял алюминиевый завод, который тогда только строился. Помню, вызывает меня генерал и говорит: «Пойдешь в строительство». Ну а что? Пришел в библиотеку, понабрал книжек и давай учиться. Я тогда на четвереньках этот завод обходил, чтобы его не обокрали».
— А какая самая сложная операция была с Вашим участием?
— Как-то за день нам пришлось провести более сорока обысков…

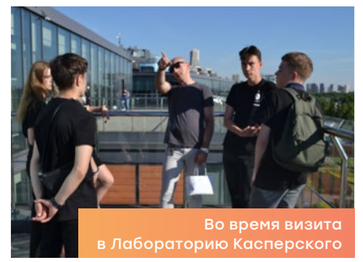
За свою карьеру Владимир Никитович успел побывать во многих уголках нашей необъятной страны. Но самым красивым местом считает свою малую родину — Красноярский край: «Знаете, когда весной Енисей разливается, а природа оживает, эту красоту ни на что не променяешь!» Чем больше он рассказывал, тем больше мы проникались уважением к этому человеку. Каждое его слово, даже пауза были пропитаны любовью к Родине. Глядя на него, подумалось: он воплощает то самое русское, что должно быть в каждом гражданине страны с гордым именем Россия. Но, к большому сожалению, не в каждом есть.
К своей работе Владимир Никитович относился ответственно, проверяя все до мелочей. Чтобы никто не мог сказать ту самую противную фразу, которую мы так часто слышим: «Разворовали страну!» «Везде надзоры, а контроля нет» — именно так прозвучали главные, как мне показалось, слова, которые, как порыв души, вырвались из уст генерала-лейтенанта. Тогда он говорил уже не о прошлом, а о настоящем. И пусть фраза «Раньше было лучше» заезжена не только до дыр, а, кажется, уже до полусмерти, в тот момент я был с этим согласен.
Интервью подходило к концу — настал момент прощаться. И тут Владимир Никитович взял со стола книги и протянул их нам. «Возьмите, пусть я уже не успею дать вам больше, но они, они смогут», — читалось в его глазах.
Несмотря на то, что это знакомство было мимолетным, оно оставило отпечаток в моей душе. И теперь, если врачи мне скажут, что размер человеческого сердца с кулак, я им не поверю. Сердце этого человека и размах его души можно сопоставить только с бескрайними просторами нашей необъятной Родины!

Касперский, зловреды-шпионы и… кубик Рубика

Софья Бычкова, участник проекта «Агенты безопасности», выпускник Медиашколы
Владимир Наумов, участник проекта «Агенты безопасности»

«Лаборатория Касперского… Что-то знакомое», — скажете вы. Чтобы помочь побыстрее вспомнить, мы расскажем об этом потрясающем месте, где нам посчастливилось побывать.
С приходом цифровых технологий появилась необходимость обеспечивать безопасность не только в реальном, но и в виртуальном мире. Именно этим и занимается «Лаборатория Касперского». Центральный офис международной компании, которая разрабатывает системы защиты от компьютерных вирусов, спама и хакерских атак, занимает три (!) пятиэтажных здания из стекла на Ленинградском шоссе. Когда мы зашли на его территорию, моментально погрузилась в мир инноваций, современности и будущего. Судите сами: площадки для пляжных видов спорта, яхт-клуб, тренажерный зал, сады, парки, комнаты будущего… И, конечно, — сам шикарный офис.
На входе в этот умный дом нас встретил Андрей Журавлев, ведущий специалист по обучению в сегменте B2C *(дословно «би ту си», означает коммерческие взаимоотношения организации с конечными потребителями — ред.)*. С первых минут общения мы поняли, что Андрей очень любит свою работу: с такой любовью и горящими глазами он рассказывал нам о Лаборатории. Конечно, мы не могли не взять интервью у столь харизматичного гида!





Во время визита в Лабораторию Касперского

— Из-за карантина вашей компании пришлось вести работу удаленно. Как подстраивались под новые реалии?
— До изоляции многие руководители были убеждены, что на удаленке человек расслаблен и его необходимо контролировать. Более того, считали, если работник долго не появляется в офисе, возникает вопрос: нужен он здесь или нет.
На удивление, оказалось, что персонал стал полностью отдаваться работе.
В результате компания, обеспечив в пандемийный период хорошие продажи, получила достойный доход. Теперь все смотрят на этот формат работы спокойно — человек даже может выбрать, как ему работать. Причем это будет не в ущерб качеству. Так каждый делает свой вклад в безопасный Интернет.
Но сначала нас ждала небольшая экскурсия по небольшому музею, своего рода визитной карточки Лаборатории. Затем, после необходимых формальных процедур на КПП, нам удалось пройти внутрь офиса. Здесь мы увидели много локаций, в том числе для отдыха, и… море цветов.
Среди всех рабочих зон внимание привлекла та, что свои кратко называют вирлабом *(вирусная лаборатория – ред.)*. Это место, где «отлавливают», изучают и классифицируют зловредов-шпионов, которых зафиксировали антивирусные программы Касперского в различных уголках мира. Бросились в глаза стеклянные стены с нанесенной на них частью исходного кода некогда самого опасного трояна ZeuS *(тип вредоносных программ — ред.)*. За ними мы увидели огромный круглый стол на восемь рабочих мест, где трудились «вирусологи» (чем не рыцари круглого стола!).
В завершение нашей команде посчастливилось посмотреть кабинет самого Евгения Валентиновича Касперского. Скромный, без изысков, но с ощущением присутствия хозяина. Так, на одном из столов мы заметили… кубик Рубика, механическую головоломку, изобретенную в 1974 году другим умным человеком.
Приятным сюрпризом для каждого из нас стали памятные подарки от компании, о которой мы узнали так много интересного.
После этой экскурсии захотелось вернуться в «Лабораторию» и пойти обучаться тем наукам, которые пригодятся в этом очень важном деле!

Даниил Илюхин:

будущий экономист, журналист или политик?

Мы познакомились в поездке в г. Москву, организованной для лучших участников проекта «Агенты безопасности», выпускников Медиашколы и Школы журналистики КДЦ ФосАгро. Улыбающийся, открытый, он удивил своей скромностью и готовностью помочь без... лишних слов. Согласитесь, качества на фоне привычного подросткового понтовства – довольно редкие.
О чем они говорят? О внутренней наполненности и зрелости личности.
Знакомьтесь: Даниил Илюхин, учащийся 11-го «ФосАгро-класса» МАОУ «СОШ № 10 с углубленным изучением отдельных предметов», президент Совета учащихся школьного самоуправления (ШУС).

Даниил, как ты стал президентом ШУС? С чего начал?

Выборы проходили 24 сентября 2021 года. Поскольку я интересуюсь политикой, решил предложить свою кандидатуру. Кампания запомнилась всплеском активности ребят.
По всей школе висели наши плакаты. А в соцсетях появились комментарии типа: «Обсуждали семьей, на кухне, кто победит...». В результате за меня проголосовали 56 % ребят.
ШУС делает жизнь учеников насыщеннее и интересней.
Мы рассказываем о нашей работе в группе школы в «ВКонтакте» и в группе школьного самоуправления. Так о нашей школе больше узнают в городе.
Например, в начале года Совет ШУС совместно с администрацией школы организовал квесты для первоклашек и пятиклассников, чтобы ребята быстрее адаптировались к школе.
В сентябре провели кибертурнир по популярной мобильной игре «Brawl Stars» *(«Битва звезд» — ред.)* по линии РДШ *(Российское движение школьников — ред.)*.
К слову, чтобы у участников была дополнительная мотивация, член Совета Дима Лебедев распечатал на 3D-принтере кубок для победителей. Потом мы раскрасили его специальными маркерами. Ребята были в восторге!
А по итогам соревнований сборная школы заявилась на турнир по Северо-Западу, организованный РДШ. Выступила достойно: дошла до четвертьфинала. Я рад, что у нас все получается!

А как ШУС относится к экологическим акциям?

Поддерживаем! Прошлым летом собрали около тонны макулатуры, в октябре того же года — еще 450 кг. А в декабре уже участвовали в городском этапе Всероссийской акции «БумБатл». Так, меньше чем за неделю сдали 895,8 кг, заняв призовое место. Еще собираем пластиковые крышки от бутылок. Такие акции наш Совет организует как соревнования между классами: победителям вручаем переходящие кубки. Чтобы получить ожидаемый результат, подключаем элемент интерактива: взаимодействуем через соцсети. Кстати, активнее всего в этих мероприятиях проявляют себя малыши.
Раскрою секрет: на вырученные от сдачи вторсырья средства хотим приобрести родной школе подарок — аэрохоккейный стол.

Школьное ученическое самоуправление (ШУС) – форма реализации учащимися права участвовать в управлении школой. А именно в решении совместно с педагогическим коллективом и администрацией вопросов организации учебно-воспитательного процесса.

Прислушивается ли руководство школы к вашим предложениям?

Считаю, нам повезло! Нас поддерживают, отзываются на любую инициативу, одобряют и помогают. Прежде всего хотелось бы поблагодарить директора Анну Олеговну Леоненко, завучей: Светлану Георгиевну Ненилину, Маргариту Викторовну Куксу и Елену Николаевну Лаврову, а также секретаря директора Елену Васильевну Богачеву.
В нашем сотрудничестве важно все: и поддержка, и результат, и обратная связь. Не менее ценно одобрение самих ребят. Чтобы получить их оценку, узнать, что они хотят, мы проводим соцопросы через Google Формы. Приятно, что получаем много положительных отзывов.

Анна Леоненко, директор школы №10: «Даниил любит школу и хочет, чтобы у нас было лучше всех. Поэтому с избранием его президентом Совета ШУС работа закипела. В том числе среди педагогов. Мы несколько раз встречались – все, что вместе запланировали, выполнено. Чувствуем помощника в лице лидера Совета».

Что тебе дает работа в Совете ШУС?

Прежде всего возможность направить в дело энергию: интеллектуальную, креативную и т. д. Еще много новых знакомств, в том числе на городском фестивале школьных самоуправлений *(Фестиваль школьного актива «Мы в деле!» — ред.)*, который проходил в октябре 2021 года.
Далее — опыт выборов, коммуникаций. Но главное — под руководством нашего куратора Ольги Александровны Кудряшовой мы сплотились со своей командой. Именно командный дух определяет успех любого мероприятия. В состав нашего Совета входят 10 человек. Причем каждый незаменим. Особенно хотел бы отметить Диму Величко (занимается дизайном и видеомонтажом, один из организаторов кибертурнира), Лизу Чащину (мой заместитель, и этим все сказано), Асю Рыжову и закончивших в этом году школу Диму Лебедева (поступил в Горный университет) и Ульяну Ганичеву (студентка биофака МГУ).

Ты возглавил Совет с ноля, или уже имел опыт общественной работы?

Скорее да, чем нет. Я был создателем общественно-политического проекта в Интернете, куда в качестве лекторов приглашал кандидатов в депутаты, их помощников и молодежных политиков. Они рассказывали о своей работе, карьере, выборной деятельности и т. д. Также мы с друзьями раздавали газету одной из демократических партий. Словом, руководство ШУС — не первый, но пока самый ценный опыт в моей общественной работе.
Между тем политика для меня — это все-таки больше увлечение, хотя раньше я хотел с ней связать свою жизнь. Так, во втором классе мечтал стать министром иностранных дел... Кстати, дома о событиях в нашей стране и в мире общаемся с папой. Вообще, у меня родители — врачи. И они видели меня в медицине.

А сам ты в чем хотел бы реализовать свои таланты?

Признаться, думал о медицине, как, впрочем, и о юриспруденции. Но больше склоняюсь к экономике. В том числе прорабатываю вариант целевого обучения по направлению компании «ФосАгро».
Уже присмотрел ряд университетов Санкт-Петербурга: Горный, Политехнический или СПбГЭУ.
А также вузы государственной службы. Дополнительно, возможно, поступлю на журфак: нравится писать, размышлять... Ведь журналистика, как и политика, связана с социумом. А вообще, к вопросу о выборе профессии, мне очень нравятся слова великого Конфуция: «Найдите работу, в которую влюбитесь, и вам больше не придется трудиться ни одного дня в жизни».

Твои ожидания от этого учебного года?

Для меня это особенный год: заканчиваю школу, учусь в физ-мат классе. Поэтому в приоритете — успешно сдать ЕГЭ. Кстати, подготовиться и легче войти в 11-й класс помог летний школьный лагерь с факультативами по физике, математике и химии.
У нас замечательные учителя по всем предметам. И прежде всего — по профильным: математик Юлия Васильевна Бобкова, физик Татьяна Сергеевна Потапова, химик Татьяна Испульевна Зимоздра. А как в нашей школе преподают историю и английский язык! Свою любовь к предмету педагоги передают нам. Впрочем, как и любовь к школе.
А она благодаря ФосАгро выглядит более чем достойно. Даже не скажешь, что это бюджетное образовательное учреждение... На мой взгляд, наша десятая — лучшая в городе! Неудивительно, что учиться здесь — одно удовольствие!

Для этого номера я подобрала пару книг, прочитав которые ты сможешь выработать для себя тактику противостояния хейтерам.

Лариса Минина, заведующий детским отделом Центральной городской библиотеки им. В. В. Верещагина (г. Череповец)

Джастин Пэтчин
и Самир Хиндуя

«НАПИСАННОЕ ОСТАЕТСЯ»

Книга «Написанное остается» — это пошаговая инструкция по цифровому поведению. С реальными историями, примерами и даже тестами.
Ее написали доктора наук, мировые эксперты в детской психологии, в области цифрового поведения.
Ты узнаешь, как защитить от недоброжелателей и избежать травли кибербуллинга — себя и друзей. Словом, научишься вести себя в Интернете так, чтобы не было стыдно, обидно или больно.

Кибербуллинг – одна из главных угроз, с которой ты можешь столкнуться в Интернете. Ранящие комментарии, ругань, онлайн-домогательства, гуляющие в Сети личные фотографии и переписка – такие неприятности унижают подростка, разрушают его дружбу, приводят к школьным разборкам и стрессу. Как выстроить вокруг себя здоровую и безопасную среду в Интернете? Как оградить себя от опасности?

Светлана Иконникова

«ТРОЛЛОЛОГИЯ. КАК НЕЙТРАЛИЗОВАТЬ ХЕЙТЕРОВ И ПРОТИВОСТОЯТЬ ИМ В СОЦСЕТЯХ»

Светлана Иконникова — психолог, журналист, автор книг «Троллология. Как нейтрализовать хейтеров и противостоять им в соцсетях», «ЕГЭ без стресса», «Больно не будет. Нефантастика».

«Троллология. Как нейтрализовать хейтеров и противостоять им в соцсетях» — книга о типах троллей и пяти тактиках противодействия им. Ты не только найдешь в ней приемы их нейтрализации, но и узнаешь, что делать, чтобы они как можно реже появлялись на твоей странице в соцсетях. Автор на примерах из жизни объясняет, как бороться с хейтерами *(люди, которые пишут оскорбительные и агрессивные комментарии, посты и сообщения в социальных сетях — ред.)* в Интернете.
Книга, безусловно, может иметь терапевтическое значение для всех, кто страдает от хейтеров.

КИБЕРГОРОСКОП 2023

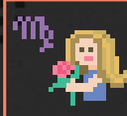
На что обращать внимание в

Овнов в грядущем году ждут неожиданные приятные перемены — судьба на вашей стороне! Однако и в киберпространстве не стоит терять голову и идти на поводу своих чувств. Для профилактики не забывайте время от времени менять пароли в социальных сетях! Ваша Безопасность в ваших руках!

Для **Львов** 2023 год — год изменений, преображений и улучшений. Самое время — взять дело (и свою кибербезопасность) в свои руки! Не забывайте вовремя обновлять программное обеспечение и операционную систему. Помните, чем старше ваша система, тем больше времени у хакеров найти пути украсть ваши данные. Используя новое ПО, вы получаете свежие исправления безопасности.

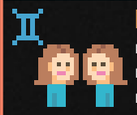
Стрельцы, в грядущем году развлечения и праздники не обойдут вас стороной — у вас буквально не будет времени скучать дома! Однако агенты безопасности предупреждают, что следует избегать незащищенных сетей Wi-Fi в общественных местах. Злоумышленники используют такие сети как инструмент для перехвата данных с помощью MITM-атак, то есть атак посредника.

Тельцы, вас ждет настоящий прорыв! А значит — новые решения, которые вам придется принимать быстро и на свой страх и риск. Помните, что не все файлы в Интернете являются безопасными для скачивания. Тщательно проверяйте информацию, поступающую вам из киберпространства!



Девам звезды говорят, что в грядущем году следует оставлять свои планы в секрете от окружающих. Убедитесь в сохранности своей приватности в социальных сетях. Зайдя в настройки соцсети, в графе «приватность» вы можете отрегулировать, какие данные находятся во всеобщем доступе, а какие видны только вам или вашим друзьям.

Козерогам в следующем году будет поступать множество необычных предложений, сюрпризов, что будет, несомненно, приятно для представителей этого знака зодиака. Однако следует ставить все под сомнение: агенты безопасности рекомендуют не открывать почтовые вложения от неизвестных отправителей, так как они могут быть заражены вредоносным ПО.



Близнецы, в прошедшем году вы узнали много новой информации — время применять ее в жизнь и делиться с окружающими! Звезды говорят, что ваш друг столкнется с проблемой в киберпространстве и вы станете именно тем человеком, который сможет защитить близкого человека от киберугрозы!

Весы, в наступающем году в вашей жизни появится надежная опора и дела пойдут в гору! Агенты безопасности, посоветовавшись с астрологами, выяснили, что речь идет именно об установке безопасного пароля. Помните, что надежный пароль должен содержать около 12 символов, в том числе цифры, заглавные и прописные буквы. Учтите, что варианты «12345» и «qwerty» не подходят!

Жизнь **Водолеев** будет полна активностей и различных дел. Волна воодушевления и продуктивности накроет вас с головой! Однако не забывайте отдыхать и проводить время с близкими. Отличным решением станет цифровой детокс — временный отказ от использования электронных устройств.
Он точно поможет вам расслабиться и набраться новых сил!

Ракам следует помнить, что тенденции киберугроз постоянно меняются! За мошениками в Интернете не уследить: каждый день они придумывают новые схемы обмана. Будьте готовы к неожиданностям и внезапным поворотам событий. Следуйте своей интуиции — вам удастся с легкостью обойти все опасности!

Скорпионов в этом году будет поджидать удача в каждом их начинании! Однако звезды предупреждают, что нужно быть вдвойне аккуратными! Задумайтесь об установке двухфакторной аутентификации на тех площадках в Интернете, где это возможно. Она обеспечит двухслойную, более эффективную защиту ваших данных и отгородит от нежелательных авторизаций в ваши аккаунты.

Рыб в 2023 году настигнет желание поразмышлять о прошлом, предаться воспоминаниям. А чтобы это всегда было возможно, не забывайте делать бэкапы — резервные копии своих данных. Любой ценной и важной для вас информации нужны копии на случай, если с оригиналом что-то случится.

Если вам нравится журнал,
то вы можете оставить нам
несколько приятных
слов или пожеланий
по улучшению издания
на нашем паблике
«ВКонтакте»

№ 1 декабрь 2022 г. Тираж 500 экземпляров
Распространяется бесплатно. Возрастные ограничения 12+
Редактор: Светлана Цветкова
Авторы материалов: Светлана Цветкова, Даниил Илюхин, Софья Бычкова,
Антон Микеров, Ульяна Дорофеева, Полина Усманова
Заказчик: ИПЦ «Зеленая планета» / ЧОУ ДПО «Учебный центр ФосАгро»
Оформление: ООО «СибПроект»
Отпечатано: ООО «Издательский дом «Череповецъ», ул. Металлургов, 14а