Муниципальное бюджетное общеобразовательное учреждение
гимназия № 42 г. Пензы
(МБОУ ГИМНАЗИЯ № 42Г. ПЕНЗЫ)

II РЕГИОНАЛЬНЫЙ ФЕСТИВАЛЬ ТВОРЧЕСКИХ ОТКРЫТИЙ И ИНИЦИАТИВ «ЛЕОНАРДО»

секция: «Социальная инициатива»

Исследовательская работа

«Безопасный смартфон – защита личных данных в цифровом мире»

Выполнил:
Брякин Петр Сергеевич
МБОУ гимназия № 42 г. Пензы,
4 а класс

Руководитель:
Алексеева Н.Н.,
учитель начальных классов,
высшей категории
МБОУ гимназия № 42 г. Пензы

Пенза, 2022

Оглавление

Введение

Актуальность исследования: нельзя представить современного человека без смартфона и множества полезных приложений в нём. Дети малого возраста уже ежедневно пользуются мобильными телефонами, а многие владеют своими гаджетами. Мои ровесники 10 – 11 лет пользуются смартфонами осознанно, но они могут даже не догадываться, сколько опасностей подстерегает их в цифровом мире. Актуальность защиты личного устройства школьника повышается тем, что последние годы быстрыми темпами развиваются джуниор банковские карты, приложения от которых устанавливаются на детские смартфоны.

В этой работе я рассмотрю такое важное направление безопасности, как безопасность мобильного устройства, в частности смартфона. Рассмотрим настройку, эксплуатацию и защиту смартфона.

Цели работы: изучение информации о пользовании, настройке и защите смартфона, для повышения его безопасности**.**

Гипотеза: я предположил, что не существует таких правил и способов пользования, настройки и защиты смартфона, и таких приложений, которые сделают смартфон на 100% защищённым.

Объект исследования: смартфон, его безопасность и настройка.

Предмет исследования: проверка безопасности смартфона.

Для достижения поставленных целей мне нужно выполнить следующие **задачи**:

1. найти в сети Интернет информацию о способах, методах и приложениях для обеспечения безопасности смартфона;
2. проанализировать антивирусы и менеджеры паролей для смартфона ребёнка, выбрать оптимальные;
3. сформулировать правила пользования, настройки и защиты смартфона;
4. провести опрос среди одноклассников;

5. рассказать одноклассникам о важности соблюдения правил пользования, настройки и защиты смартфона, а также о важности использования антивируса и менеджера паролей на телефоне;
6. показать одноклассникам, как установить на свой смартфон антивирус и менеджер паролей;
7. создать памятку о правилах пользования, настройки и защиты смартфона.

Методы исследования: теоретический анализ научной литературы и статей в сети Интернет; отбор информации; анализ; опрос; обобщение.

Теоретическая часть

Современные мобильные телефоны (смартфоны) уже давно перестали быть просто телефонами. По сути, у каждого из нас в кармане находится мини-компьютер, способный на многое. Установленное на нем стандартное программное обеспечение позволяет просматривать интернет-сайты, читать книги, слушать музыку, смотреть фильмы и многое другое. И это уже не говоря о дополнительном программном обеспечении, которое можно установить абсолютно бесплатно или за символическую плату.

Мобильный телефон, ставший смартфоном, постепенно превратился в средство хранения и обработки персональной информации: через него можно общаться в мессенджерах и соцсетях, хранить на телефоне конфиденциальную (и даже платежную) информацию — можно оплачивать со своего банковского счета покупки, используя для этого смартфон.

Но всю свою персональную информацию нужно защищать — от вирусов и вредоносных программ, которые могут похитить платежную информацию и пароли или личные данные и использовать это вам в ущерб, а также и от недоброжелателей, которым тем или иным путем попал в руки ваш мобильный телефон. [1]

В своей работе я буду рассматривать смартфоны с операционной системой Андроид, так как, во-первых, у меня и всех членов моей семьи смартфоны с Андроид, во-вторых, по информации из Интернет, количество

устройств с операционной системой Андроид в России значительно превышает количество устройств с iOS (АйОС). [20]

Большая проблема, которую невозможно решить в данной работе это то, что у существуют различные версии и вариации Андроид систем, настройки в них могут выглядеть и называться по-разному, поэтому при настройке вам придётся искать похожие пункты в похожих расположениях. В своей работе я буду использовать оболочку моего телефона MIUI для настроек системы. Для установки антивируса и менеджера паролей на всех Андроидах действия будут одинаковыми.

Чаще всего телефоны взламывают из-за невнимательности пользователя. Он может загрузить вредоносную программу, открыв ссылку в сомнительном письме, перейти по ссылкам из спама и странных сообщений из мессенджеров или попытаться заполучить доступ к свежему приложению и установить его из сомнительных источников.

Социальная инженерия — самый простой способ атаки на смартфон. Это способ атаки, в котором человек сам отдает мошенникам свои данные: например, сообщает номер карты якобы сотрудникам банка; или вводит логин и пароль от соцсети в сомнительном приложении. Если устанавливать приложения не из «Гугл-плея», вводить данные от соцсетей и банковских приложений на незнакомых сайтах, то Андроид не спасёт, каким бы безопасным он ни был. [20]

Как защитить свой смартфон (правила защиты и настройки смартфона)

Установка пароля на телефон

Установка пароля для разблокировки — первое, что защищает данные на смартфоне при попадании в чужие руки. Для доступа к информации нужно разблокировать экран.

Злоумышленники могут разве что сбросить телефон к заводским настройкам — тогда они получат на руки чистое устройство без личных данных.

Всего есть 5 способов заблокировать смартфон — 2 из них биометрические, по отпечатку пальца или по особенностям лица.

Способ «блокировки» экрана	**Особенности**
PIN-код	4 цифры в любом порядке
Пароль	От 6 до 8 цифр в любом порядке
Графический ключ	Есть 9 точек, нужно соединить хотя бы 4 из них любым способом
Отпечаток пальца	Специальный сенсор сканирует палец владельца, после чего система разблокирует экран
Сканирование лица	Телефон «сканирует» лицо ИК-лучами или через фронтальную камеру. Если лицо в базе смартфона совпадает с лицом взявшего в руки, смартфон разблокируется.

Лучше, если защитой станет надежный пароль, можно использовать и графический ключ его сложно подобрать (я на своём смартфоне пользуюсь графическим ключом). Простенький ПИН-код или отпечаток пальца делают устройство более уязвимым. Комбинацию из четырех цифр можно подобрать (хоть и долго), а приложить к сканеру палец вас могут заставить.

Отключите уведомления на заблокированном экране.

Это помешает злоумышленникам видеть письма и сообщения — включая коды для подтверждения платежей.

Отключите вывод содержания сообщений на экране блокировки. Иначе, если смартфон попадет в чужие руки, злоумышленник сможет прочесть важную информацию даже на заблокированном устройстве.

Установка двухфакторной авторизации на сервисах.

Это такой тип входа в профиль на сервисе, когда после ввода основного пароля нужно ввести дополнительный. Обычно дополнительный код приходит на:

- электронную почту в раздел «Уведомления»;
- SMS-кой или в мессенджер на смартфон, если подключен номер к сервису;
- уведомлением на другое устройство, подключенное к профилю.

Каждый раз пароль разный — такое непостоянство обеспечивает дополнительную защиту. Даже если злоумышленник угадает первый пароль, для доступа к нему придется ввести еще один — случайный.

Зачастую воры выбрасывают сим-карту, к которой привязываются большинство сервисов. Так что авторизоваться к сервисам, привязанных к сим-карте (мессенджеры, соцсети и т.д.), у них не получится. Обнаружив пропажу, владелец телефона может позвонить оператору и попросить заблокировать этот номер.

Данная функция настраивается конкретно на каждом из сервисов, которыми вы пользуетесь.

Настройка безопасности Wi-Fi подключений.

По умолчанию телефон автоматически подключается к знакомым Wi-Fi сетям. Однако публичные сети часто слабо защищены, и их легко взломать. Так мошенники получат доступ ко всем данным на вашем смартфоне.

Подключайтесь только к тем беспроводным сетям, которые защищены паролем. Подключаясь к общественному Wi-Fi, вы, можно сказать, приглашаете хакеров на экскурсию по своему смартфону. Не подключайтесь к сомнительным бесплатным открытым сетям Wi-Fi, в чьей принадлежности вы не уверены.

Смартфон может «запоминать» ваши Wi-Fi подключения. Это удобно не нужно каждый раз вводить пароль. Но, если устройство все-таки попадет в руки злоумышленника, он сможет получить еще одно подтверждение ваших

перемещений. Возможно, лучше удалить из истории хотя бы те места, куда не собираетесь возвращаться. Если раздаете Wi-Fi, не пренебрегайте парольной защитой. Включайте WPA2-PSK с надежным паролем

Разрешения и доступы для приложений.

Многие приложения получают доступ к локации, фото, соцсетям, интернет-трафику. Этим могут воспользоваться мошенники. Строго следите за разрешениями, которые просят у вас приложения.

Когда устанавливаете приложение, проверяйте, какие данные оно запрашивает. Например, если фонарику нужен доступ к телефонным звонкам, сообщениям, это повод насторожиться, потому что фонарику для работы нужна только вспышка. Изменить разрешения можно в настройках приложений смартфона. Контролируйте разрешения приложений.

Создание резервных копий всех данных на телефоне.

Регулярное копирование системы должно стать полезной привычкой. Порой можно лишиться файлов из-за глупости после случайного заражения. Кроме этого, только через копирование можно быстро перенести конфиденциальную информацию (включая номера телефонов и переписку) при покупке нового телефона.

Загрузка приложений только из официальных источников.

Загрузка приложений со сторонних сайтов грозит попаданием вируса и последующими хакерскими попытками изменить что-то в телефоне. В лучшем случае — будет постоянно светиться реклама. А в худших вариантах взломщики получают доступ к личным данным и банковским приложениям, блокируя телефон навсегда.

Эти проблемы можно избежать, если использовать только официальные магазины приложений. Выбирая приложение, смотрите на:

- количество скачиваний — чем их больше, тем лучше;
- оценку — не рискуйте, устанавливая программы с рейтингом ниже «4 звезд»;

- количество отзывов — если у приложения нет отзывов, это должно насторожить.

Остерегайтесь универсальных мессенджеров, приложений типа «Музыка ВК» или «Кто был на вашей странице». Любые неофициальные приложения, которые запрашивают ваши личные данные, могут использовать их против вас.

Будьте осторожны, если какой-либо сайт предлагает вам установить обновление, почистить телефон, продлить срок службы батареи или что-нибудь ещё многообещающее. Чаще всего за всеми этими чудо-программами будут скрываться вирусы.

У официального магазина есть функция Google Play Защита: она ежедневно сканирует 50 миллиардов приложений на более чем 2 миллиардах устройств, чтобы защитить их от вирусов и злоумышленников.

Регулярное обновление системы телефона.

Наличие свежей версии системы — важнейший шаг к безопасности данных. Хакеры для взлома устройств используют уязвимости системы. Разработчики ОС борются с этим «на опережение», закрывая дыры в новых обновлениях.

Поэтому наличие свежей версии системы — критически важно для сохранения конфиденциальности данных. Пока хакеры находят «дырки» в одной версии, разработчики уже выпускают другую. И с такой игрой «на опережение» владельцы свежих ОС остаются защищёнными от многих атак.

Ссылки в сообщениях.

Ни в коем случае не открывайте ссылки из писем или SMS-сообщений от отправителей, которых вы не знаете. Сразу же удаляйте сообщения в мессенджерах от неизвестных контактов.

Хранение личных фото и видео.

Регулярно переносите со смартфона в надежное место фотографии и видеозаписи в компьютер. Пусть они «в случае чего» останутся с вами и не достанутся злоумышленнику.

Быстрая блокировка.

Настройте систему так, чтобы блокировка экрана активировалась не через полчаса, а уже через минуту-две бездействия. Если телефон окажется в чужих руках, будет меньше шансов злоумышленнику добраться до ваших данных.

Ненужные приложения.

Удалите приложения, которыми больше не пользуетесь, или которые скачали когда-то «попробовать» и «на всякий случай». Меньше неожиданностей, больше свободного места. Устанавливайте только те приложения, которые действительно нужны.

GPS-навигация.

Заведите на смартфоне приложение для навигации с офлайновыми картами. Это поможет при ориентировании на местности во множестве ситуаций (а также повысит ощущение контроля и безопасности).

Не оставляйте без присмотра и не давайте другим.

Не оставляйте устройство вне вашего контроля. Даже ненадолго. Например, не выкладывайте его на столик в кафе, а также не оставляйте в школе на парте. Существует риск кражи и физического повреждения.

По возможности не передавайте смартфон другим людям.

Полезные приложения для защиты смартфона.

В этой части работы рассмотрим, какие приложения обязательно должны быть установлены на ваш смартфон для обеспечения его безопасности.

Антивирус.

Антивирус – это «китайская стена» внутри вашего смартфона, он защитит его от различного рода вирусов. Отсутствие антивируса на смартфоне ставит его под угрозу!

Я нашёл в Интернете много сайтов сравнения антивирусов для смартфона, выбрал один [20] и рассмотрел антивирусы из списка с точки зрения использования детьми, очень важны 2 фактора в моём выборе, во-первых, отсутствие платы, во-вторых, надежность и безопасность.

Вот список ТОП-5 антивирусов, из которых я и выберу подходящий:

1. **ESET Mobile Security & Antivirus**

Продвинутый защитник, по многим показателям возглавляющий рейтинг. ESET Mobile Security & Antivirus характеризуется не только высокой оценкой пользователей, но готов похвастать массой объективных преимуществ. К таковым следует отнести одновременную защиту до 5 устройств с одного аккаунта, настройки пользовательских сообщений и функцию создания автоматических селфи в ситуации, когда телефон попадает в руки другому человеку. Со своими прямыми обязанностями антивирус справляется на отлично. Бесплатно вы сможете пользоваться ESET Mobile Security & Antivirus только 30 дней, после чего придется, оплачивать Pro-доступ.

2. **McAfee Mobile Security.**

McAfee Mobile Security – это достаточно популярный антивирус для смартфона. В приложении Google Play Market более 100 000 000 людей скачали этот антивирус. Программа помимо антивируса имеет возможность защитить телефон от кражи и почистить его память. Основные возможности доступны и в бесплатной версии. Огромным минусом программы является её медлительность.

3. **Sophos Mobile Security.**

Sophos Mobile Security – это бесплатная программа с невысокой оценкой пользователей, которая при этом готова похвастать высоким уровнем защиты и миниатюрным размером, благодаря чему антивирус удается поставить на смартфон со скромным накопителем. В тестах приложение обнаруживает 99.9 % угроз, что можно назвать прекрасным результатом.

Вместе с этим пользователями отмечаются недостатки, способные испортить общее впечатление от антивируса. Sophos нет на русском языке, поэтому нам она точно не подходит. Еще одним минусом является долгое сканирование системы, что, впрочем, компенсируется высокой степенью защиты.

4. **Avast Mobile Security.**

Рассматривая антивирусные программы, нельзя обойти стороной Avast Mobile Security. Он известен многим владельцам персональных компьютеров, а потому версия для мобильных устройств получилась такой же популярной. Avast Mobile Security является бесплатным антивирусом.

Приложение не только защищает пользователя в онлайне и офлайне, но и присылает ежедневный отчет. Он сообщает владельцу смартфона, на какие аспекты устройства стоит обратить внимание при эксплуатации. Разумеется, в отчет попадают и найденные угрозы, которые можно устранить одним нажатием.

5. Kaspersky Internet Security для Android.

Наряду с Avast популярностью пользуется Kaspersky. К сожалению, бесплатная версия приложения упускает много угроз во время проверки, из-за чего ее нельзя назвать оптимальным защитником. То есть необходимо покупать полную версию.

Я считаю, что лучшей программой является Avast Mobile Security. Потому что эту программу предпочитают много людей, она бесплатная, надежная и безопасная, а также каждый день присылает отчёт о безопасности устройства.

Менеджер паролей.

Самым лучшим способом хранения паролей является менеджер паролей. Это ваш личный банк внутри смартфона и, если вы сами не пустите туда чужака, ваши пароли будут в безопасности.

В Интернете [20] я прочитал о 10 менеджерах паролей, из них я выбрал ТОП-5:

1. Dashlane Password Manager.

У него удобный интерфейс пользователя (недоступный на русском) и множество очень полезных дополнительных функций. У Dashlane есть бесплатный тариф, однако с ним вы сможете использовать только одно устройство и хранить не более 50 паролей. Если вам этого не хватает вы можете оформить платную подписку.

2. RoboForm.

RoboForm – это очень безопасный менеджер паролей с уникальными возможностями автозаполнения. RoboForm предоставляет шаблоны для любых данных, начиная с паспорта и банковской карты и заканчивая регистрационными данными автомобиля, при этом он автоматически и безошибочно заполняет личные и платёжные данные на любых веб-формах. Вам будет приятно узнать, что пользовательский интерфейс доступен на русском языке, поэтому у вас не возникнет сложностей с управлением всеми функциями приложения. RoboForm также предоставляет неплохие функции обеспечения безопасности. Все инструменты и функции RoboForm работают безупречно.

Работать с RoboForm очень удобно, поэтому даже начинающим пользователям не составит труда воспользоваться всеми его инструментами. Бесплатный тариф в RoboForm предоставляет безлимитное хранилище паролей и функцию автозаполнения, если вы купите платный тариф у вас будет больше возможностей.

3. LastPass Password Manager.

С ним вы получите все базовые функции для простого и безопасного управления паролями на Android-устройстве.

Огромный минус в нашем случае отсутствие русского языка. LastPass – отличный бесплатный менеджер паролей.

4. RememBear: Password Manager and Secure Wallet.

RememBear – это удобное приложение для Android с хорошим уровнем защиты, интуитивным интерфейсом и милейшими медвежатами. RememBear станет отличным выбором для новичков в мире менеджеров паролей и неопытных пользователей. В приложении есть простая система достижений, которая предоставляет чёткие инструкции для получения доступа к функциям приложения – каждый раз, когда вы “зарабатываете” новое достижение, вам дарят милого медвежонка. При этом помните, что в настоящий момент

интерфейс RememBear не доступен на русском языке – приложение поддерживает только английский язык.

5. Bitwarden.

Bitwarden – это доступный менеджер паролей, в котором есть хорошая бесплатная версия, полноценное приложение для Android и множество дополнительных функций для продвинутых пользователей. Вам будет полезно знать, что интерфейс приложения можно отобразить на русском языке.

Однако данное приложение не так удобно в управлении, и в нём множество продвинутых настроек, которые новичкам могут показаться слишком сложными.

На мой взгляд, лучшим менеджером паролей из этого списка является RoboForm. Эта программа является удобной и надёжной, в ней можно выбрать русский язык, а ещё все основные функции бесплатные и их легко настроить.

Практическая часть.

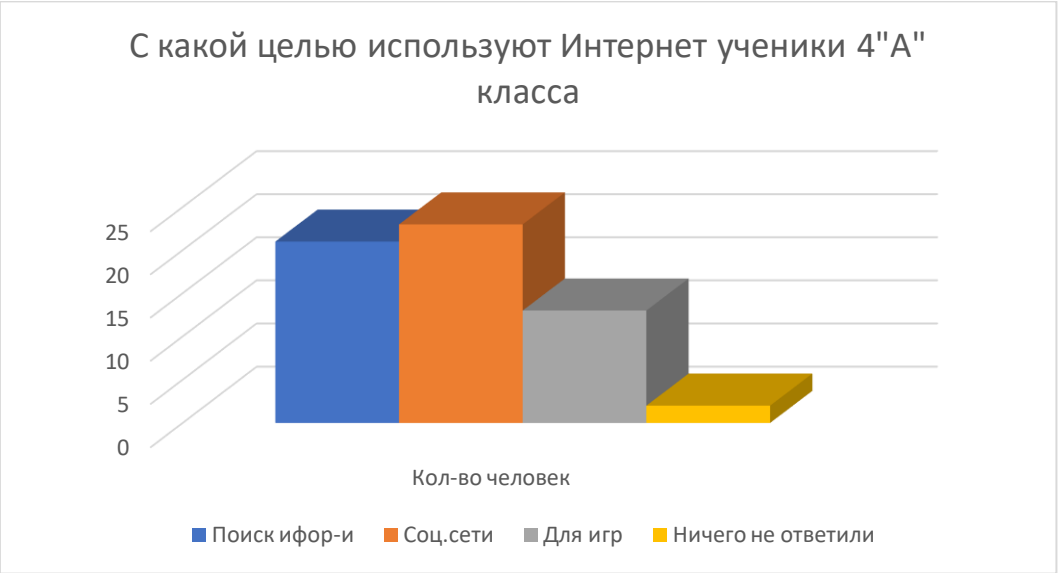
Практические указания для настройки правил защиты и настройки смартфона я вынес в приложение 2, а в приложении 3 и 4, расположены инструкции установки антивируса и менеджера паролей. Хочу напомнить, что все настройки показаны на моем личном смартфоне Xiaomi, с операционной системой MIUI, на других Андроид системах настройки могут отличаться, скорее всего незначительно.

В своем классе я провел опрос «Безопасный смартфон – защита твоих личных данных в цифровом мире», чтобы выяснить, зачем ребята используют свои личные смартфоны, что думают о защите своего смартфона и знают ли что такое антивирус и какие бывают антивирусы.

В опросе участвовало 30 учеников моего класса. Опрос показал, что у всех моих одноклассников уже есть личные смартфоны.

На вопрос: *Есть ли у тебя личный смартфон?* Практически все единогласно ответили – *Да*, один человек воздержался от ответа.

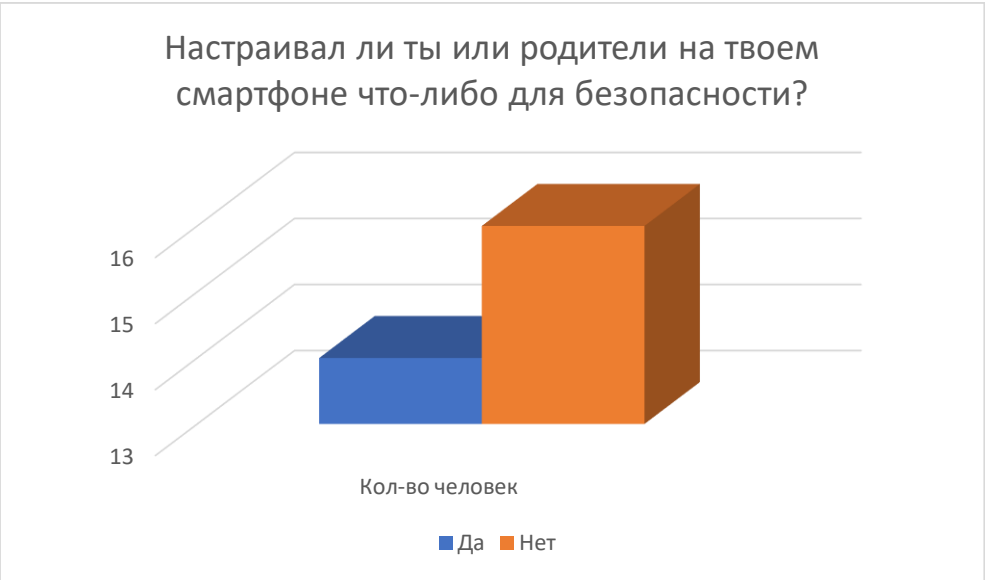
Пользуются же они смартфоном с разными целями:



На графике видно, что мои одноклассники больше общаются с друзьями и занимаются поиском информации, чем играют, я считаю, что это хорошая информация об учениках 4 «А» класса.

На вопрос: *Уверен ли ты в безопасности твоего смартфона?* только 6 человек из 30 ответили - Нет, воздержался – 1. Хочется верить, что одноклассники осознают необходимость защиты смартфона, 23 человека ответили – *Да*, я считаю, что это высокий показатель!

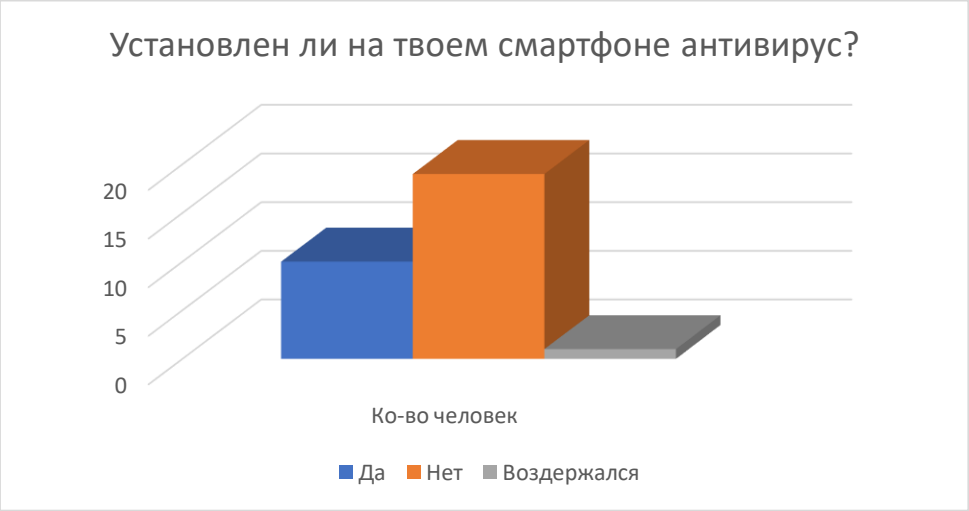
Мне интересно было узнать: *Настраивал ли ты или родители на твоём смартфоне что-либо для безопасности? Да ответили – 14 ребят, Нет – 16.*



Исходя из диаграммы можно сделать вывод, что большинство, к сожалению, не настраивали что-то для безопасности смартфона ребенка. Но

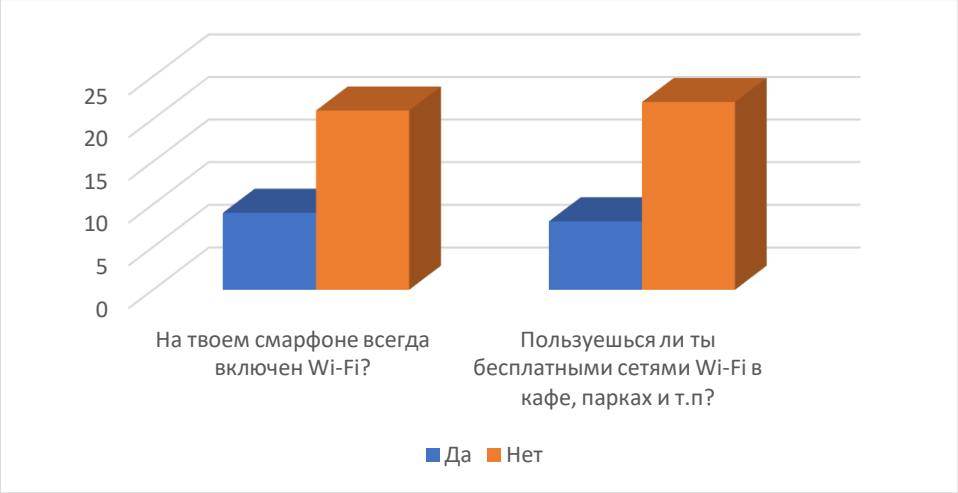
разница в результатах ответа всего 2 голоса. Это совсем немного, меня радует, что 14 ребят обезопасили свой смартфон.

На следующий вопрос: *Установлен ли на твоём смартфоне антивирус? ребята ответили так – у 10 человек установлен, у 19 – Нет, ничего не ответил – 1 человек.*



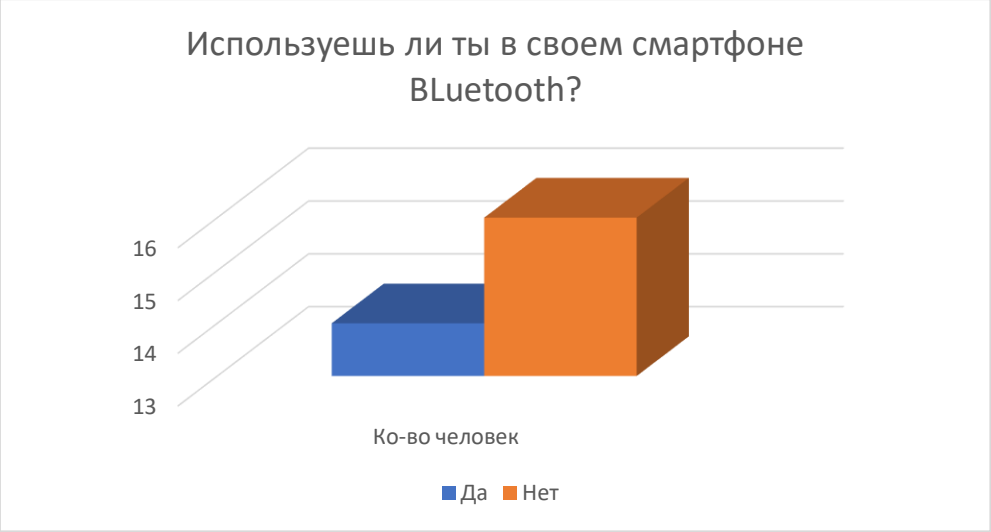
Из графика я понял, что больше половины учеников не знают о необходимости антивируса и не устанавливали себе его на телефон. Из тех ребят, кто ответил – *Да,* некоторые даже написали названия антивирусов (virus Hanter, Dr.Web, Comodo).

На вопросы: *На твоём смартфоне всегда включен Wi-Fi? Да* ответили - 9 человек, *Нет* - 21 человек. *Пользуешься ли ты бесплатными сетями Wi-Fi, например, в кафе или парках? Да* ответили - 8 человек, *Нет* -22 человека.



Вопросы схожи и по результатам ответов я вижу, что примерно у трети одноклассников всегда на их смартфонах включен Wi-Fi и почти треть ребят пользуются бесплатным доступным Wi-Fi. Это конечно не безопасно для их смартфонов. Хорошая информация в том, что у большей части класса Wi-Fi выключен и они не используют бесплатный Wi-Fi.

Ещё одной проблемой безопасности смартфона является Bluetooth. Поэтому, я задал ребятам вопрос: *Используешь ли ты на своём смартфоне Bluetooth?* Здесь мнения ребят разделились примерно пополам. 14 человек ответили, что используют, *Нет* – 16 человек.

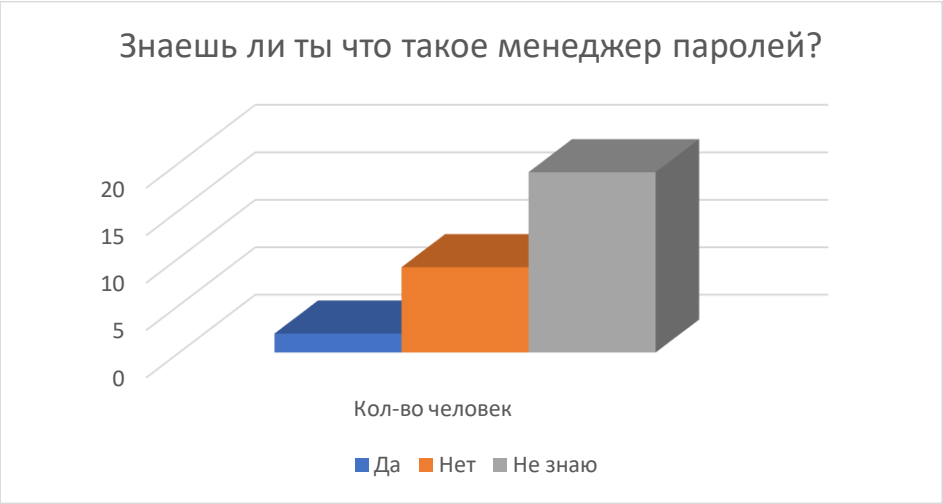


Это конечно очень плохо, что большинство ребят не выключают Bluetooth. Постоянно активированный в смартфоне Bluetooth представляет угрозу для владельца устройства — недоброжелатели могут использовать его, для того чтобы взломать смартфон.

Ребята ответили, что Bluetooth им нужен для подключения к часам и к наушникам.

На два последних вопроса ребятам видно было ответить сложнее всего. Нужно было не только сказать - *Да, Нет*, но и дать описания.

Например, на вопрос: *Знаешь ли ты что такое менеджер паролей?* Только 2 человека твердо ответили *Да,* 9 человек – *Нет* и *Не знаю* – 19 человек.



Из тех, кто ответил - Да, описали, что менеджер паролей — это *место для хранения паролей* и *место, где сохраняются все пароли*.

То, что всего 2 человека знают про защиту паролей - это плохо.

И последний вопрос: *Как ты хранишь свои пароли?* Одноклассники большинство написали - в блокноте или в уме. Записывать пароль, например, в блокноте можно, главное ограничить доступ к нему чужих людей. В прошлом году я проводил ребятам мастер-класс, в котором говорил, как хранить придуманные пароли. И я решил, что нужно повторить этот мастер-класс и напомнить ребятам полезную информацию.

Из проведенного опроса я делаю вывод, что много учеников 4 «А» класса используют небезопасные сети Wi-Fi и Bluetooth соединения на своих смартфонах. Антивирус у большинства не установлен, а для придуманных паролей «менеджером паролей» не пользуется никто.

Мои одноклассники, как я понял из опроса, либо мало знают правила безопасности смартфона, либо не знают совсем. Поэтому я решил им об этом рассказать и научить их устанавливать на смартфон антивирус и менеджер паролей.

Я рассказал ребятам правила защиты и настройки смартфона, мы вместе установили на их личные смартфоны антивирус и менеджер паролей. Каждый из ребят в конце занятия получил памятку.

Теперь у моих одноклассников на смартфонах установлены антивирус и менеджер паролей, пользуясь методичкой они настроят свои смартфоны на максимальную безопасность.

Планирую провести подобные мастер-классы для учащихся начальной школы гимназии, а памятку распространить среди родителей нашей гимназии.

Заключение.

Я провел актуальное исследование по теме. Сделал важные выводы, определил, что эта тема очень важная и нужная, особенно для моих сверстников. Как выяснилось, многие одноклассники не знают и не подозревают насколько важно защищать свои смартфоны и как это делать. Благодаря моим практическим действиям (выступление с презентацией, беседами, распространение памятки «Правила пользования, настройки и защиты смартфона»), я надеюсь, что моя работа улучшила ситуацию в этом вопросе и обратила внимание на его важность.

Моя гипотеза подтвердилась, теоретически не существует таких правил и способов пользования, настройки и защиты смартфона и таких приложений, которые сделают смартфон 100% защищённым. Но соблюдая мои рекомендации Вы защитите свой смартфон от вирусов и потери данных.

Считаю, что мною достигнута цель работы: определить осведомленность учащихся о защите смартфона и рассказать, как его защитить, я разработал и распространил рекомендации по защите смартфона.

Также достигнуты все задачи, которые я ставил перед собой.

Считаю, что материалы моей работы могут быть использованы на уроках окружающего мира и информатики в начальной школе. Планирую провести ознакомительные беседы и мастер-класс для учащихся всей начальной школы гимназии.

Список литературы

1. Колисниченко Д.Н. Безопасный Android: защищаем свои деньги и данные от кражи. – СПб.: БХВ-Петербург, 2015. – 161 с.
2. ОС Android: статистика, оценка и перспективы для рекламодателей. [Электронный ресурс https://www.byyd.me/]
3. Супрунюк Наталья. Блог moyo.ua [Электронный ресурс https://www.moyo.ua/]
4. Зуйкова Ася. РБК Тренды. [Электронный ресурс https://trends.rbc.ru/]
5. Марфицин Александр. Тинькофф журнал. [Электронный ресурс https://journal.tinkoff.ru/]
6. Леонтьев В.П. Все о смартфонах и планшетах в одной книге. – Издание 2-е, обновленное. - Москва: Эксмо, 2020 – 448 с.
7. Смирнов Сергей. Теплица социальных технологий. [Электронный ресурс https://te-st.ru/]
8. Верещака Евгений. Инфо-портал IT-техник. [Электронный ресурс https://it-tehnik.ru/]
9. Мартенс Бен. SafetyDetectives [Электронный ресурс https://ru.safetydetectives.com/]

Приложение 1. Опросник

Безопасный смартфон –

защита твоих личных данных в цифровом мире.

1. Есть ли у тебя личный смартфон? (да, нет) Подчеркни нужное.
2. С какой целью ты используешь свой смартфон? Выбери ответ.

- поиск информации в сети Интернет;
- общение с друзьями в мессенджерах или соцсетях;
- играю;
- Напиши свой вариант _____

3. Уверен ли ты в безопасности твоего смартфона? (да, нет) Подчеркни нужное.
4. Настраивал ли ты или родители на твоём смартфоне что-либо для безопасности? (да, нет) Подчеркни нужное.
5. Установлен ли на твоём смартфоне антивирус? (да, нет) Подчеркни нужное.

   Если да, то какой: _____ (Напиши)
6. На твоём смартфоне всегда включен Wi-Fi? (да, нет) Подчеркни нужное.
7. Пользуешься ли ты бесплатными сетями Wi-Fi, например, в кафе или парках? (да, нет) Подчеркни нужное.
8. Используешь ли ты на своём смартфоне Bluetooth? (да, нет) Подчеркни нужное.

   Если да, то для чего _____ (Напиши)
9. Знаешь ли ты что такое менеджер паролей? Напиши _____
10. Как ты хранишь свои пароли? Напиши _____

Дата: ____января 2022

Приложение 2. Рецензия

Рецензия на исследовательскую работу
ученика 4 а класса МБОУ гимназия №42 г. Пензы
Брякина Петра

Исследовательская работа «Безопасный смартфон – защита личных данных в цифровом мире», выполненная учеником 4 «А» класса Брякиным Петром очень познавательна и актуальна.

Актуальность этой темы обусловлена тем, что в современном мире смартфон является не только средством связи, но и хранилищем большого объема важной, в том числе и персональной информации. В последние годы быстрыми темпами развиваются банковские карты - «джуниор», приложения для которых, устанавливаются в том числе и на детские смартфоны. Поэтому тема безопасности информации в смартфоне важна для рассмотрения.

Пётр поставил перед собой цель – изучение информации об использовании, настройке и защите смартфона, в частности для повышения сохранности информации в нем. Исследовательская работа структурирована, в работе четко сформулированы цель и задачи, есть логическая связь между частями работы. В своей работе Пётр уделил особое внимание анализу доступной информации, сделал правильные выводы и подтвердил гипотезу исследования. Заслугой автора является проведения мастер-класса для сверстников и составление правил «пользования, настройки и защиты смартфона», которые помогут решить проблемы безопасности их смартфонов. Соблюдая простые правила дети смогут сделать использование смартфона безопасным.

Завершают работу приложения, содержащие иллюстративный материал.

Работа «Безопасный смартфон – защита личных данных в цифровом мире» отвечает выбранной теме, может использоваться в качестве обзорного факультативного материала на классных часах и на уроках ОБЖ в начальной и основной школе.

Таким образом, рассматриваемая работа заслуживает оценки «отлично».

Заведующий кафедрой
«Вычислительная техника»
Пензенского государственного университета, _____ Д.т.н. Митрохин М.А.

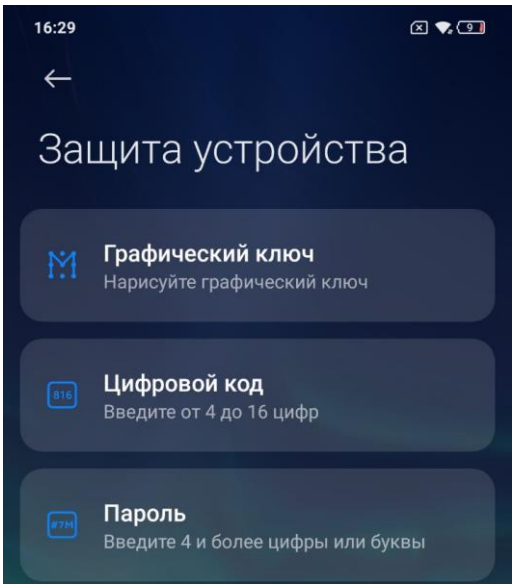
Зам. декана ФВТ /Писарь/

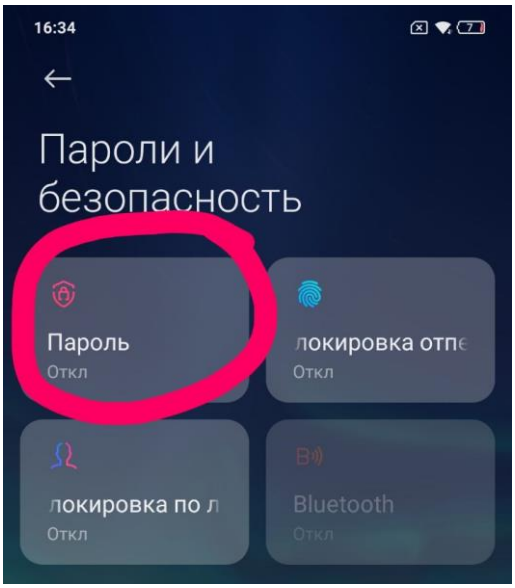
Приложение 3. Настройки смартфона.

Установка пароля на телефон

«Настройки» → «Пароли и безопасность» → «Блокировка экрана», выберите «Пароль» или «Графический ключ» в качестве способа блокировки экрана и установите пароль из букв и цифр.

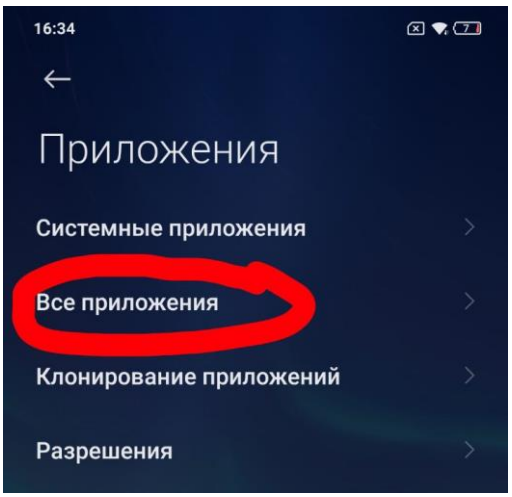
Затем «Настройки» → «Пароли и безопасность» → «Конфиденциальность», уберите галочку «Показывать пароли».

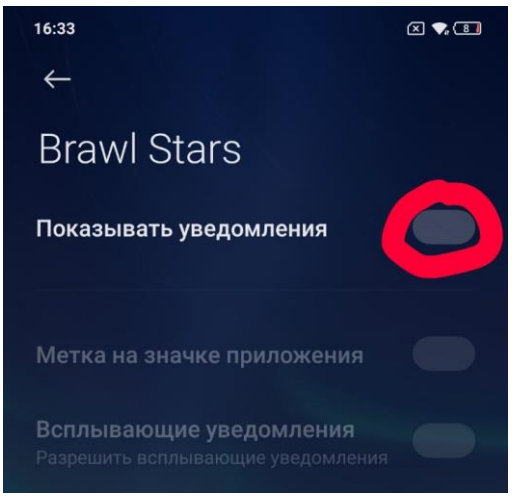




Отключите уведомления на заблокированном экране

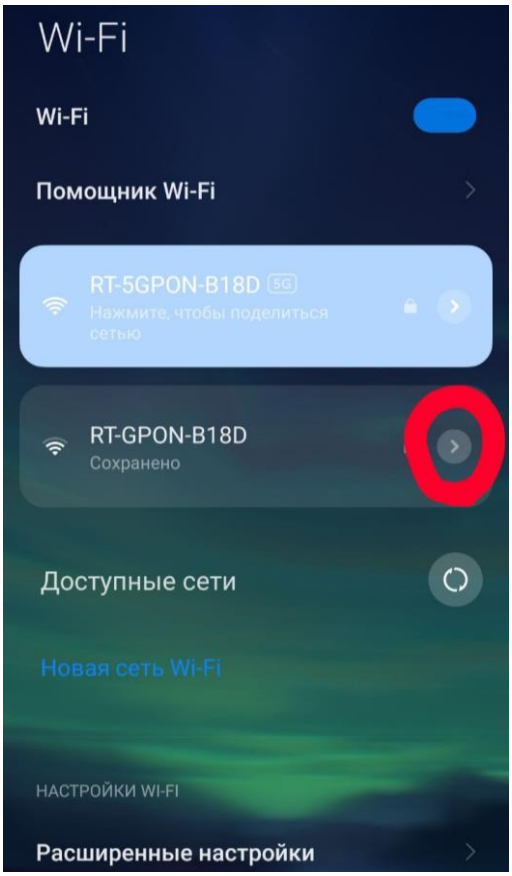
«Настройки» → «Приложения» → «Все приложения», выберите приложение и уберите галочку «Показать уведомления».

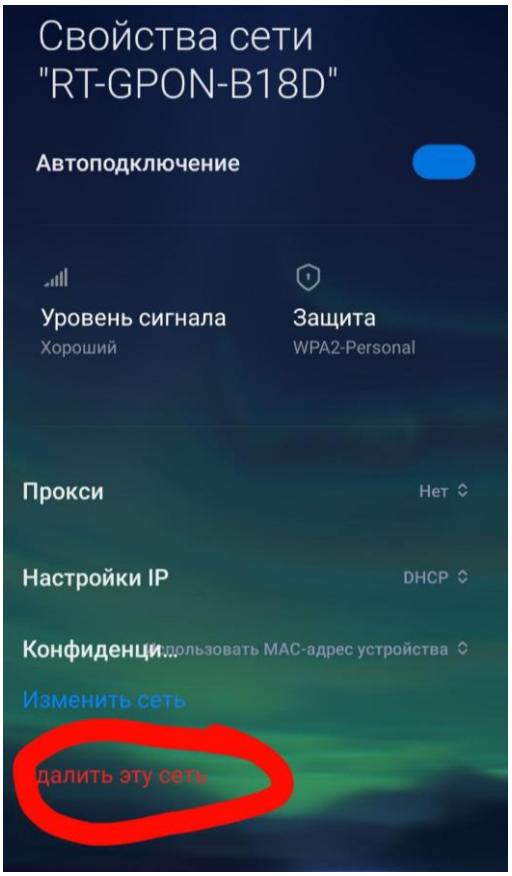




Настройка безопасности Wi-Fi подключений

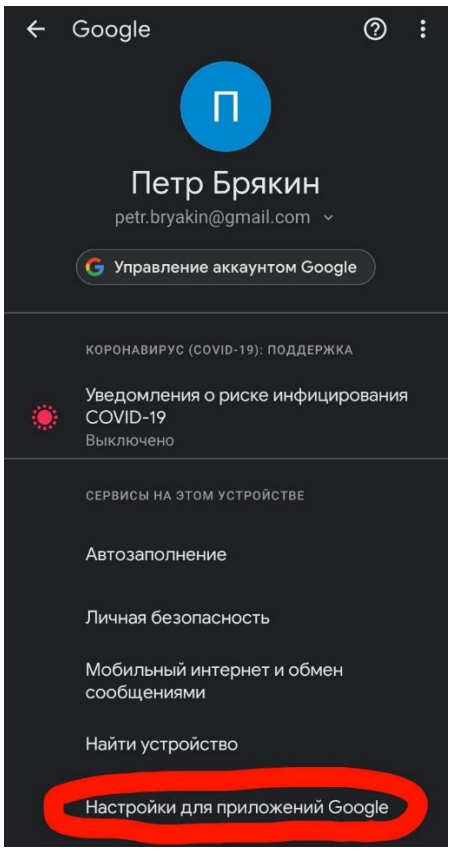
«Настройки» → «Wi-Fi», нажмите на стрелочку нужной сети, в появившемся меню удалите ее.

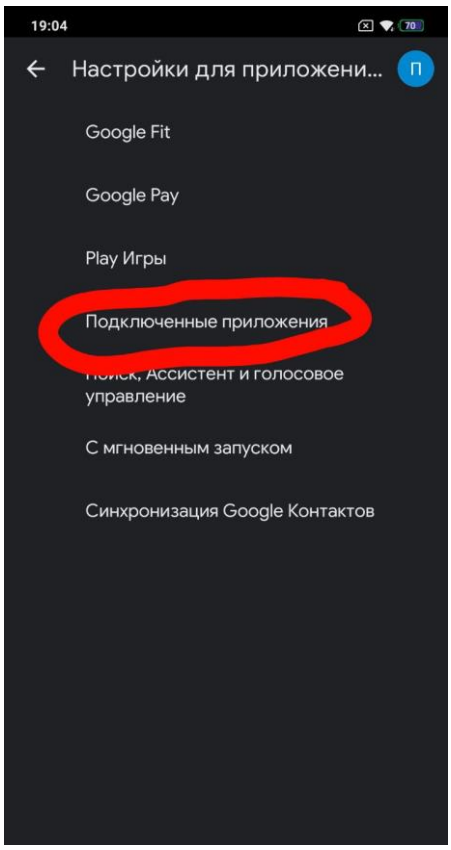


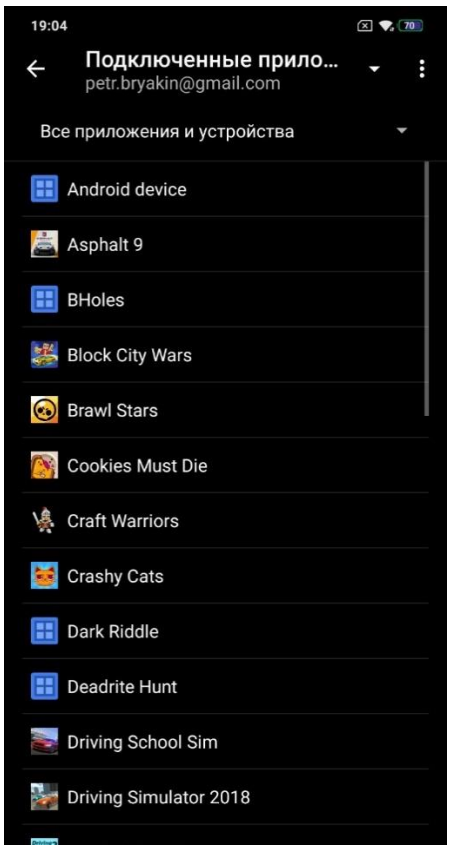


Разрешения и доступы для приложений

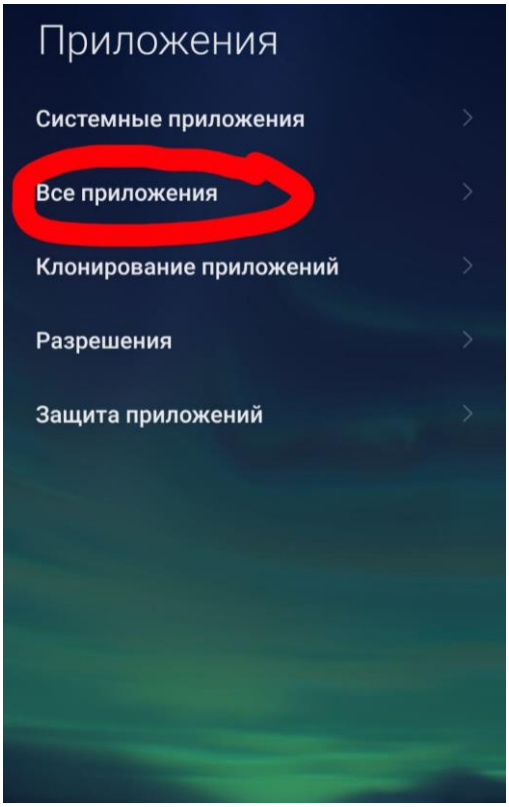
«Настройки» → «Google» → «Настройки для приложений Google» → «Подключенные приложения» — отключите все лишние.

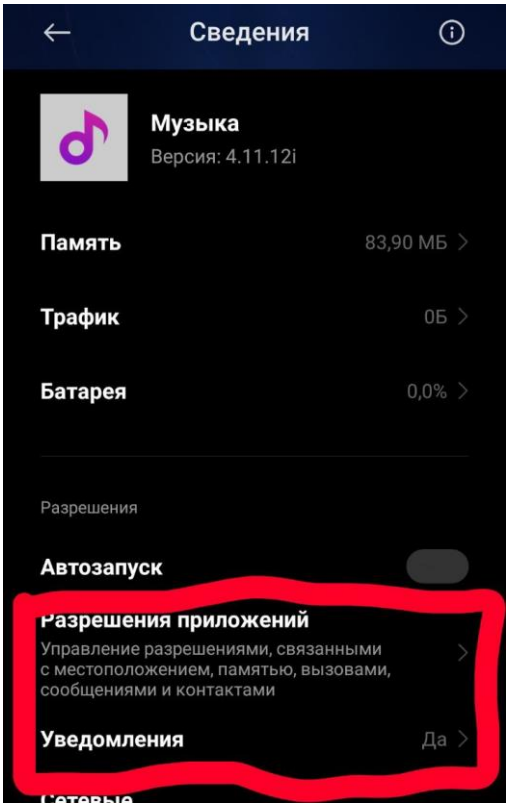






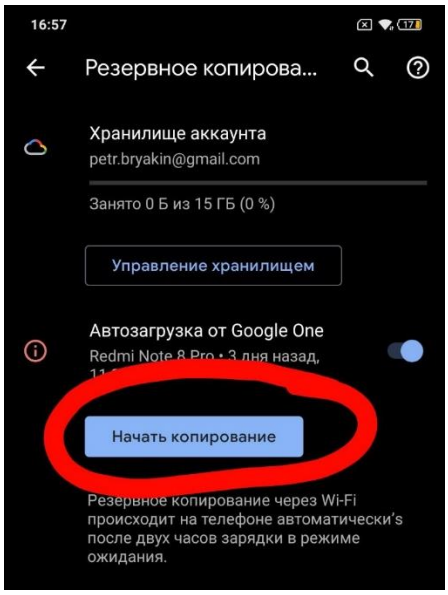
«Настройки» → «Приложения» → «Все приложения», выберите приложение и настройте «Разрешения приложений» и «Уведомления».





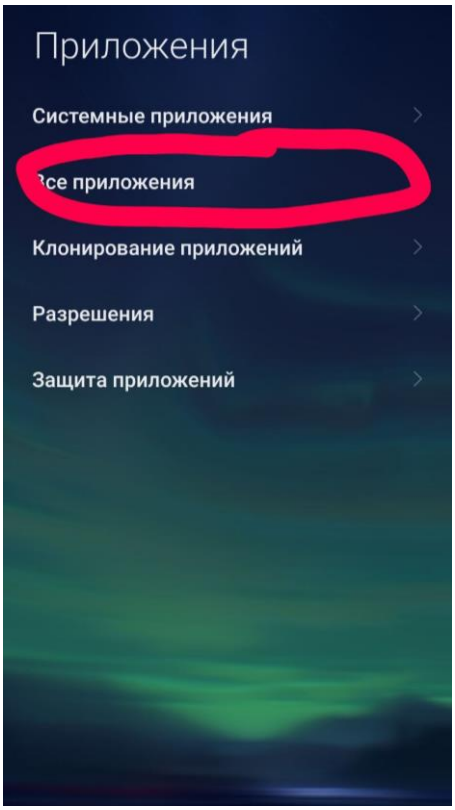
Создание резервных копий всех данных на телефоне

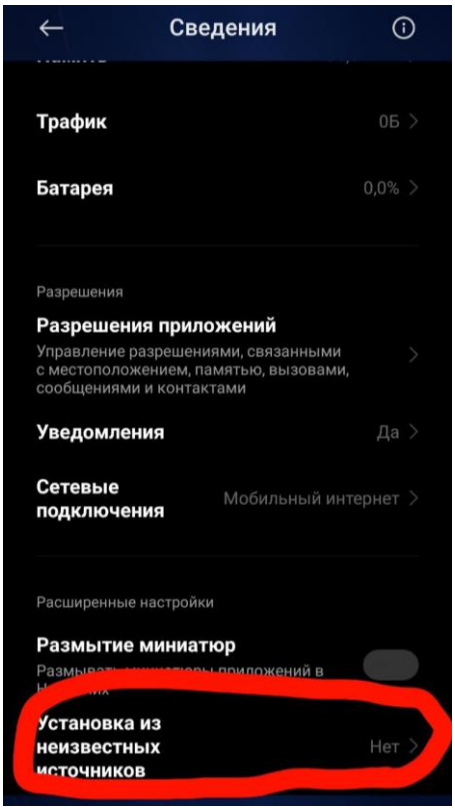
«Настройки» → «Google» → «Резервное копирование», выбрать аккаунт, на который будут сохраняться данные и тип сохраняемых данных, нажать кнопку «Начать копирование».



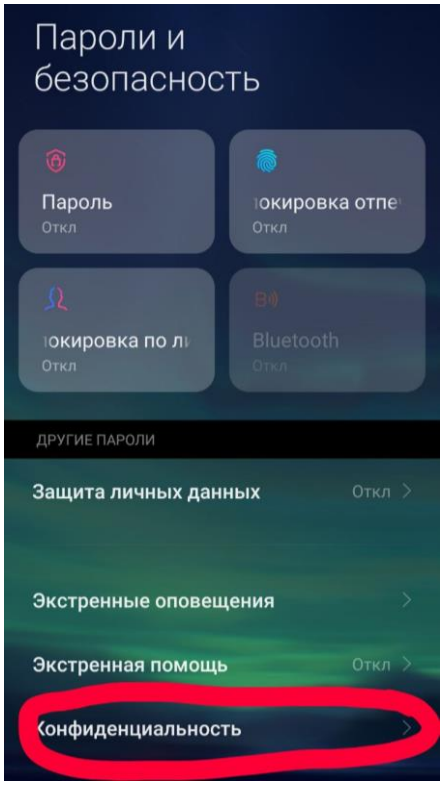
Загрузка приложений только из официальных источников

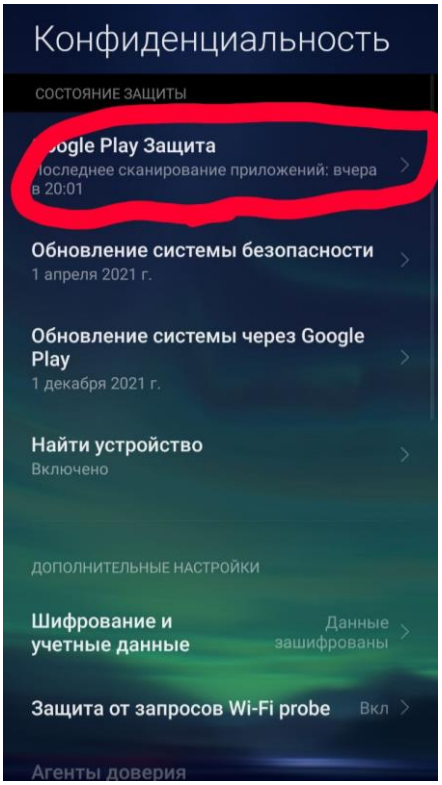
«Настройки» → «Приложения» → «Проводник», уберите галочку «Установка из неизвестных источников»

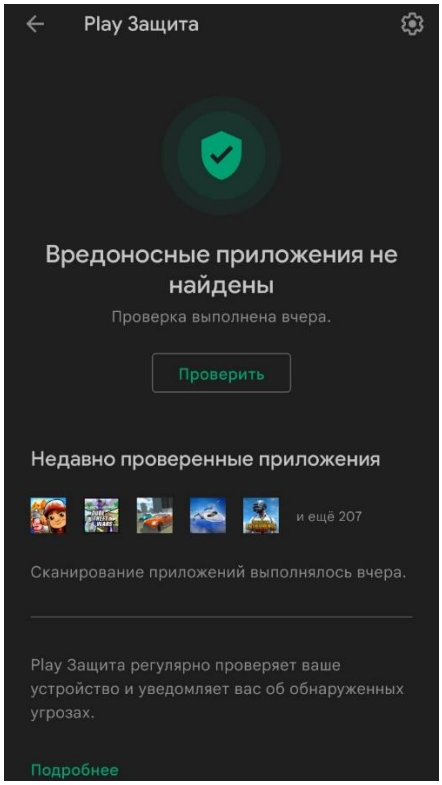




«Настройки» → «Пароли и безопасность» → «Конфиденциальность», убедитесь, что «GooglePlay Защита» активна.

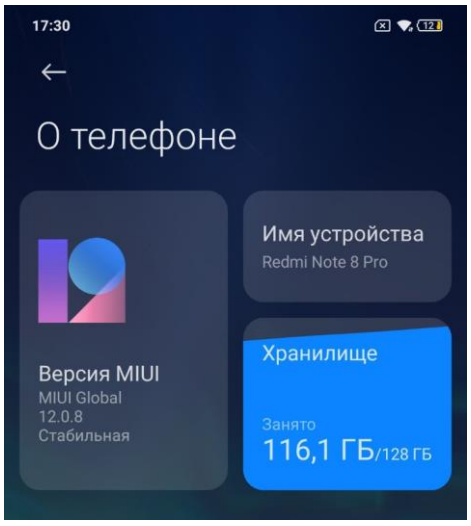






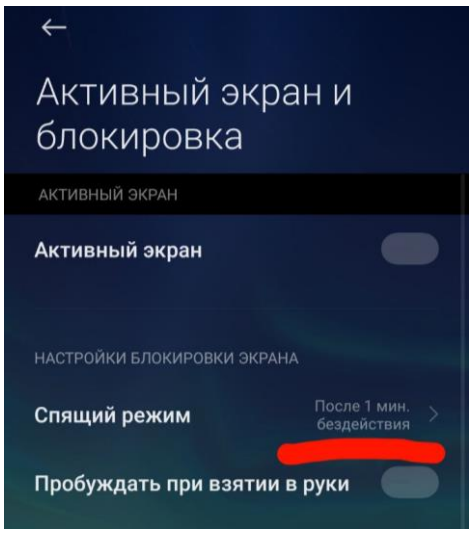
Регулярное обновление системы телефона

«Настройки» → «О телефоне» нажать на Версия MIUI, тут проверить обновление.



Быстрая блокировка

«Настройки» → «Блокировка экрана» → «Спящий режим»



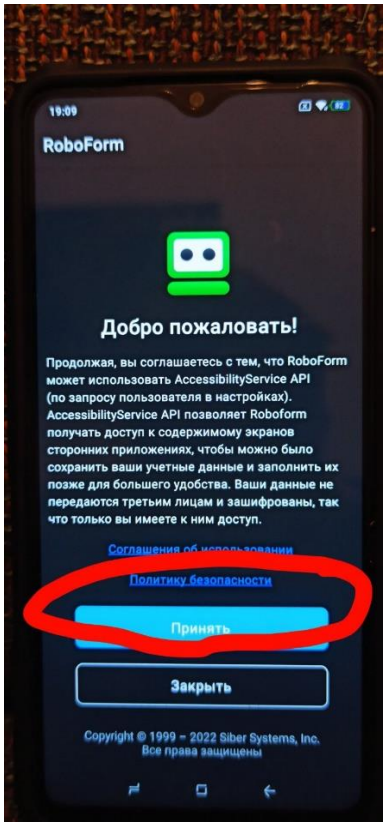
Ненужные приложения

«Настройки» → «Приложения» → «Все приложения». Вкладка «Все приложения» показана выше.

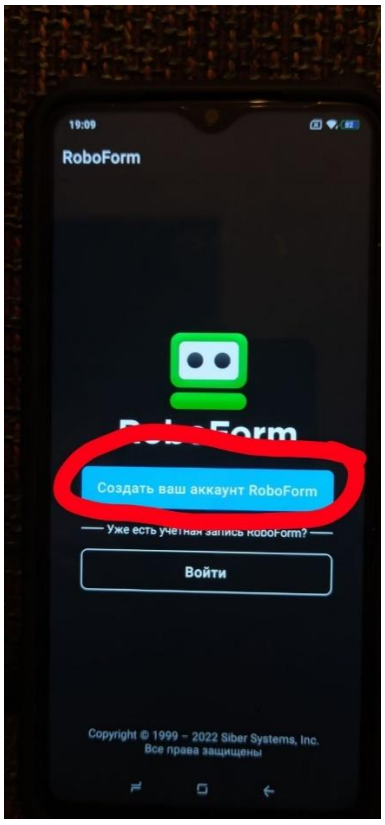
Приложение 4. Установка менеджера паролей RoboForm.

В части, где я устанавливал антивирус, было показано, как заходить в Google Play и устанавливать приложение. В случае с менеджером паролей в поиске необходимо ввести RoboForm.

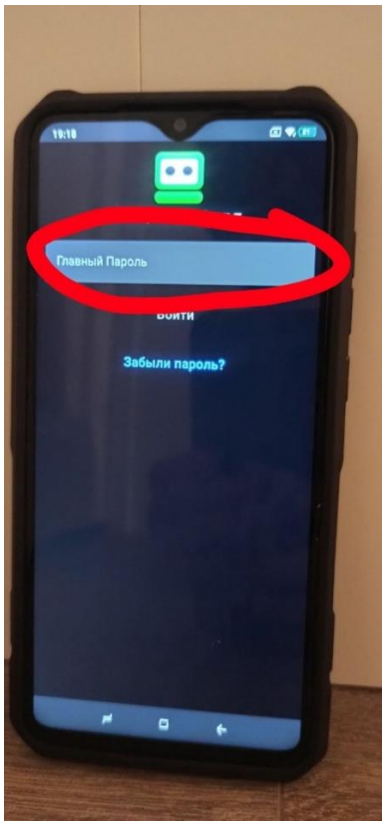
После установки приложения, открываем менеджер паролей RoboForm.



Нажимаем кнопку «Принять»

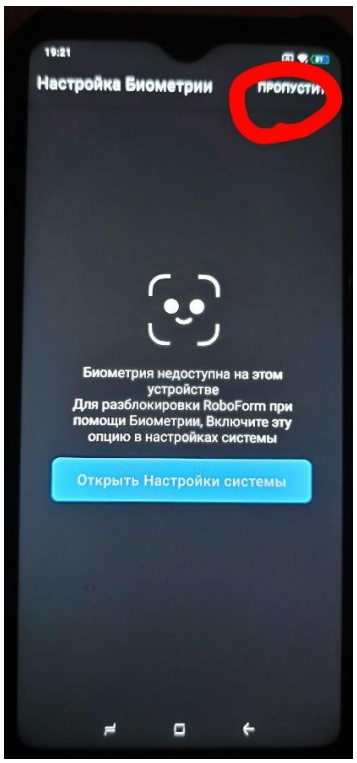


Нажимаем кнопку «Создать ваш аккаунт RoboForm»

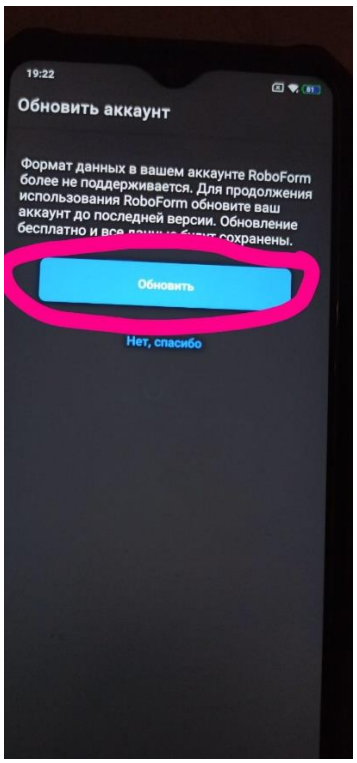


Вводим самый главный пароль(мастер-пароль)

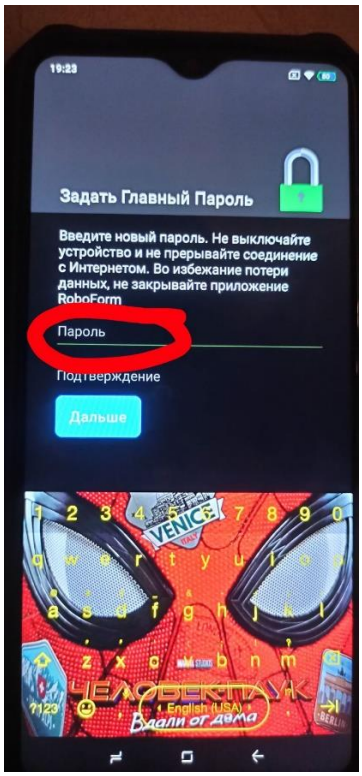
Вводим пин-код.



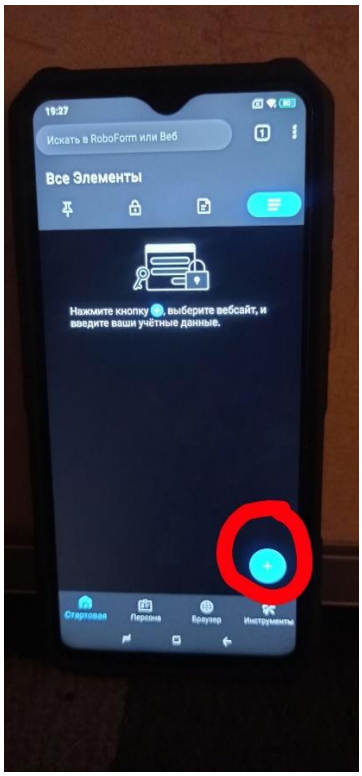
Настройка Биометрии, нажимаем пропустить.



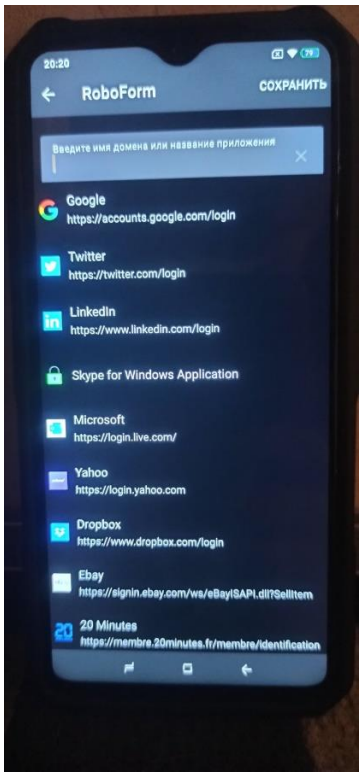
Программа может сказать что аккаунт старый, нажимаем «Обновить»



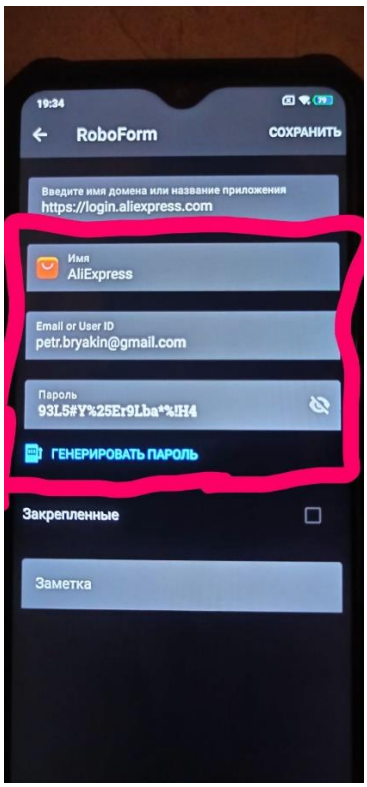
Вводим новый пароль или добавляем что-то к первому



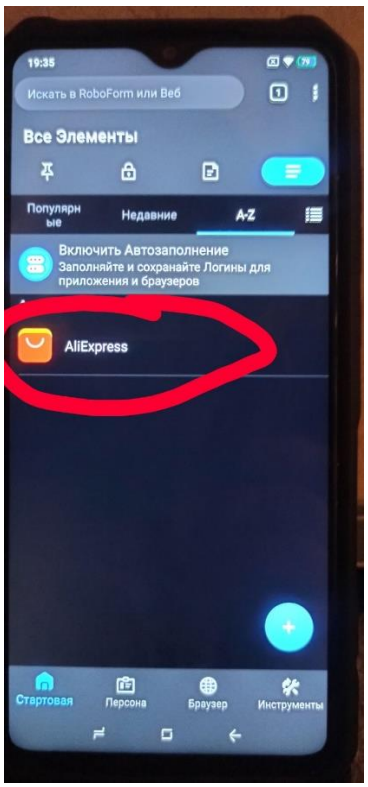
Нажимаем на плюс в правом нижнем углу



Выбираем сайт или приложение, для которого сохраняем пароль

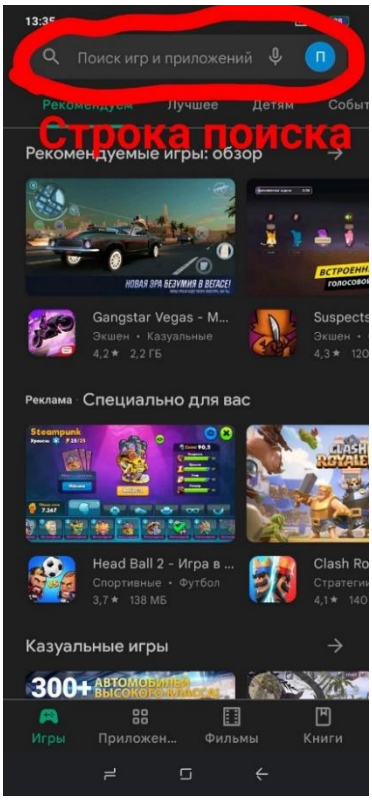


Заполняем данные от сайта/приложения. Пароль можно сгенерировать.

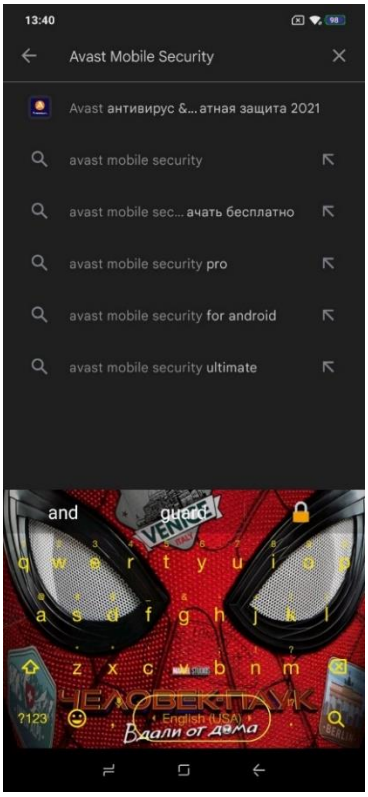


Поздравляю! Вы установили менеджер паролей и сохранили первый пароль.

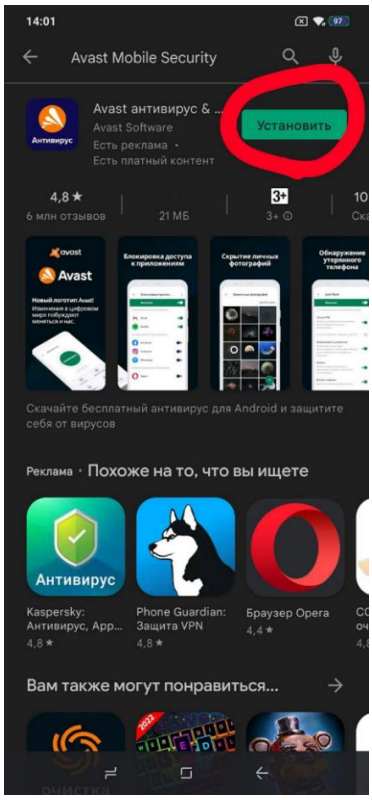
Приложение 5. Установка антивируса Avast Mobile Security.



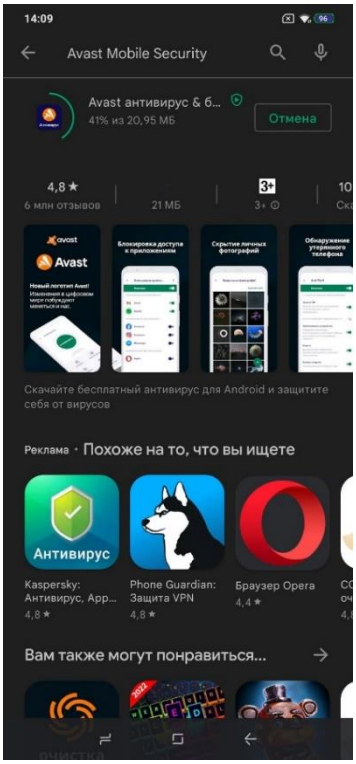
Заходим в «Google Play Market»



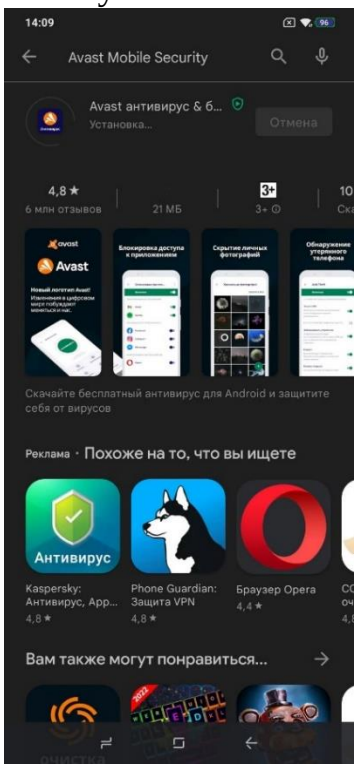
Пишем в строку поиска Avast Mobile Security



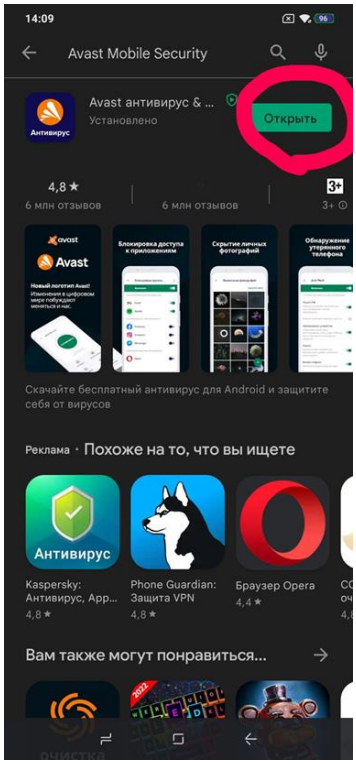
Нажимаем на кнопку «Установить»



Ждём, когда закончится процесс скачивания

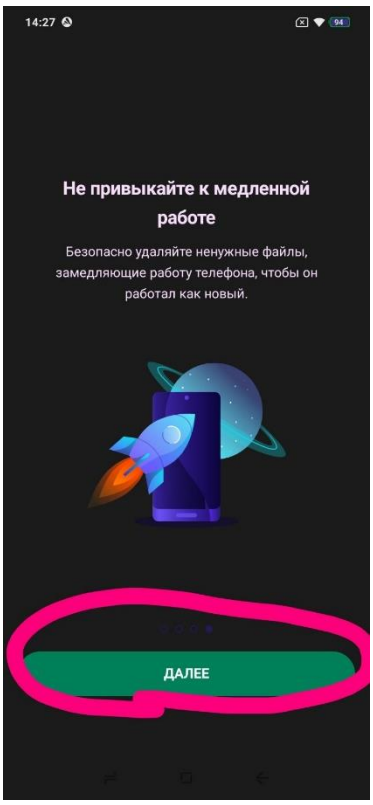


и установки.

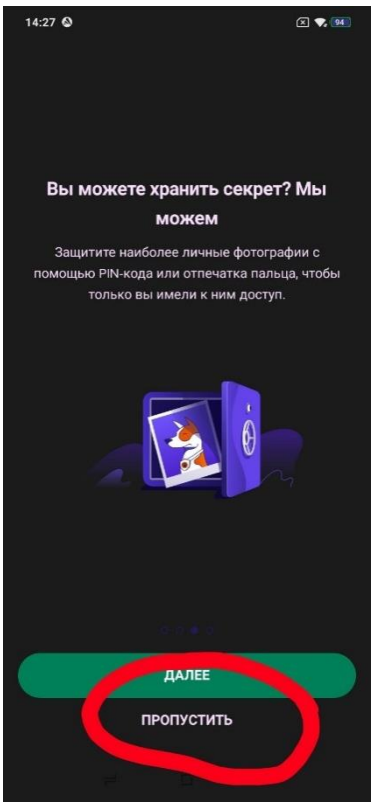


Нажимаем кнопку «Открыть»

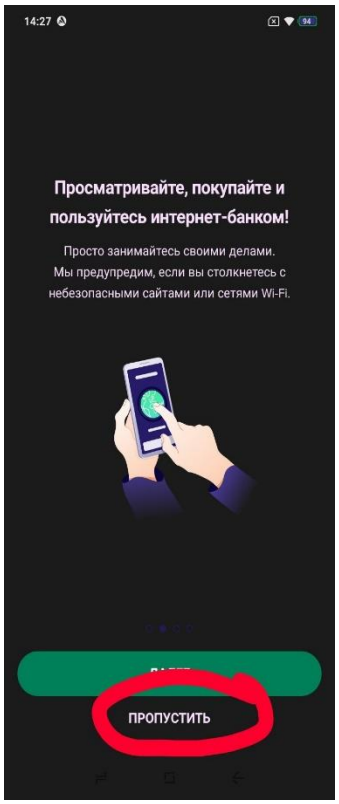
Нажимаем кнопку «Начать использование»



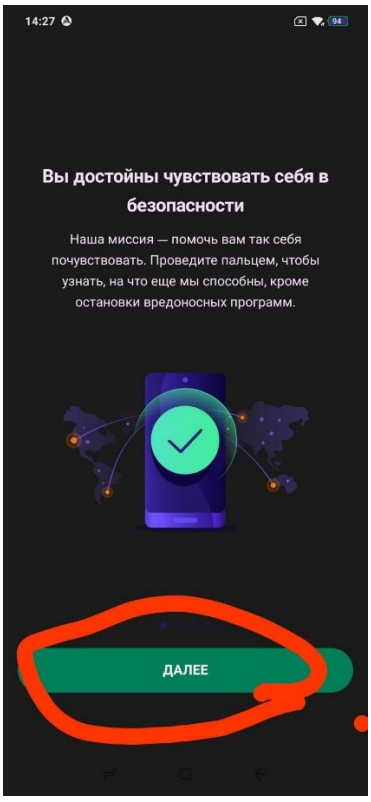
Нажимаем «Далее»



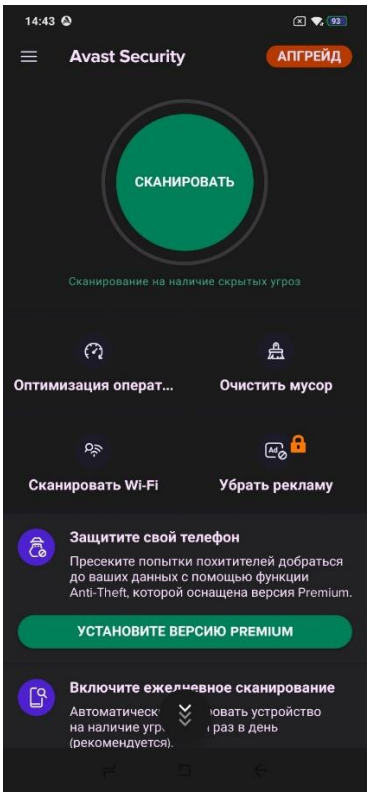
Нажимаем «Далее» или «Пропустить»



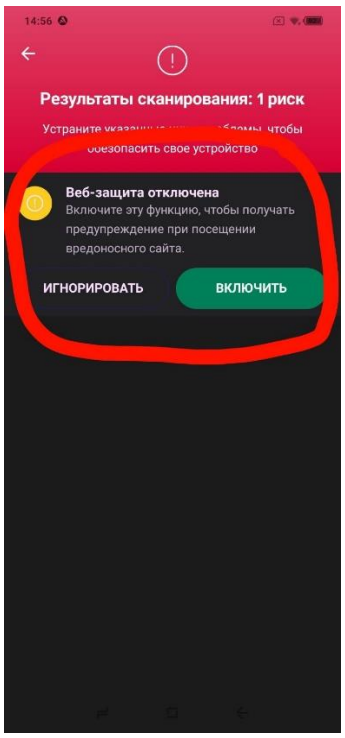
Нажимаем «Далее» или «Пропустить»



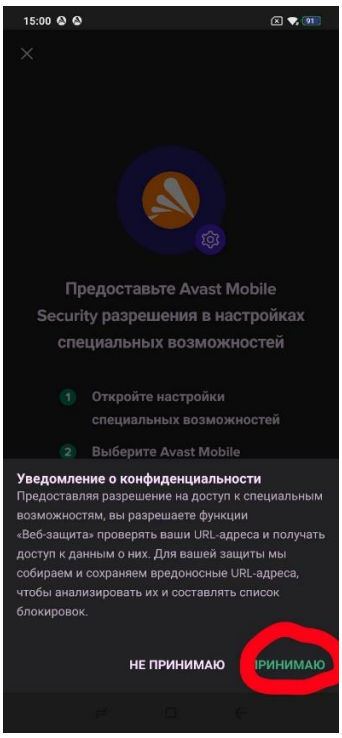
Нажимаем «Далее»



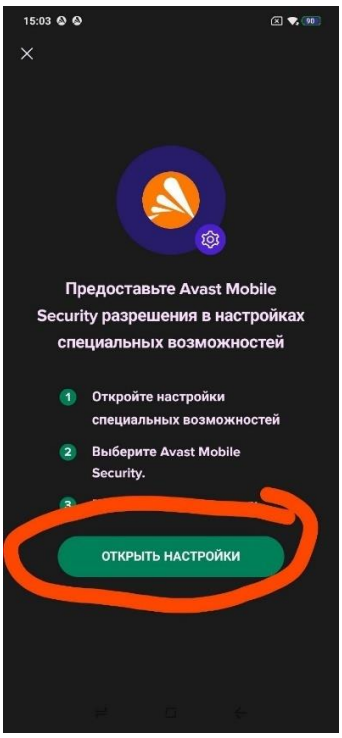
Нажимаем кнопку «Сканировать» и ждём окончания проверки.



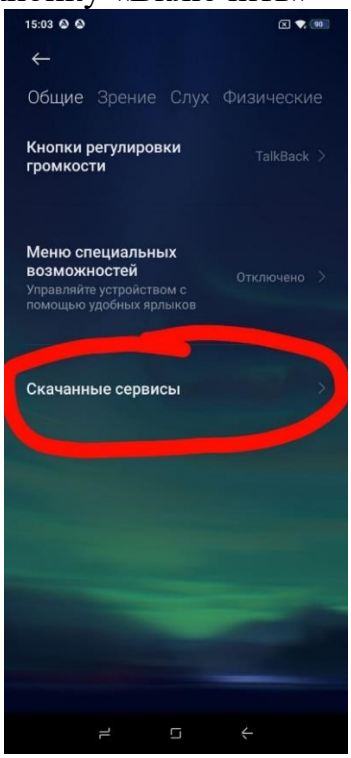
Если он выдаёт ошибку «Веб-защита отключена», нажимаем кнопку «Включить»



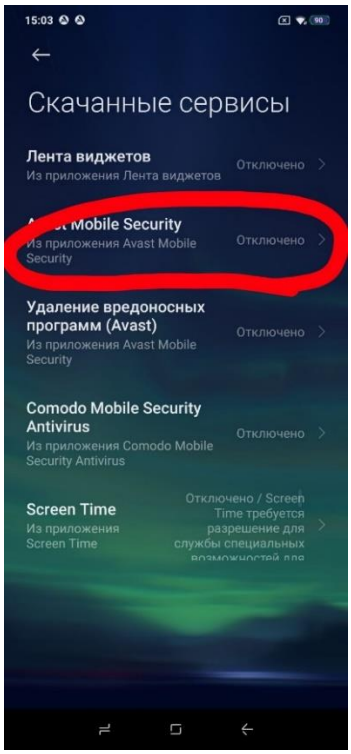
Нажимаем кнопку «Принимаю»



Нажимаем на кнопку «Открыть настройки»

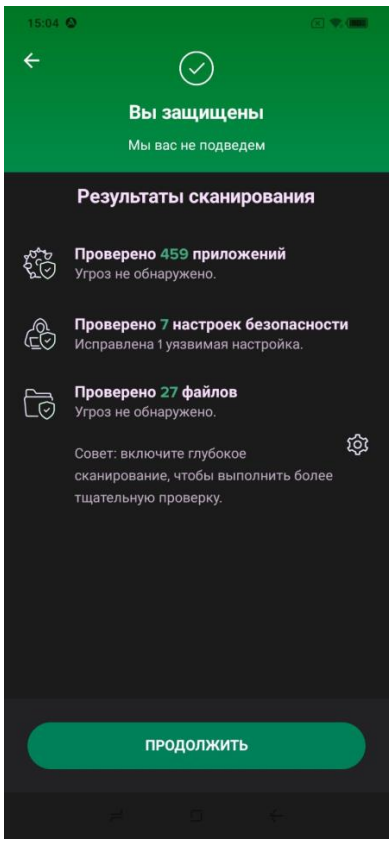


Нажимаем на кнопку «Скачанные сервисы»



Заходим в Avast Mobile Security

Нажимаем на переключатель «Включить возможность», после этого нажимаем «Разрешить»



Поздравляю! Вы установили и запустили антивирус.

Приложение 6. Памятка

13. Установите GPS-навигацию

Установите на смартфон приложение для навигации с офлайн картами. Приложение для навигации выберите любое, которое вам больше понравится.

14. Не оставляйте смартфон без присмотра и не давайте другим

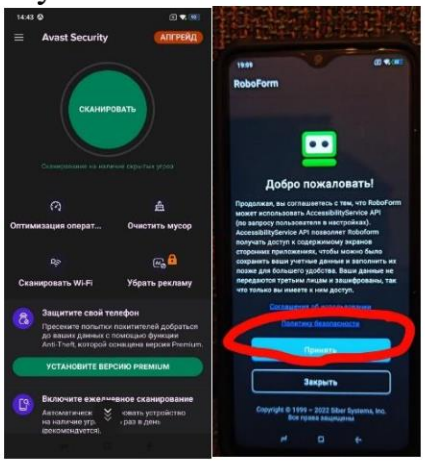
Пусть смартфон всегда будет в зоне вашего внимания или в укромном месте, например, сумке.

15. Установите на смартфон антивирус

Антивирус – это «китайская стена» внутри вашего смартфона, он защитит его от различного рода вирусов. Отсутствие антивируса на смартфоне ставит его под угрозу!
Советую установить Avast Mobile Security.

16. Установите на смартфон менеджер паролей

Менеджер паролей – это ваш личный банк для хранения паролей.
Советую установить RoboForm.



Соблюдение правил, изложенных в этой памятке, не даёт 100% гарантии защиты смартфона, но повышает её в разы, если даже вы выполните хотя бы половину из пунктов.

Любая информация, даже если вам она кажется незначительной, может быть использована злоумышленником. Поэтому защищать свои личные данные и всю информацию о себе нужно тщательно.
Никто не знает, какие уловки придумают завтра, но если всегда быть начеку, вероятность попадания в неприятную ситуацию снижается.

г. Пенза 2022 год

ЕДИНСТВО ВСЕХ СКВОЗЬ ПРИЗМУ УНИКАЛЬНОСТИ КАЖДОГО

МБОУ Гимназия №42

ПАМЯТКА

«Правила пользования, настройки и защиты смартфона»

Автор: Пётр Брякин
4 «А» класс

Как же защитить свой смартфон?

1. **Установить пароль на телефон**

Есть 5 способов заблокировать смартфон, лучшей защитой будет надёжный пароль или графический ключ.
«Настройки» → «Пароли и безопасность» → «Блокировка экрана»

2. **Отключить уведомления на заблокированном экране**

Отключите вывод содержания сообщений на экране блокировки.
«Настройки» → «Приложения» → «Все приложения», выберите приложение и уберите галочку «Показать уведомления».

3. **Установите двухфакторную авторизацию на сервисах**

Это тип входа в профиль на сервисе, когда после ввода основного пароля нужно ввести дополнительный.
Настраивается конкретно в каждом из сервисов, которыми пользуетесь.

4. **Настройте безопасность Wi-Fi подключений**

Старайтесь не подключаться к публичным бесплатным сетям, тем более без пароля. Удалите из истории смартфона не нужные вам сети. При раздаче Wi-Fi обязательно устанавливайте пароль WPA2-PSK.
«Настройки» → «Wi-Fi», нажмите на стрелочку нужной сети, в появившемся меню удалите ее.

5. **Следите за разрешениями и доступами приложений**

Строго следите за разрешениями, которые просят у вас приложения при установке или использовании.
«Настройки» → «Google» → «Настройки для приложений Google» → «Подключенные приложения» — отключите все лишние.
«Настройки» → «Приложения» → «Все приложения», выберите приложение и настройте «Разрешения приложений» и «Уведомления».

6. **Настройте создание резервных копий всех данных смартфона**

Регулярное копирование системы – ваша полезная привычка.
«Настройки» → «Google» → «Резервное копирование», выбрать аккаунт, на который будут сохраняться данные и тип сохраняемых данных, нажать кнопку «Начать копирование».

7. **Загружайте приложения только из официальных источников**

Используйте только официальные магазины приложений. Выбирайте приложения по количеству скачиваний, оценке не ниже 4 и количеству отзывов (их должно быть много). Не устанавливайте приложения с ненадежных сайтов. Включите Google Play Защиту.
«Настройки» → «Приложения» → «Проводник», уберите галочку «Установка из неизвестных источников»
«Настройки» → «Пароли и безопасность» → «Конфиденциальность», убедитесь, что «GooglePlay Защита» активна.

8. **Регулярно обновляйте систему смартфона**

Наличие свежей версии системы – критически важно для сохранения конфиденциальности данных.
«Настройки» → «О телефоне» нажать на Версия MIUI, тут проверить обновление.

9. **Не открывайте ссылки из писем, SMS сообщений или мессенджеров от незнакомых вам отправителей**
10. **Не храните важные вам личные фото и видео на смартфоне, копируйте на компьютер или ноутбук**
11. **Настройте быструю блокировку**

Экран смартфона должен блокироваться через 1 – 2 минуты бездействия.
«Настройки» → «Блокировка экрана» → «Спящий режим»

12. **Удалите ненужные приложения**

Не устанавливайте приложения, которыми не будете пользоваться. Удалите ненужные здесь:
«Настройки» → «Приложения» → «Все приложения»