# РАБОЧАЯ ТЕТРАДЬ

# по учебной программе

# **«ОСНОВЫ БЕЗОПАСНОЙ РАБОТЫ В СЕТИ ИНТЕРНЕТ»**

Ханты-Мансийск
2020

Учебный курс по программе «Основы безопасной работы в сети Интернет» : рабочая тетрадь. - Ханты-Мансийск, 2020 – 18 с.
Тираж 400 экз.

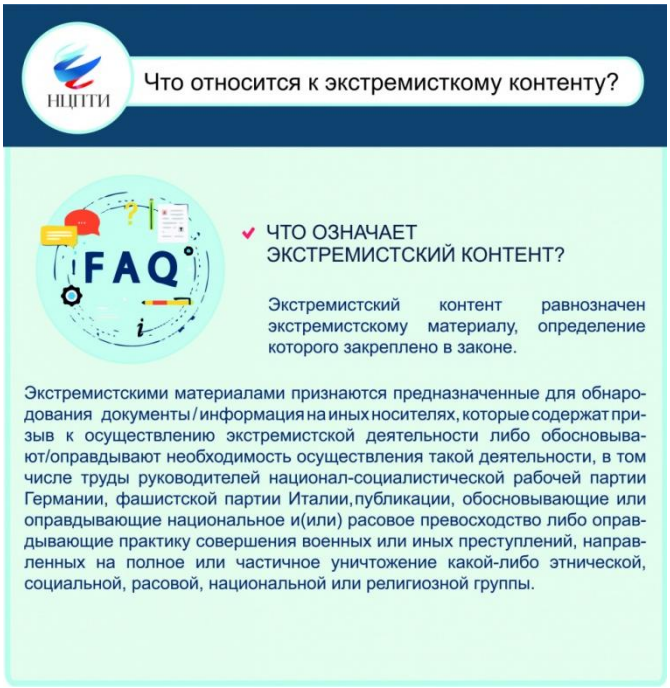
Разработано в автономном учреждении Ханты-Мансийского автономного округа – Югры «Югорский научно-исследовательский институт информационных технологий» по заказу Департамента информационных технологий и цифрового развития Ханты-Мансийского автономного округа – Югры

Данное учебное пособие предназначено для самостоятельной работы и использования слушателями курса «Основы безопасной работы в сети Интернет» для закрепления теоретического материала и формирования практических умений и навыков при подготовке к прохождению итогового тестирования.

# МОДУЛЬ 1. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПЕРСОНИФИЦИРОВАННОЙ РАБОТЫ С КОММУНИКАЦИОННЫМИ СЕРВИСАМИ

## ЗАДАНИЕ 1.1. Информационные ресурсы за «чистый интернет»

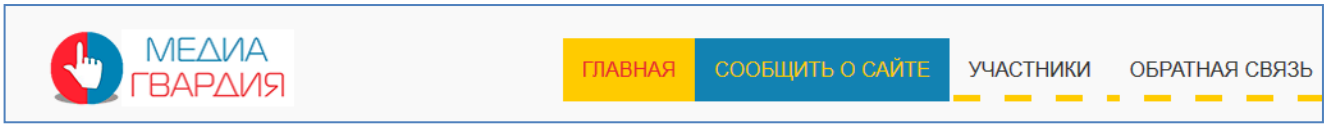
1. Запустите любой Интернет-браузер, установленный на Вашем компьютере.
2. Откройте сайт «Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет» (ncpti.su).
3. Перейдите в раздел «Материалы для скачивания», ознакомьтесь с инфографикой.

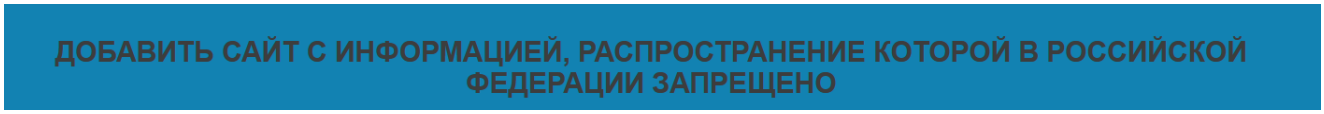



4. Скачайте заинтересовавшие вас материалы.
5. Перейдите на сайт «Молодежь за Чистый Интернет» (honestnet.ru) в раздел «Проблемы сегодня» - «Экстремизм».
6. Внимательно ознакомьтесь с содержимым данного раздела.

## ЗАДАНИЕ 1.2. Сообщить о «плохом» сайте

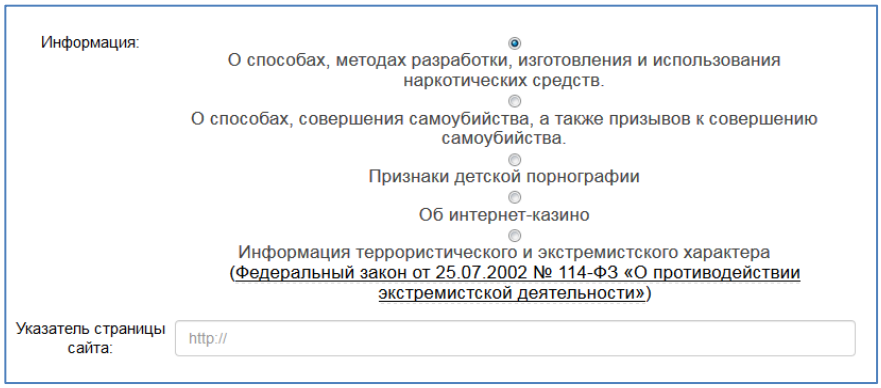
1. Откройте сайт «Медиа Гвардия» (mediagvardia.ru)
2. Зайдите в раздел «Сообщить о сайте».



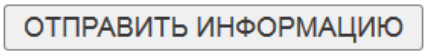




3. Система предложит авторизоваться через социальную сеть или зайти анонимно.


4. Откроется форма для подачи сообщения о ресурсе, содержащем запрещенную информацию.



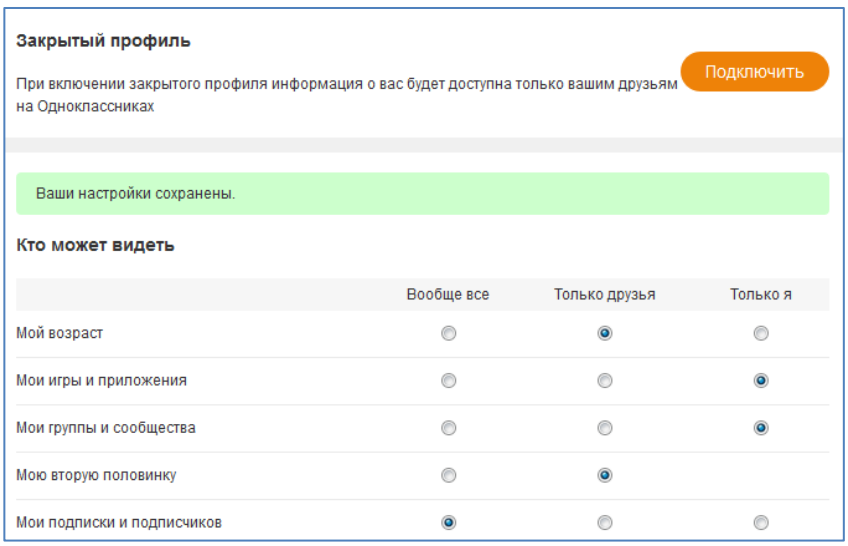

5. Заполните необходимые поля и нажмите кнопку




6. После этого Ваша заявка будет рассмотрена специалистами данного проекта и если материал действительно нарушает законодательство, он будет направлен на рассмотрение в Генеральную прокуратуру РФ или Роскомнадзор для блокировки.

## ЗАДАНИЕ 1.3. Ограничение доступа к вашим личным данным

1. Откройте сайт любого коммуникационного сервиса (далее на примере социальной сети «Одноклассники»).
2. Авторизуйтесь в системе.
3. Через меню профиля зайдите в раздел «Публичность» и проверьте настройки ограничения доступа к вашим личным данным.



4. Если есть возможность, ограничьте доступ к вашим личным данным по максимуму, который обеспечит Вам комфортное использование данного сервиса.
5. Если вы хотите знакомиться и активно общаться, закройте доступ хотя бы для тех пользователей, которые не входят в список ваших друзей. В настройках стоит отдавать предпочтение столбикам «Только я», «Только друзья».

# МОДУЛЬ 2. КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ И ИНТЕРНЕТ-БЕЗОПАСНОСТЬ

## ЗАДАНИЕ 2.1 Вредоносные программы

Отметьте галочкой виды программ, которые Вы считаете вредоносными:

| | |
|---|---|
| Вирус | |
| Черви | |
| Троянская программа | |
| Веб-браузер | |
| Фишинговая программа | |
| Клавиатурный шпион | |
| Виджеты | |
| Рекламные системы (adware) | |

## ЗАДАНИЕ 2.2 Признаки заражения системы

Перечислите известные Вам признаки того, что Ваш компьютер заражен вирусом:

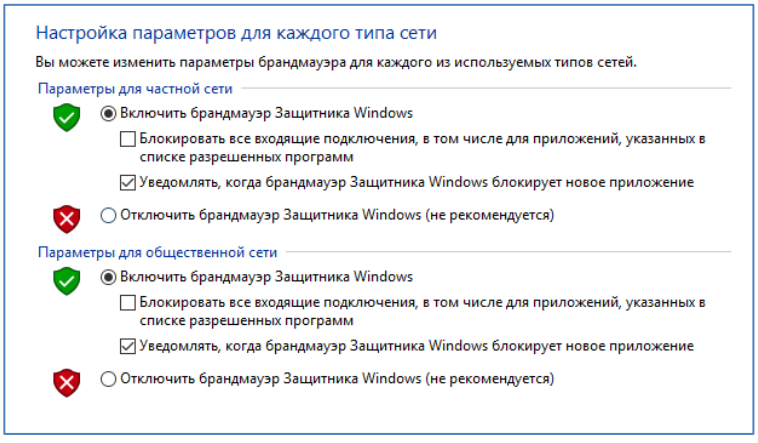
1)_____

2)_____

3)_____

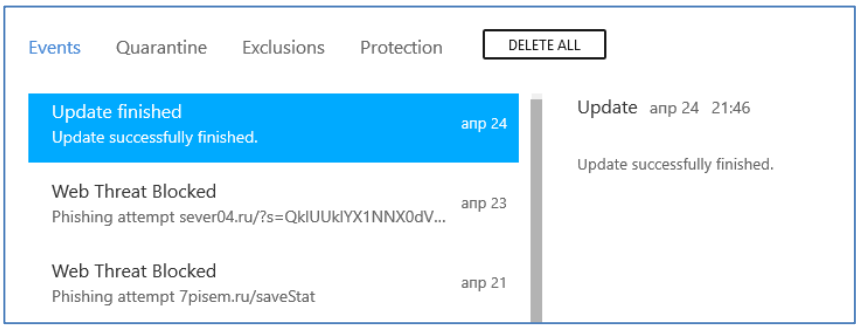
## ЗАДАНИЕ 2.3 Оценка защищенности компьютера

1. Откройте меню «Пуск» и выберите «Панель управления».
2. Откройте «Система и безопасность» - «Брандмауэр защитника Windows» - «Настроить параметры».

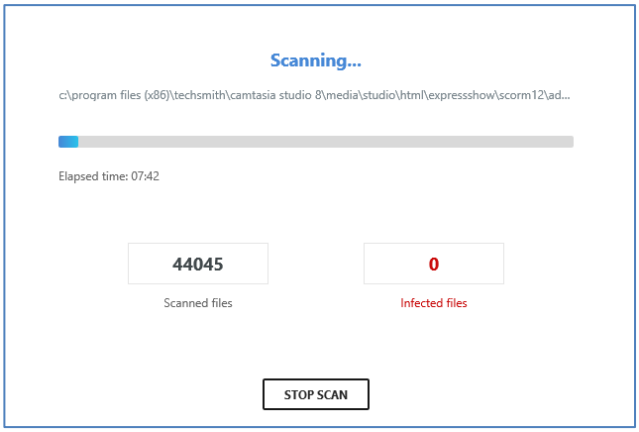


3. Выберите необходимые настройки и закройте окно.
4. Определите, какой антивирус установлен на Вашем компьютере. Обычно в области уведомлений можно увидеть значок программы (показано на примере Bitdefender).


5. Откройте интерфейс антивирусной программы и проверьте актуальность антивирусных баз.



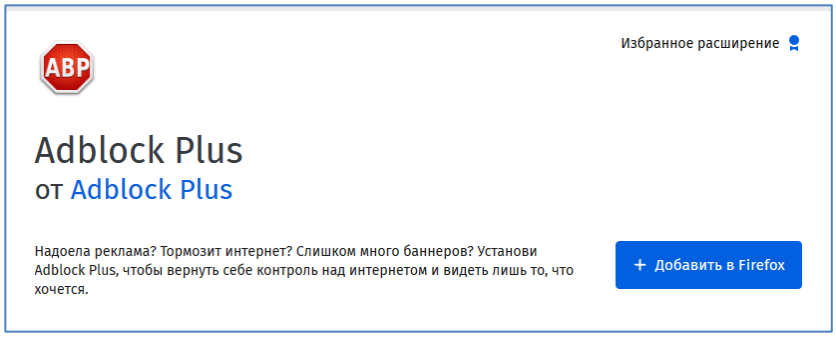

6. Запустите сканирование системы.




7. По итогам проверки удалите зараженные файлы.

## ЗАДАНИЕ 2.4 Блокировка рекламы в браузере

1. Откройте сайт поисковой системы и сделайте запрос «блокировка рекламы “наименование браузера”».
2. Один из вариантов поисковой выдачи - расширение браузера для блокировки рекламы Adblock Plus.

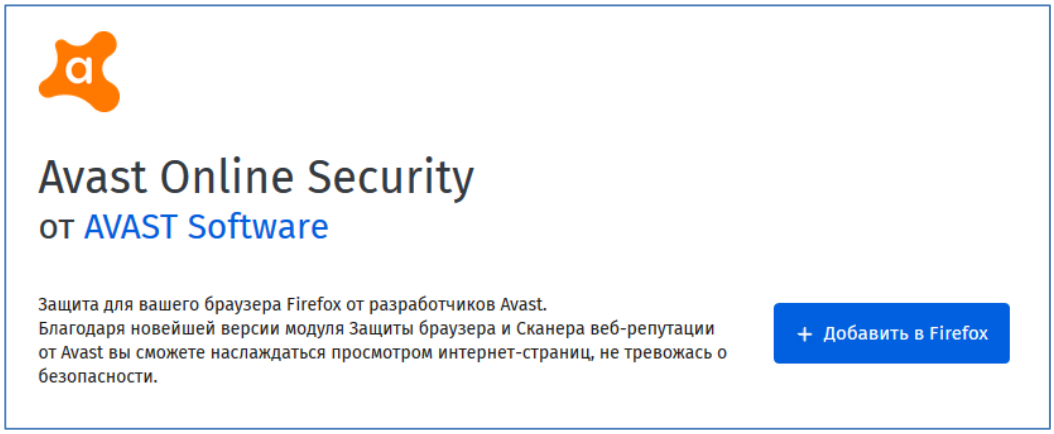


3. Нажмите кнопку «Добавить».
4. Расширение встроится в Интернет-браузер, и его пиктограмма появится в панели инструментов.

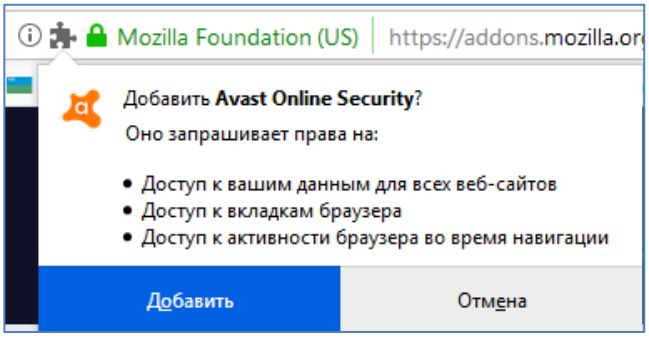

5. Теперь при просмотре Интернет-сайтов будет блокироваться реклама, выскакивающие сверху окна, мигающие баннеры и т. д. Когда эта раздражающая реклама заблокирована, страницы загружаются быстрее.

## ЗАДАНИЕ 2.5 Проверка сайта с Avast Online Security

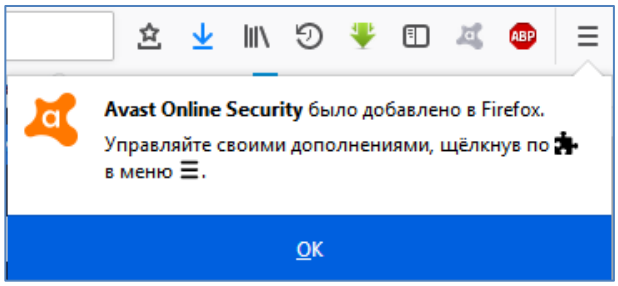
1. Откройте сайт поисковой системы и сделайте запрос «avast online security “наименование браузера”».
2. Система выдаст ссылку на расширение для браузера Avast Online Security.
3. Нажмите кнопку «Добавить».



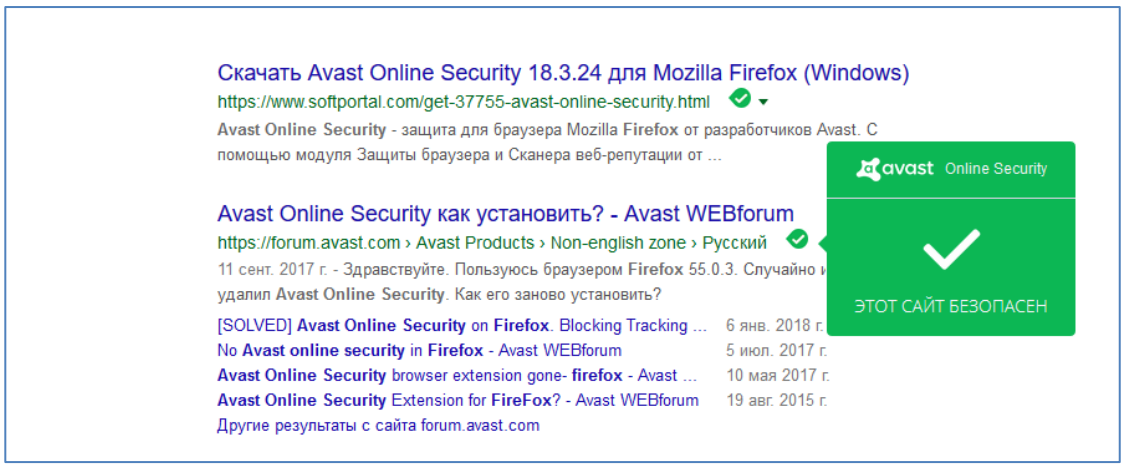

4. В процессе установки дайте запрашиваемые разрешения.




5. Расширение встроится в Интернет-браузер



6. Если наведете курсор на результат поисковой выдачи, то получите результат анализа данного сайта.




## ЗАДАНИЕ 2.6 Проверка гиперссылки

1. Откройте сайт «Цифровой гражданин Югры» (eduhmao.ru)
2. Наведите курсор мышки на раздел меню «Контакты».
3. Проверьте ссылку, отображаемую в левом нижнем углу браузера и впишите ее в поле ниже:

_____

## ЗАДАНИЕ 2.7 Проверка шифрованного соединения

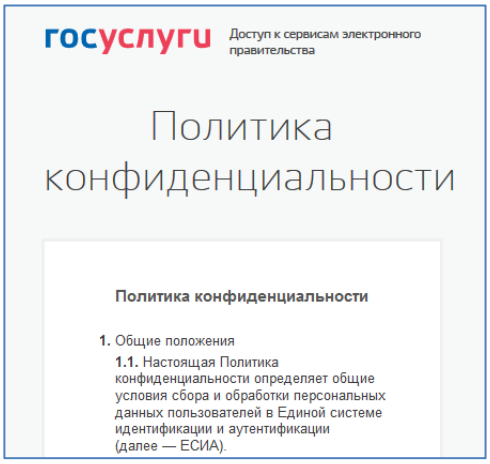
1. Откройте портал госуслуг (gosuslugi.ru).
2. Для того чтобы определить, является ли данное соединение шифрованным, обратите внимание на адресную строку браузера.


3. Пиктограмма закрытого замка обозначает шифрованное соединение.
4. Откройте следующие сайты для проверки соединения:
   Все самое интересное из мира IT-индустрии (3dnews.ru)
   Молодежь за Чистый Интернет (honestnet.ru)
   Единый официальный сайт государственных органов (admhmao.ru)
5. Впишите наименование сайта с незащищенным соединением:

_____

## ЗАДАНИЕ 2.8 Политика конфиденциальности

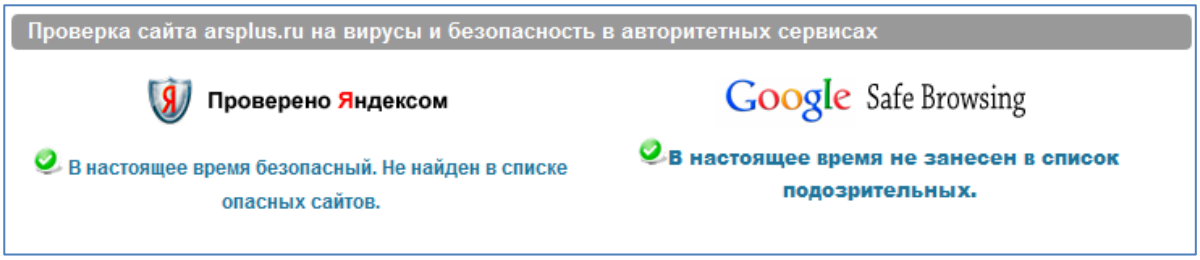
1. Откройте портал госуслуг (gosuslugi.ru).
2. Перейдите в раздел «Правовая информация».
3. Найдите в данном разделе политику конфиденциальности и ознакомьтесь с ней.




## ЗАДАНИЕ 2.9 Определение степени доверия сайту

1. Откройте сайт [довериевсети.рф](довериевсети.рф)
2. Определите степень доверия к сайту [https://arsplus.ru/](https://arsplus.ru/)
3. Чтобы проверить сайт на мошенничество необходимо вставить адрес сайта в форму и нажать кнопку "Проверка сайта".

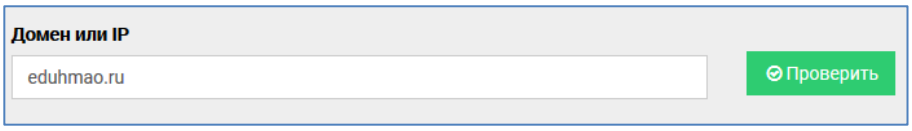

4. В результате вы получите информацию о положительном уровне доверия.




5. Попробуйте проверить сайт, на который вы часто заходите.

## ЗАДАНИЕ 2.10 Проверка домена

1. Откройте один из сервисов для проверки доменов (например, 2whois.ru).
2. В онлайн-форме на главной странице укажите проверяемый домен, например портал «Цифровой гражданин Югры» (eduhmao.ru).




3. По результатам проверки определите, когда был создан данный домен и впишите в поле ниже:

_____

## ЗАДАНИЕ 2.11 Безопасные ресурсы в сети Интернет

Приведите примеры популярных информационных (новостных) сайтов или государственных порталов, как наименее опасных ресурсов в сети Интернет.

1)_____

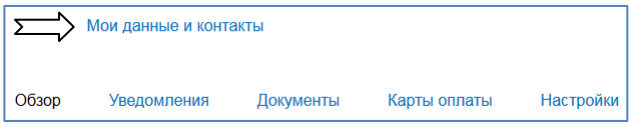
2)_____

3)_____

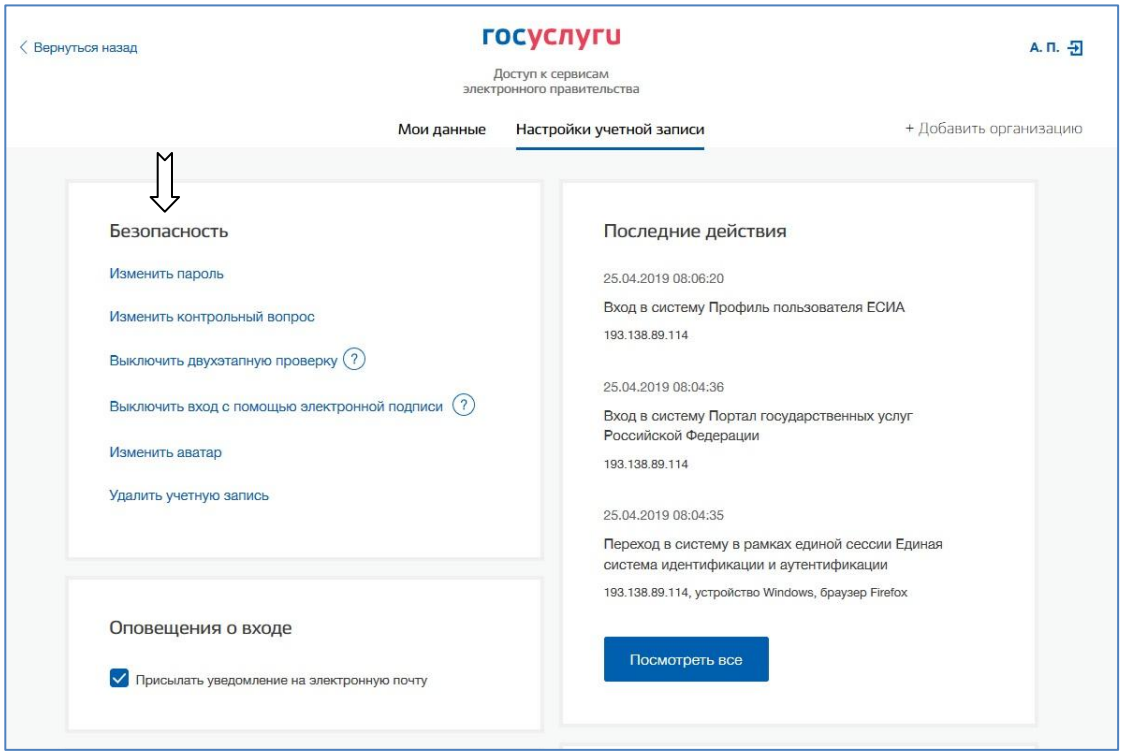
# МОДУЛЬ 3. НАВЫКИ БЕЗОПАСНОЙ РАБОТЫ В СЕТИ ИНТЕРНЕТ И СОЦИАЛЬНЫХ СЕТЯХ

## ЗАДАНИЕ 3.1 Настройки безопасности в личном кабинете

1. Откройте портал госуслуг (gosuslugi.ru).
2. Перейдите в «Личный кабинет» - «Мои данные и контакты» - «Настройки учетной записи».

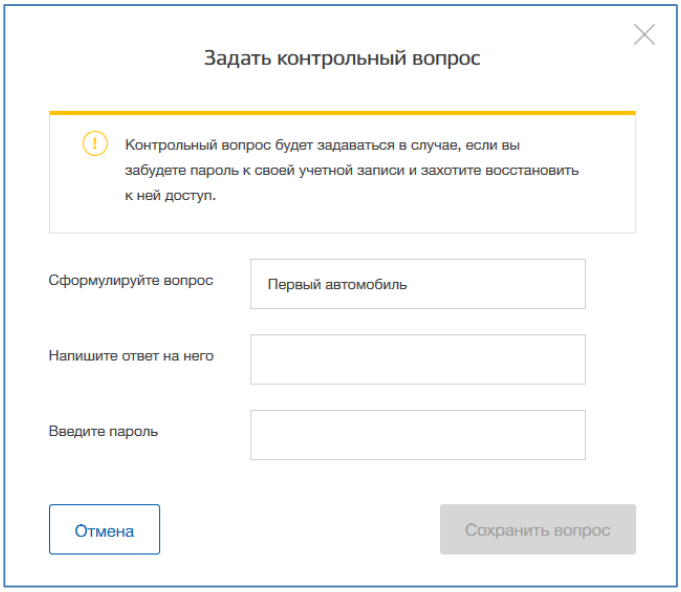



3. Ознакомьтесь с содержанием раздела «Безопасность».




4. Произведите настройки безопасности Вашего личного кабинета в соответствии с рекомендуемыми требованиями безопасности:
   Надежный пароль
   Контрольный вопрос

Двухэтапная проверка включена (двухфакторная аутентификация)
Оповещение о входе включено

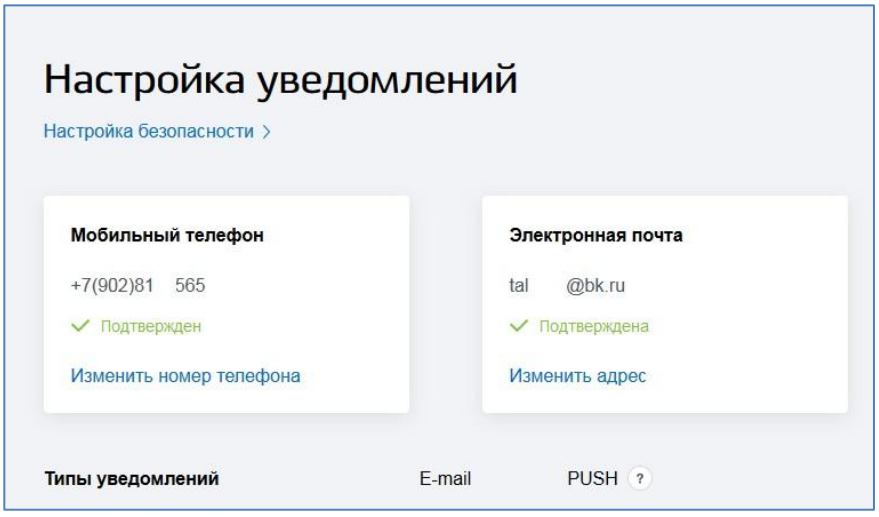



5. Выйдите из личного кабинета.

**Внимание!**
**Двухфакторная аутентификация – одна из обязательных процедур для защиты ЛК. Авторизация будет происходить в два этапа. После авторизации с помощью пароля необходимо подтвердить вход при помощи кода, который будет отправлен в SMS-сообщении на указанный номер телефона.**
**Даже если ваш пароль взломают или украдут, второй этап авторизации по телефону обеспечит вашу безопасность!**

## ЗАДАНИЕ 3.2 Настройки уведомлений в личном кабинете

1. Откройте портал госуслуг (gosuslugi.ru).
2. Перейдите в Личный кабинет - «Настройки».
3. Произведите настройку уведомлений, указав контактную информацию.



4. Теперь при каждом входе в Личный кабинет на указанные контакты будет приходить уведомление.

## ЗАДАНИЕ 3.3 Формирование надежного пароля

1. Придумайте алгоритм для составления паролей. Например, возьмите за основу любимое стихотворение или изречение. Запишите его строчными и заглавными латинскими буквами и замените некоторые из них похожими цифрами или символами: I_p0Mn|O_4y9n0e Mg№vEn|E (Я помню чудное мгновенье).
2. В качестве альтернативного варианта воспользуйтесь генератором паролей, например, Kaspersky Password Manager.
3. Запишите полученные результаты в поле ниже:

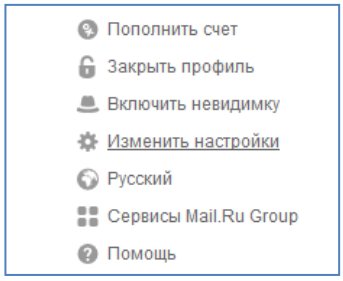
_____

_____

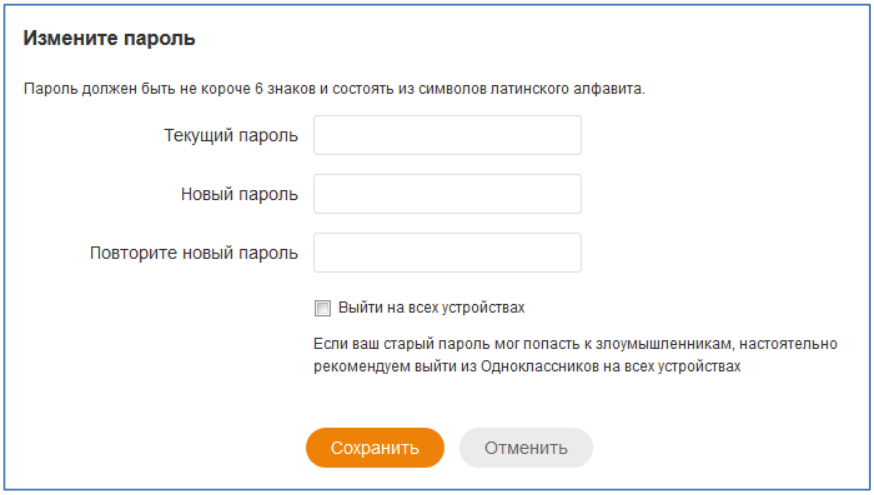
**Внимание!**
**Для создания надежного пароля рекомендуется использовать буквы как нижнего, так и верхнего регистра, а также цифры и другие символы.**

## ЗАДАНИЕ 3.4 Настройки безопасности для профиля социальной сети

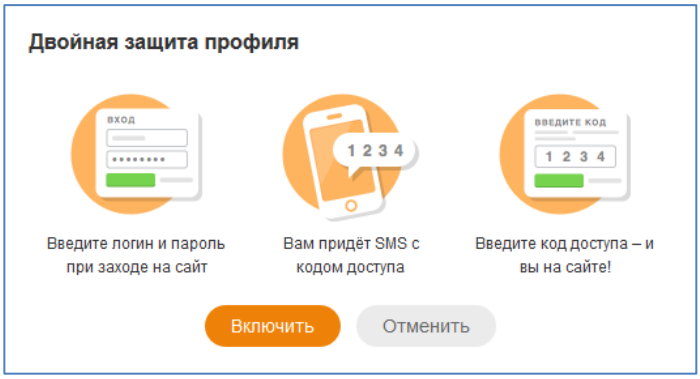
1. Откройте сайт социальной сети «Одноклассники» (Вконтакте и др.).
2. Авторизуйтесь в системе.
3. Кликните меню профиля и выберите «Изменить настройки.



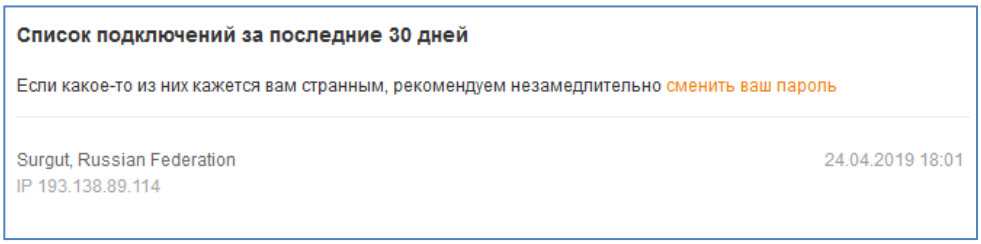

4. Измените настройки профиля на вкладке «Основные», в том числе пароль с учетом данных рекомендаций



а также использование двойной защиты




5. Просмотрите историю посещений




6. Завершите работу с настройками и выйдите из профиля.

**Внимание!**
**Не регистрируйтесь в социальных сетях под чужими именами! Если хотите сохранить инкогнито – используйте псевдоним. Не используйте чужие изображения, особенно это касается реальных людей.**

### ЗАДАНИЕ 3.5 Безопасное общение в социальных сетях

Перечислите основные правила общения в социальных сетях, соблюдение которых избавит Вас от возможного обмана, хамства и прочих неприятных ситуаций:

_____

_____

_____

_____

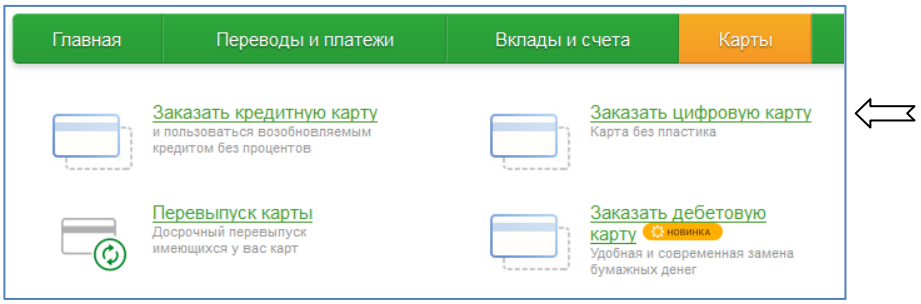
_____

## МОДУЛЬ 4. МЕРЫ ПРЕДОСТОРОЖНОСТИ ПРИ ПРОВЕДЕНИИ ИНТЕРНЕТ-ТРАНЗАКЦИЙ

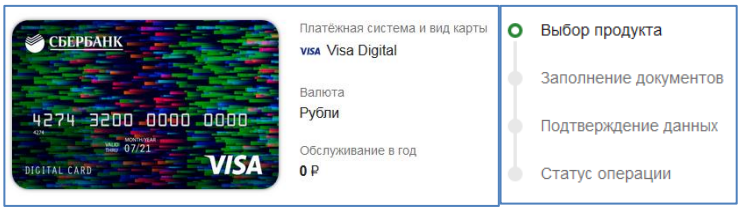
### ЗАДАНИЕ 4.1 Создание виртуальной платежной карты (пользователям Сбербанк Онлайн)

1. Авторизуйтесь в системе Сбербанк Онлайн.

2. На вкладке «Карты» выберите «Заказать цифровую карту».




3. Следуя дальнейшим инструкциям, пройдите все этапы оформления виртуальной карты.



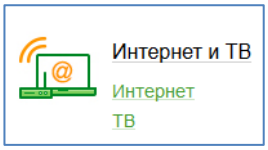

4. Проверьте список Ваших карт


5. Используйте данную карту для онлайн платежей, не храня на ней большие суммы денег.

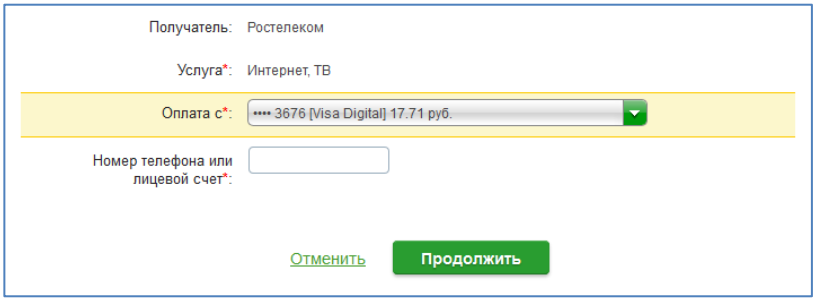
**Внимание!**
**Для оплаты онлайн, в целях безопасности, лучше иметь отдельную банковскую карту с небольшой суммой на счете. Удобно использовать виртуальную карту!**

## ЗАДАНИЕ 4.2 Оплата услуг

1. Авторизуйтесь в системе Сбербанк Онлайн.
2. На вкладке «Переводы и платежи» выберите например, «Интернет» и поставщика услуги.



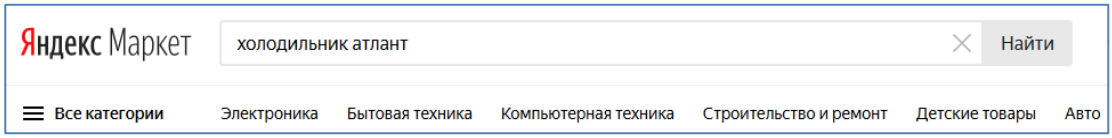

3. Выберите карту списания, лицевой счет и после указания суммы произведите оплату.



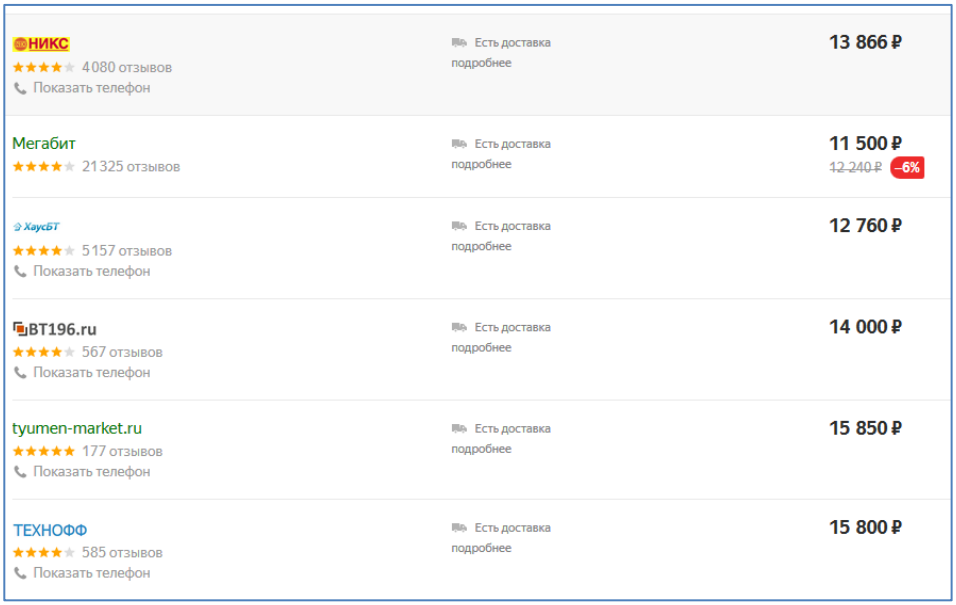
4. Выйдите из Личного кабинета.

### ЗАДАНИЕ 4.3 Выбор Интернет-магазина

1. Откройте сервис для поиска и подбора товаров Яндекс.Маркет (market.yandex.ru)
2. Напечатайте поисковый запрос по интересущему Вас товару.




3. Для приобретения нужного товара выберите подходящий магазин, учитывая его рейтинг и отзывы покупателей с целью минимизации рисков обмана.

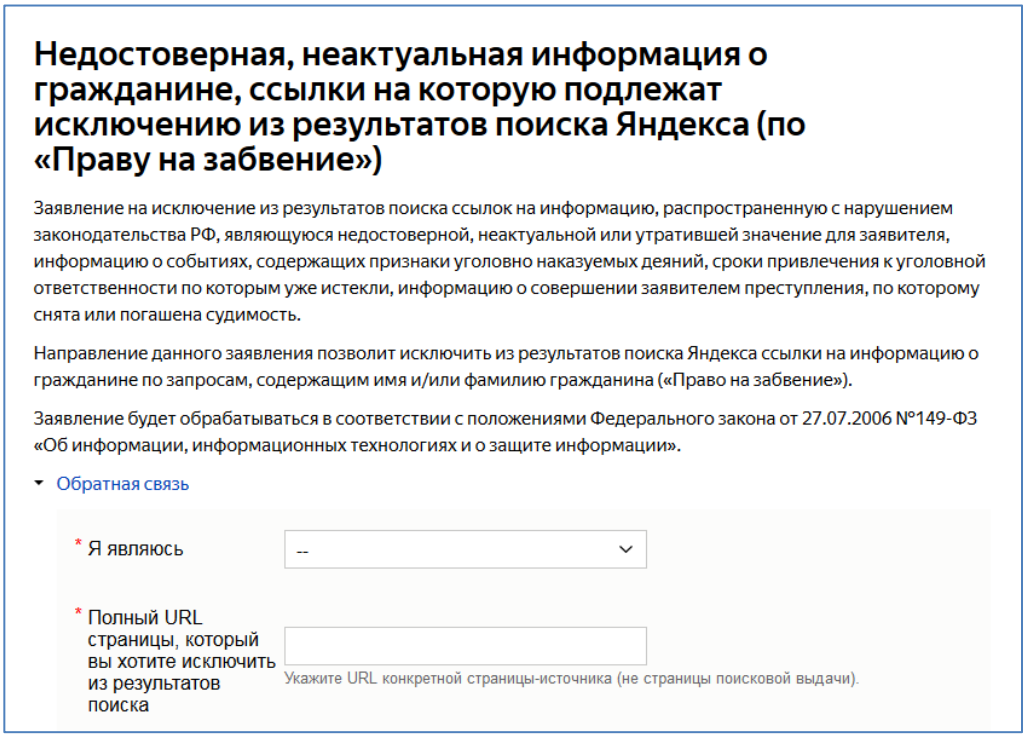



**Внимание!**
**При выборе магазина будьте осторожны. Надежный интернет-магазин имеет ряд отличительных признаков: контактные данные с адресом офиса; менеджеры открыты к диалогу; сайт выглядит красиво и работает без сбоев; отзывы реальных покупателей; доступны различные способы оплаты и доставки.**

## МОДУЛЬ 5. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

### ЗАДАНИЕ 5.1 Удаление данных из поисковой выдачи Яндекс (право на забвение)

1. Откройте страницу сервиса Яндекс.Помощь «Сообщить о нарушении» (по ссылке yandex.ru/support/abuse), а далее «Поиск» - «Общий поиск» - «Недостоверная, неактуальная информация о гражданине, ссылки на которую подлежат исключению из результатов поиска Яндекса (по «Праву на забвение»)».
2. Впишите свои персональные данные и актуальные контакты (достаточно будет адреса электронной почты), чтобы сотрудники поисковика могли связаться с Вами.

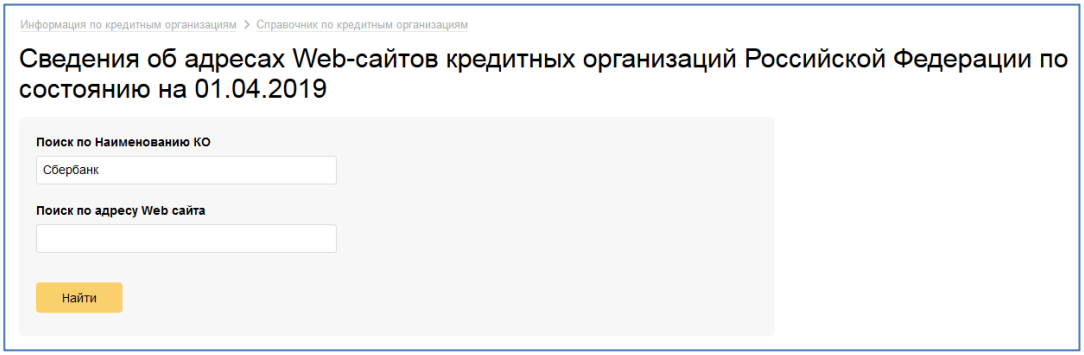



3. Приложите скан паспорта.
4. Скопируйте все ссылки, которые хотите удалить из поисковой выдачи. Важно, чтобы это были прямые ссылки на нежелательный контент.
5. Укажите категорию, к которой относится информация: недостоверная, неактуальная или противоправная.
6. Объясните, почему вы считаете эти данные некорректными. Если есть доказательства вашей позиции, приложите их (это может быть ссылка на другую информацию, говорящую в Вашу пользу, сканы решения суда и т.п.).
7. Дайте поисковику согласие на обработку персональных данных.
8. Заявление будет обработано за 10 рабочих дней.

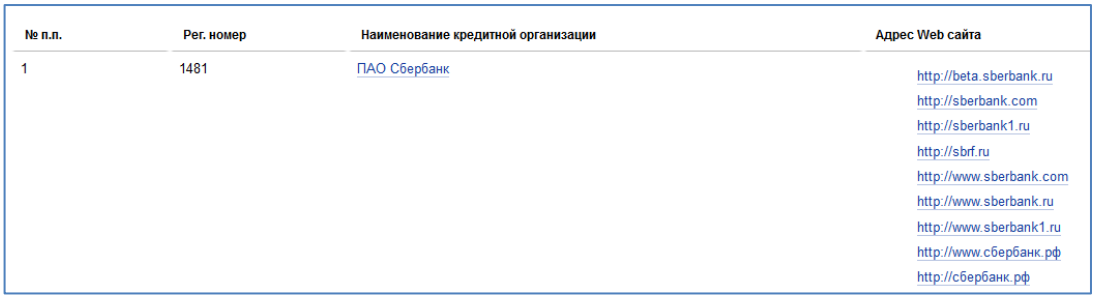
# МОДУЛЬ 6. КИБЕРБЕЗОПАСНОСТЬ

## ЗАДАНИЕ 6.1 Проверка адреса сайта банка

1. Откройте сайт Центрального банка Российской Федерации.
2. Перейдите в раздел «Информация по кредитным организациям» - «Справочник по кредитным организациям» (http://www.cbr.ru/credit/main/cowebsites/).
3. В открывшейся форме укажите название банка или адрес его сайта в сети Интернет.



4. Нажмите кнопку найти.
5. Выберите из открывшегося списка ссылку для безопасного перехода на сайт учреждения.

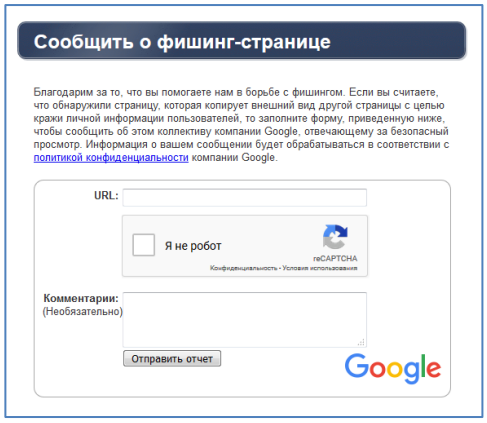


| № п.п. | Рег. номер | Наименование кредитной организации | Адрес Web сайта |
|---|---|---|---|
| 1 | 1481 | ПАО Сбербанк | http://beta.sberbank.ru<br>http://sberbank.com<br>http://sberbank1.ru<br>http://sbrf.ru<br>http://www.sberbank.com<br>http://www.sberbank.ru<br>http://www.sberbank1.ru<br>http://www.сбербанк.рф<br>http://сбербанк.рф |

**Внимание!**
**При переходе на сайт с целью публикации конфиденциальной информации проверяйте адрес страницы: если он отличается хотя бы на один символ (например, paypa1.com вместо paypal.com), вполне вероятно, что это фишинговый сайт. Будьте бдительны!**

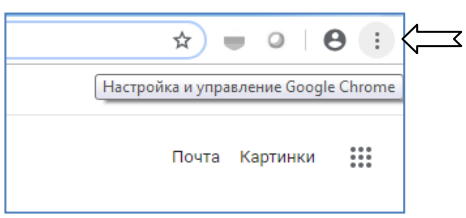
## ЗАДАНИЕ 6.2 Сообщить о фишинг-странице

1. Откройте специальную страницу сервиса Google, предназначенную для направления информации о фишинговых сайтах (www.google.com/safebrowsing/report_phish/)
2. Укажите адрес Интернет-сайта, который по Вашему мнению незаконно собирает информацию.
3. Поставьте галочку **Я не робот** и при необходимости добавьте комментарии к своей заявке.
4. Нажмите **Отправить отчет**.



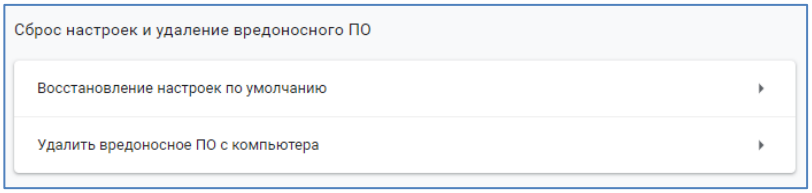

## ЗАДАНИЕ 6.3 Настройки конфиденциальности в Интернет-браузере

1. Откройте Интернет-браузер Chrome.
2. Нажмите на значок с тремя точками в правом верхнем углу экрана



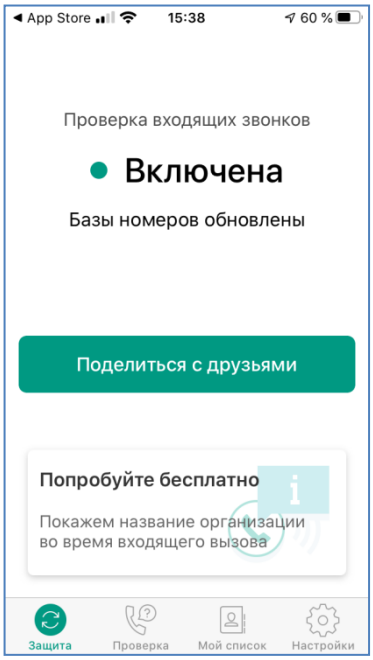
3. Откройте «Настройки» - «Дополнительные».
4. Перейдите в раздел "Конфиденциальность и безопасность".
5. Перейдите на вкладку «Синхронизация сервисов Google».
6. Проверьте, чтобы была включена опция «Безопасный просмотр».

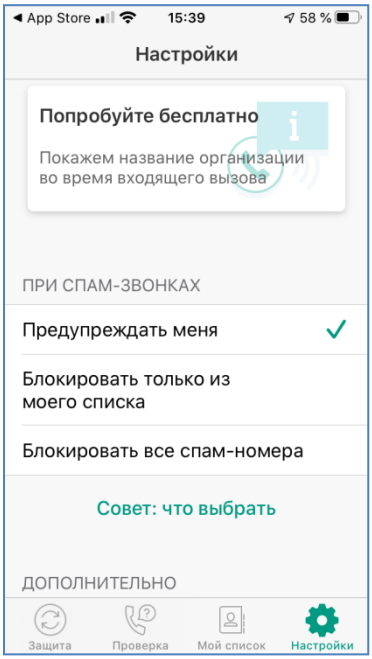

7. Выберите «Очистить историю», чтобы удалить сведения о посещенных сайтах или сохраненные пароли.
8. При необходимости можете воспользоваться опцией «Удалить вредоносное ПО с компьютера»



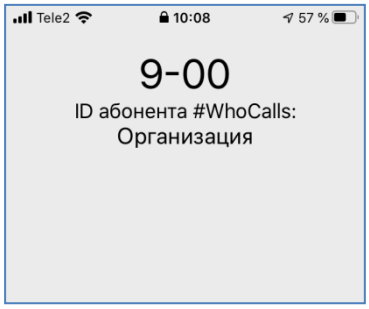

## ЗАДАНИЕ 6.4 Мобильное приложение для блокирования подозрительных телефонных вызовов

1. Откройте на своем мобильном устройстве магазин приложений (AppStore или Google Play).
2. В поисковой строке напечатайте «who calls».
3. Выберите приложение «Определитель номера, антиспам: Kaspersky Who Calls».
4. После загрузки откройте приложение.
5. Обновите базы и выберите соответствующие настройки, которые будут вам удобны при использовании смартфона.








6. Теперь при всех подозрительных звонках вы будете получать соответствующее предупреждение.

## ДЛЯ ЗАМЕТОК