**Центральная городская библиотека**

353290 г. Горячий Ключ,

ул. Ленина, 203/1

E- mail: [**bibla@bk.ru**](mailto:bibla@bk.ru)

Сайт: **librarygk.ru**

Часы работы

10.00-18.00

Без перерыва

Выходной – понедельник

Последний день месяца – санитарный

**МБУК «ЦБС»**

**Центральная городская библиотека**

**Отдел методической работы**

**Безопасность**

**в сети интернет.**

*Буклет*

Горячий Ключ

2017 год

Безопасность в интернете – очень важная проблема нынешнего времени. Она становится все актуальнее в связи с массовым приходом в интернет не подготовленных к поджидающим их угрозам пользователей.

**Опасности в сети**

Можно привести две потенциальные возможности попадания вируса на ваш компьютер.

Первый вариант – по вине пользователя. Очень часто странствуя по различным сайтам или устанавливая программное обеспечение с непроверенных источников, а иногда и с проверенных, вы сами заражаете свой компьютер.

Второй вариант – активность троянских программ и вирусов. При помощи данных инструментов злоумышленники преднамеренно, делают ваше устройство источником опасности.

В результате компьютер начинает выполнять рассылку спама, участвует в DDoS-атаках на различные сайты, крадет пароли. В некоторых случаях провайдер вынужден принудительно отключить зараженное устройство от [глобальной сети.](http://fb.ru/article/44664/globalnyie-seti)

## http://static.commentcamarche.net/www.commentcamarche.net/pictures/0tu7iEqp-mot-de-passe-s-.pngЗачем злоумышленникам доступ к компьютеру пользователя

Многие пользователя считают, что их компьютер никому не нужен. Лет 20 тому назад злоумышленник получал удовольствие от того, что мог просто отформатировать жесткий диск. Сейчас же они делают все возможное, чтобы владелец компьютера как можно дольше не знал о том, что его устройство заражено и втайне от него выполняет дополнительные функции.

Для чего все это делается? Кроме того, о чем было сказано выше, хакеры стараются получить доступ к вашим электронным почтам, кошелькам, аккаунтам в социальных сетях, форумах. Случается так, например, что вы ложитесь спать с 20 000 рублей на электронном кошельке, а утром получаете СМС-сообщение о том, что денег на нем уже нет. А с почты все ваши контакты, да и не только, получают спам-письма, а то еще и трояны. Хакеры могут провести DDoS-атаку даже на мощные государственные серверы. Из самого простого, но также приносящего деньги: заблокируют работу операционной системы и потребуют деньги за устранение проблемы. Так что безопасность в сети интернет должна стать основой вашей работы в ней.

## Как злоумышленники проникают в компьютер?

Для того чтобы взломать защиту ПК, даже если она есть, хакеры применяют целый ряд способов, и пользователи зря думают, что, просто установив антивирус, они избавились от опасности, например, подцепить вредоносную программу. Поэтому, прежде чем искать информацию о том, как правильно соблюдать безопасность в сети интернет, нужно понять, а откуда берутся вирусы.

**Основные пути получения доступа злоумышленниками к компьютеру и методы воровства различной информации.**

1. Первый метод – благодаря различным психологическим приемам, уловкам и доверчивости пользователей хакеры присылают вам вполне безобидный файл или письмо, а вы сами и запускаете вирусы в нем. Или же по просьбе якобы администрации сервиса выдаете все свои пароли и явки.
2. Второй метод – предлагается разное бесплатное программное обеспечение, пиратские диски, где спрятано множество вирусов.
3. Третий метод – в программном обеспечении постоянно появляются дыры в безопасности. Это относится и к операционным системам. Вот злоумышленники внимательно и следят за такими моментами, стараются их не упустить, а использовать в собственных целях.
4. Четвертый метод получил особое распространение в последнее время. Это *фишинг*, когда создаются поддельные сайты. И вы вместо странички своего банка оказываетесь на его поддельной копии.

## Защита компьютера пользователя

В идеале, купив компьютер, пользователь должен выполнить целый ряд операций, прежде чем броситься бороздить бесконечные просторы сети. Сейчас мы представим некоторые самые первые уроки безопасности в интернете.

1. Несмотря на то что Windows имеет встроенный файрволл, рекомендуется установить более надежный, так как имеющийся - далеко не самый лучший. Выбирайте платный или бесплатный, исходя из их рейтингов.
2. Следующий шаг – установка антишпионского и антивирусного программного обеспечения. Нужно сразу же его обновить и настроить на автоматическое обновление. Также оно должно запускаться автоматически, вместе с операционной системой. И постоянно работать. И обязательно проверяйте любую устанавливаемую программу.
3. Как только появляются обновления для используемых вами браузеров, тут же скачивайте их и устанавливаете.
4. Отключайте все неиспользуемые службы на своем устройстве, это уменьшит шансы для хакеров получить к нему доступ.

## Уроки безопасности

Выполнив указанное в предыдущем разделе, пне забывайте о ежедневной защите.

1. Удаляйте сразу же все письма подозрительного содержания, не вздумайте открывать файлы из неизвестных источников. Игнорируйте все предложения легкого заработка, никому не высылайте свои пароли, не переходите по подозрительным ссылкам.
2. Используйте только сложные пароли, состоящие из сложного набора цифр, букв и символов.
3. Выходя в сеть из мест общего пользования, будьте аккуратны и осторожны. Это же касается и использования прокси-серверов. Желательно не проводить никаких банковских и других подобных операций из таких мест.
4. Предпочитайте работать с платежными системами через их собственные приложения, а не через сайт. Это намного безопаснее.
5. Следите за интернет-траффиком, даже если он безлимитный. Если он без особой причины значительно увеличился, это может быть признаком активности вируса. Если будете соблюдать эти минимальны правила безопасности в сети интернет, то избежите многих проблем.

**Безопасности в интернете**

Если с вашего банка пришло письмо с проверкой пароля, не вздумайте им его отправлять. Банки никогда таких запросов не делают. Все [почтовые программы](http://fb.ru/article/64084/kakie-byivayut-pochtovyie-programmyi) имеют фильтр от спама. Доверяйте ему. Получив письмо о выигрыше в миллион рублей или наследстве в пять миллионов долларов, удаляйте их сразу же. Рекомендуем устанавливать комплексную защиту. Она надежнее, чем антивирус – от одного производителя, файрволл – от другого, а антишпионская программа – от третьего.

Отдавайте предпочтение платным версиям. Так как Opera и Internet Explorer – самые распространенные браузеры, для них и вирусов существует более всего. Например используйте альтернативные варианты: Google Chrome, Mozilla Firefox. Не пользуйтесь нелицензионным программным обеспечением, так как в нем изначально может быть установлено шпионское ПО. Если делайте покупки в онлайн-магазинах, то пользуйтесь только проверенными вариантами. Это же относится и к любому иному онлайн-сервису. Выполняйте все эти требования, и тогда безопасность в сети интернет будет более-менее гарантирована.