**Статья**

**по теме**

**«Компьютерная безопасность»**

**Учитель информатики Троицкой Л.П.**

**Москва 2023 г.**

1. **Введение**

Развитие информационных технологий и вычислительной техники существенно изменило окружающий нас мир в последние десятилетия до неузнаваемости. Мы выполняем электронные платежи, расплачиваемся банковскими картами и смартфонами, на которых установлены специальные программы, обмениваемся мгновенными сообщениями посредством многочисленных интернет-сервисов, управляем с помощью мобильных телефонов, подключенных к сети интернет, различными инфраструктурными компонентами (начиная от удаленного включения обогревательных элементов в загородных домах, и, заканчивая управлениям параметрами термоядерных реакций на атомных станциях) и т.д. Перечислять можно бесконечно долго, поскольку информационные технологии проникли едва ли не вовсе аспекты нашей жизни. Безусловно, главный двигатель развития информационных технологий и компьютерной техники – это повышения уровня комфорта людей, обеспечение максимального удобства и простоты при выполнении как рутинных бытовых манипуляций, так и сложных, требующих повышенной внимательности и точности операций (например, при работе со сложными инфраструктурными или производственными объектами). Обратной стороной достижения указанных целей является повышение уязвимости объектов, представляющих определенную ценность для сторон информационного взаимодействия (информация личного характера, данные о банковских счетах, денежные средства, параметры удаленного доступа к охраняемым объектам и т.д.). Действительно, давайте сравним уровень угрозы потери денежных средств человеком, приходящим в отделение банка и выполняющего операцию, например, перевода определенной суммы со своего банковского счета, с помощью сотрудника банка, и человеком, выполняющего ту же операцию, используя сервис онлайн-банкинга. В первом случае, если не брать в расчет форс-мажорные обстоятельства (стихийные бедствия, вооруженное нападение и т.п.), риски можно оценить как низкие, в то время, как во втором случае риски заметно повышаются, учитывая все возрастающую активность киберпреступников. Для подтверждения высокого уровня опасности достаточно привести следующую статистику по данным, представленным в [1].



**Рис. 1 Топ-10 стран по доли компьютеров, зараженных различными вирусами**

Для полноты картины добавим лишь, что лидирует в списке стран по доле зараженных компьютеров Швеция с долей 19,8%. Таким образом, даже в наиболее благополучных в этом смысле странах заражен практически каждый пятый компьютер, а в России – каждый третий. Другими словами, даже если не брать в расчет другие способы кибермошенничества риск во втором случае рассмотренного примера превышает 1/3.

В данной работе будут рассмотрены основные виды и способы компьютерной преступности, а также предложен набор базовых правил по минимизации рисков стать жертвой киберпреступников при использовании современных информационных технологий. При этом основное внимание будет уделено опасностям, угрожающим конкретному пользователю (что называется, обычному человеку), поскольку решение проблем компьютерной безопасности на уровне банка, объекта промышленности, организации, города, страны решаются централизованно специально для этого предназначенными службами, в то время как компьютерная безопасность на стороне конечного пользователя целиком и полностью лежит на нем самом (спасение утопающего – дело самого утопающего).[[1]](#footnote-1)

1. **Классификация угроз компьютерной безопасности**

Прежде, чем говорить о разновидностях угроз и о мерах противодействия им, рассмотрим определение понятия «компьютерная безопасность» (далее - КБ). Существуют два определения (см., например, [2]).

1. Компьютерная безопасность — раздел безопасности, характеризующий невозможность возникновения ущерба компьютера, превышающего величину приемлемого ущерба для него от всех выявленных и изученных источников его отказов в определенных условиях работы и на заданном интервале времени.
2. Компьютерная безопасность — меры безопасности, применяемые для защиты вычислительных устройств (компьютеры, смартфоны и другие), а также компьютерных сетей (частных и публичных сетей, включая Интернет).

Как видно из приведенных определений, с одной стороны, КБ – один из разделов «безопасности вообще», а с другой – комплекс мер, направленный на минимизацию рисков безопасности вычислительных устройств, компьютерных сетей и, если брать более широкую трактовку, информации, передаваемой с их помощью. С точки зрения данной работы, мы будем иметь ввиду вторую трактовку.

Соответственно, классификация угроз компьютерной безопасности может проведена по различным параметрам. Во-первых, с точки зрения источника следует выделить такие угрозы:

1. обусловленные человеческим фактором;
2. технические;
3. стихийные.

Первый тип угроз обусловлен действием человека, нарушающего предполагаемый алгоритм функционирования системы. В случае действия злоумышленника человеческий фактор является внешним, если угроза безопасности возникает от действий пользователя – внутренним. Технические угрозы – это, прежде всего, сбои оборудования, приводящие к возникновению уязвимости. Стихийные угрозы возникают в результате действия различных негативных природных факторов.

Также угрозы компьютерной безопасности можно классифицировать в зависимости от источника распространения. Очевидно, возможно несколько источников распространения – внешняя сетевая среда (Интернет), внутренняя сеть (домашняя или корпоративная), электронная почта и внешние носители информации (флеш-память, CD-диски, съёмные жесткие диски и др.).

В соответствии с классификацией Лабаратории Касперского [3] можно выделить следующие виды угроз.

1. **Вирусы -** программы, которые заражают другие программы (добавляют в них свой код, чтобы получить управление при запуске зараженных файлов). Основное действие, выполняемое вирусом – заражение. Скорость распространения вирусов несколько ниже, чем у червей.

В соответствии с классификацией, приведенной на сайте компании «Доктор Веб» [4] различают следующие типы компьютерных вирусов:

**‑ файловые вирусы**, которые инфицируют файлы операционной системы и активизируются при обращении к зараженному файлу;

**‑ макро-вирусы**, которые инфицируют документы, использующие программы Microsoft Office (и другие программы, которые используют макросы, написанные, например, на языке Visual Basic). Макросы – это встроенные программы, написанные на полноценном языке программирования, которые могут запускаться при определенных условиях (например, при открытии, закрытии или сохранении документа);

‑ **скрипт-вирусы**, которые пишутся на языках сценариев (скриптов) и в большинстве случаев заражают другие файлы сценариев (например, служебные файлы операционной системы). Они могут инфицировать также другие типы файлов, которые поддерживают исполнение сценариев, пользуясь уязвимыми сценариями в веб-приложениях;

‑ **загрузочные вирусы**, которые заражают загрузочные сектора дисков и разделов, а также главные загрузочные сектора жестких дисков. Они занимают очень мало памяти и остаются готовыми к выполнению своих функций до тех пор, пока не будет произведена выгрузка, перезагрузка или завершение работы системы.

Большинство вирусов обладает определенными защитными механизмами против обнаружения. Методы защиты от обнаружения постоянно улучшаются, поэтому для антивирусных программ разрабатываются новые способы преодоления этой защиты.

**2) Черви.** Данная категория вредоносных программ для распространения использует сетевые ресурсы. Название этого класса было дано исходя из способности червей «переползать» с компьютера на компьютер, используя сети, электронную почту и другие информационные каналы. Также благодаря этому черви обладают исключительно высокой скоростью распространения. Черви проникают на компьютер, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Помимо сетевых адресов часто используются данные адресной книги почтовых клиентов. Представители этого класса вредоносных программ иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

**3) Троянские программы -** программы, которые выполняют на поражаемых компьютерах несанкционированные пользователем действия, т.е. в зависимости от каких-либо условий уничтожают информацию на дисках, приводят систему к «зависанию», воруют конфиденциальную информацию и т.д. Данный класс вредоносных программ не является вирусом в традиционном понимании этого термина (т.е. не заражает другие программы или данные); троянские программы не способны самостоятельно проникать на компьютеры и распространяются злоумышленниками под видом «полезного» программного обеспечения. При этом вред, наносимый ими, может во много раз превышать потери от традиционной вирусной атаки.

**4) Программы-шпионы -** программное обеспечение, позволяющее собирать сведения об отдельно взятом пользователе или организации без их ведома. О наличии программ-шпионов на своем компьютере вы можете и не догадываться. Как правило, целью программ-шпионов является:

* отслеживание действий пользователя на компьютере;
* сбор информации о содержании жесткого диска (например, для составления списка программного обеспечения, установленного на компьютере);
* сбор информации о качестве связи, способе подключения, скорости модема и т.д.

Однако данные программы не ограничиваются только сбором информации, они представляют реальную угрозу безопасности. Как минимум две из известных программ – Gator и eZula – позволяют злоумышленнику не просто собирать информацию, но и контролировать чужой компьютер. Другим примером программ-шпионов являются программы, встраивающиеся в установленный на компьютере браузер и перенаправляющие трафик. Многие пользователи встречались с подобными программами, если при запросе одного адреса веб-сайта открывался совсем другой.

Одной из разновидностей программ-шпионов являются фишинг-рассылки.

**Фишинг** – почтовая рассылка, целью которой является получение от пользователя конфиденциальной информации. Такие письма составляются таким образом, чтобы максимально походить на информационные письма от банковских структур, компаний известных брендов. Письма содержат ссылку на заведомо ложный сайт, где пользователю предлагается ввести, например, номер своей кредитной карты и другую конфиденциальную информацию.

**5) Программы-рекламы** - программный код, без ведома пользователя включенный в программное обеспечение с целью демонстрации рекламных объявлений. Как правило, программы-рекламы встроены в программное обеспечение, распространяющееся бесплатно. Реклама располагается в рабочем интерфейсе. Зачастую данные программы также собирают и переправляют своему разработчику персональную информацию о пользователе.

**6) Потенциально опасные приложения -** программное обеспечение, не являющееся вирусом, но содержащее в себе потенциальную угрозу. При некоторых условиях наличие таких программ на компьютере подвергает ваши данные риску. К таким программам относятся, например, утилиты удаленного администрирования.

**7) Программы-шутки -** программное обеспечение, не причиняющее компьютеру какого-либо прямого вреда, но выводящее сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях. Такие программы часто предупреждают пользователя о несуществующей опасности, например, выводят сообщения о форматировании диска (хотя никакого форматирования на самом деле не происходит), обнаруживают вирусы в незараженных файлах и т.д.

**8) Программы-маскировщики -** это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами. Маскировщики также могут модифицировать операционную систему на компьютере и заменять основные ее функции, чтобы скрыть свое собственное присутствие и действия, которые предпринимает злоумышленник на зараженном компьютере.

**9) Прочие опасные программы -** разнообразные программы, которые разработаны для создания других вредоносных программ, организации DoS (Distributed Denial of Service)-атак на удаленные сервера, взлома других компьютеров и т. п. К таким программам относятся хакерские утилиты (Hack Tools), конструкторы вирусов и т.д.

**10) Спам -** анонимная, массовая почтовая корреспонденция нежелательного характера. Так, спамом являются рассылки политического и агитационного характера, письма, призывающие помочь кому-нибудь. Отдельную категорию спама составляют письма с предложениями обналичить большую сумму денег или вовлекающие в финансовые пирамиды, а также письма, направленные на кражу паролей и номеров кредитных карт, письма с просьбой переслать знакомым (например, письма счастья) и т. п. Спам существенно повышает нагрузку на почтовые сервера и повышает риск потери информации, важной для пользователя.

Основные источники киберугроз пользователям согласно данным «Лаборатории Касперского» [5] следующие.

1. интернет;
2. электронная почта;
3. уязвимости в программном обеспечении;
4. внешние носители информации;
5. пользователи.

Рассмотрим далее основные способы защиты от утечек по данным каналам.

**3. Правила минимизации угроз компьютерной безопасности**

Для того, чтобы сформулировать базовые правила, которым должен следовать конкретный пользователь во избежание потерь персональных данных, критически важной информации и т.д. при работе с персональными компьютерами и современными гаджетами, попробуем проанализировать представленную выше информацию.

Начнем с защиты от киберугроз, поступающих из Интернета. Основным элементом любого электронного устройства, используемого для работы в сети Интернет, является операционная система (ОС). Уязвимости в операционной системе – одна из основных причин заражения персональных компьютеров и мобильных устройств. Так какая же ОС является самой надежной? Универсального ответа, по-видимому, нет. Однако, если суммировать все уязвимости (критичные и нет), то можно получить достаточно общий ответ на поставленный вопрос. По результатам исследований компании CVE Details [6] наибольшим количеством уязвимостей обладают операционные системы семейства Android, далее следуют операционные системы компании Apple (Mac OS) и ряд коммерческих версий ОС семейства Linux. Замыкают список продукты компании Microsoft и ряд сборок Linux. Полные данные представлены в таблице 1.

**Таблица 1. Количество уязвимостей, обнаруженных в операционных системах в 2016 году**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | № | **Операционная система** | **Разработчик** | **Количество уязвимостей** | | 1 | [Android](https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224) | [Google](https://www.cvedetails.com/vendor/1224/Google.html) | [523](https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/year-2016/Google-Android.html) | | 2 | [Debian Linux](https://www.cvedetails.com/product/36/Debian-Debian-Linux.html?vendor_id=23) | [Debian](https://www.cvedetails.com/vendor/23/Debian.html) | [327](https://www.cvedetails.com/vulnerability-list/vendor_id-23/product_id-36/year-2016/Debian-Debian-Linux.html) | | 3 | [Ubuntu Linux](https://www.cvedetails.com/product/20550/Canonical-Ubuntu-Linux.html?vendor_id=4781) | [Canonical](https://www.cvedetails.com/vendor/4781/Canonical.html) | [279](https://www.cvedetails.com/vulnerability-list/vendor_id-4781/product_id-20550/year-2016/Canonical-Ubuntu-Linux.html) | | 4 | [Leap](https://www.cvedetails.com/product/32606/Novell-Leap.html?vendor_id=20) | [Novell](https://www.cvedetails.com/vendor/20/Novell.html) | [260](https://www.cvedetails.com/vulnerability-list/vendor_id-20/product_id-32606/year-2016/Novell-Leap.html) | | 5 | [Opensuse](https://www.cvedetails.com/product/12345/Novell-Opensuse.html?vendor_id=20) | [Novell](https://www.cvedetails.com/vendor/20/Novell.html) | [228](https://www.cvedetails.com/vulnerability-list/vendor_id-20/product_id-12345/year-2016/Novell-Opensuse.html) | | 6 | [Linux Kernel](https://www.cvedetails.com/product/47/Linux-Linux-Kernel.html?vendor_id=33) | [Linux](https://www.cvedetails.com/vendor/33/Linux.html) | [217](https://www.cvedetails.com/vulnerability-list/vendor_id-33/product_id-47/year-2016/Linux-Linux-Kernel.html) | | 7 | [Mac Os X](https://www.cvedetails.com/product/156/Apple-Mac-Os-X.html?vendor_id=49) | [Apple](https://www.cvedetails.com/vendor/49/Apple.html) | [215](https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-156/year-2016/Apple-Mac-Os-X.html) | | 8 | [Windows 10](https://www.cvedetails.com/product/32238/Microsoft-Windows-10.html?vendor_id=26) | [Microsoft](https://www.cvedetails.com/vendor/26/Microsoft.html) | [172](https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-32238/year-2016/Microsoft-Windows-10.html) | | 9 | [Iphone Os](https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49) | [Apple](https://www.cvedetails.com/vendor/49/Apple.html) | [161](https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-15556/year-2016/Apple-Iphone-Os.html) | | 10 | [Windows Server 2012](https://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26) | [Microsoft](https://www.cvedetails.com/vendor/26/Microsoft.html) | [156](https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-23546/year-2016/Microsoft-Windows-Server-2012.html) | | 11 | [Windows 8.1](https://www.cvedetails.com/product/26434/Microsoft-Windows-8.1.html?vendor_id=26) | [Microsoft](https://www.cvedetails.com/vendor/26/Microsoft.html) | [154](https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-26434/year-2016/Microsoft-Windows-8.1.html) | | 12 | [Windows Rt 8.1](https://www.cvedetails.com/product/26435/Microsoft-Windows-Rt-8.1.html?vendor_id=26) | [Microsoft](https://www.cvedetails.com/vendor/26/Microsoft.html) | [139](https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-26435/year-2016/Microsoft-Windows-Rt-8.1.html) | | 13 | [Windows 7](https://www.cvedetails.com/product/17153/Microsoft-Windows-7.html?vendor_id=26) | [Microsoft](https://www.cvedetails.com/vendor/26/Microsoft.html) | [134](https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-17153/year-2016/Microsoft-Windows-7.html) | | 14 | [Windows Server 2008](https://www.cvedetails.com/product/11366/Microsoft-Windows-Server-2008.html?vendor_id=26) | [Microsoft](https://www.cvedetails.com/vendor/26/Microsoft.html) | [133](https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-11366/year-2016/Microsoft-Windows-Server-2008.html) | | 15 | [Enterprise Linux Workstation](https://www.cvedetails.com/product/24640/Redhat-Enterprise-Linux-Workstation.html?vendor_id=25) | [Redhat](https://www.cvedetails.com/vendor/25/Redhat.html) | [126](https://www.cvedetails.com/vulnerability-list/vendor_id-25/product_id-24640/year-2016/Redhat-Enterprise-Linux-Workstation.html) | | 16 | [Enterprise Linux Server](https://www.cvedetails.com/product/24639/Redhat-Enterprise-Linux-Server.html?vendor_id=25) | [Redhat](https://www.cvedetails.com/vendor/25/Redhat.html) | [126](https://www.cvedetails.com/vulnerability-list/vendor_id-25/product_id-24639/year-2016/Redhat-Enterprise-Linux-Server.html) | | 17 | [Enterprise Linux Desktop](https://www.cvedetails.com/product/79/Redhat-Enterprise-Linux-Desktop.html?vendor_id=25) | [Redhat](https://www.cvedetails.com/vendor/25/Redhat.html) | [126](https://www.cvedetails.com/vulnerability-list/vendor_id-25/product_id-79/year-2016/Redhat-Enterprise-Linux-Desktop.html) | | 18 | [Windows Vista](https://www.cvedetails.com/product/9591/Microsoft-Windows-Vista.html?vendor_id=26) | [Microsoft](https://www.cvedetails.com/vendor/26/Microsoft.html) | [125](https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-9591/year-2016/Microsoft-Windows-Vista.html) | | 19 | [Fedora](https://www.cvedetails.com/product/16334/Fedoraproject-Fedora.html?vendor_id=6924) | [Fedoraproject](https://www.cvedetails.com/vendor/6924/Fedoraproject.html) | [120](https://www.cvedetails.com/vulnerability-list/vendor_id-6924/product_id-16334/year-2016/Fedoraproject-Fedora.html) | | 20 | [Linux](https://www.cvedetails.com/product/21375/Oracle-Linux.html?vendor_id=93) | [Oracle](https://www.cvedetails.com/vendor/93/Oracle.html) | [118](https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-21375/year-2016/Oracle-Linux.html) | | 21 | [Apple Tv](https://www.cvedetails.com/product/32705/Apple-Apple-Tv.html?vendor_id=49) | [Apple](https://www.cvedetails.com/vendor/49/Apple.html) | [102](https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-32705/year-2016/Apple-Apple-Tv.html) | | 22 | [Watchos](https://www.cvedetails.com/product/32536/Apple-Watchos.html?vendor_id=49) | [Apple](https://www.cvedetails.com/vendor/49/Apple.html) | [77](https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-32536/year-2016/Apple-Watchos.html) | | 23 | [Solaris](https://www.cvedetails.com/product/19755/Oracle-Solaris.html?vendor_id=93) | [Oracle](https://www.cvedetails.com/vendor/93/Oracle.html) | [76](https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-19755/year-2016/Oracle-Solaris.html) | | 24 | [Enterprise Linux](https://www.cvedetails.com/product/78/Redhat-Enterprise-Linux.html?vendor_id=25) | [Redhat](https://www.cvedetails.com/vendor/25/Redhat.html) | [63](https://www.cvedetails.com/vulnerability-list/vendor_id-25/product_id-78/year-2016/Redhat-Enterprise-Linux.html) | | 25 | [Linux Enterprise](https://www.cvedetails.com/product/34242/Suse-Linux-Enterprise.html?vendor_id=61) | [Suse](https://www.cvedetails.com/vendor/61/Suse.html) | [62](https://www.cvedetails.com/vulnerability-list/vendor_id-61/product_id-34242/year-2016/Suse-Linux-Enterprise.html) | | 26 | [Enterprise Linux Hpc Node](https://www.cvedetails.com/product/25164/Redhat-Enterprise-Linux-Hpc-Node.html?vendor_id=25) | [Redhat](https://www.cvedetails.com/vendor/25/Redhat.html) | [54](https://www.cvedetails.com/vulnerability-list/vendor_id-25/product_id-25164/year-2016/Redhat-Enterprise-Linux-Hpc-Node.html) | | 27 | [Enterprise Linux Server Eus](https://www.cvedetails.com/product/25167/Redhat-Enterprise-Linux-Server-Eus.html?vendor_id=25) | [Redhat](https://www.cvedetails.com/vendor/25/Redhat.html) | [53](https://www.cvedetails.com/vulnerability-list/vendor_id-25/product_id-25167/year-2016/Redhat-Enterprise-Linux-Server-Eus.html) | | 28 | [Enterprise Linux Hpc Node Eus](https://www.cvedetails.com/product/33598/Redhat-Enterprise-Linux-Hpc-Node-Eus.html?vendor_id=25) | [Redhat](https://www.cvedetails.com/vendor/25/Redhat.html) | [49](https://www.cvedetails.com/vulnerability-list/vendor_id-25/product_id-33598/year-2016/Redhat-Enterprise-Linux-Hpc-Node-Eus.html) | |  |

Данные, представленные в таблице 2, показывают, что имеющееся в обществе предубеждение против ОС семейства Windows в плане их защищенности от кибератак является неоправданным.

Второй источник проникновения нежелательного программного обеспечения (ПО) на компьютеры и мобильные устройства конечных пользователей – интернет-браузеры. Для оценки их защищенности приведем опять данные, представленные в [6].

**Таблица 2. Количество уязвимостей, обнаруженных в браузерах в 2016 году**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | № | **Браузер** | **Разработчик** | **Количество уязвимостей** | | 14 | [Chrome](https://www.cvedetails.com/product/15031/Google-Chrome.html?vendor_id=1224) | [Google](https://www.cvedetails.com/vendor/1224/Google.html) | [172](https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-15031/year-2016/Google-Chrome.html) | | 19 | [Edge](https://www.cvedetails.com/product/32367/Microsoft-Edge.html?vendor_id=26) | [Microsoft](https://www.cvedetails.com/vendor/26/Microsoft.html) | [135](https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-32367/year-2016/Microsoft-Edge.html) | | 22 | [Firefox](https://www.cvedetails.com/product/3264/Mozilla-Firefox.html?vendor_id=452) | [Mozilla](https://www.cvedetails.com/vendor/452/Mozilla.html) | [133](https://www.cvedetails.com/vulnerability-list/vendor_id-452/product_id-3264/year-2016/Mozilla-Firefox.html) | | 23 | [Internet Explorer](https://www.cvedetails.com/product/9900/Microsoft-Internet-Explorer.html?vendor_id=26) | [Microsoft](https://www.cvedetails.com/vendor/26/Microsoft.html) | [129](https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-9900/year-2016/Microsoft-Internet-Explorer.html) | | 44 | [Safari](https://www.cvedetails.com/product/2935/Apple-Safari.html?vendor_id=49) | [Apple](https://www.cvedetails.com/vendor/49/Apple.html) | [56](https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-2935/year-2016/Apple-Safari.html) | |  |

Данные, представленные в таблице 2, говорят о том, что наиболее популярный интернет-браузер Chrome обладает наибольшим количеством уязвимостей, в то время как браузер от Apple является существенно более надежным по сравнению со всеми остальными.

Для оценки уровня надежности компьютеров от компьютерных атак, эксплуатирующих уязвимости в браузерах, я провел опрос среди знакомых. 32 людям в возрасте от 15 до 18 лет был задан вопрос: каким браузером вы пользуетесь на своем домашнем компьютере/ноутбуке. Результаты опроса представлены на рисунке 2.

**Рис. 2 Результаты социологического опроса об используемых браузерах**

Таким образом, почти половина опрошенных использует наиболее уязвимый браузер.

Для минимизации риска угроз, поступающих через сеть Интернет, можно сформулировать следующие правила.

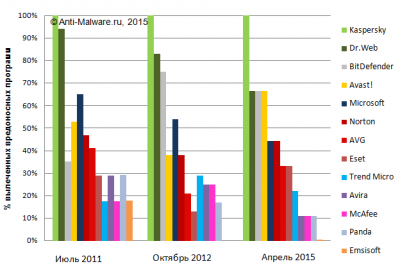
1) Необходимо использовать лицензионную ОС (желательно, актуальной версии) с установленными сервиспаками. Приведенные выше данные свидетельствуют о том, что приемлемым вариантом является использование ОС Windows 7 и новее.[[2]](#footnote-2)

2) При необходимости выхода в Интернет пользователю необходимо заходить в систему под учетной записью с ограниченными правами, а при необходимости настройки системы, требующей права администратора, следует отключить соединение с глобальной сетью.

3) Действенным способом, существенно осложняющим доступ злоумышленников к критически важным компонентам ОС, является использование так называемых «виртуальных машин». Выход в Интернет из-под виртуальной машины в большинстве случаев предоставляет злоумышленникам доступ только к ней, а не к ОС хост-машины.

4) Исходя из данных, представленных в таблице 2, и отзывов пользователей, целесообразно использовать интернет-браузер Firefoх.

5) Безусловно, необходимо использование лицензионных версий антивирусных средств. В соответствии с тестированием, регулярно проводимым специалистами Интернет-ресурса Anti-Malware.ru [7], с серьезным перевесом по результативности борьбы с вирусами побеждают решения «Лаборатории Касперского».



**Рис. 3 Результаты тестирования известных антивирусов**

При этом отметим, что использование комплексных решений по компьютерной безопасности, которые имеются практически у всех крупных производителей и включают в себя, как правило, антивирус, антиспам, родительский контроль, защита от потери данных, файрволл и др. Кроме того, несмотря на кажущуюся очевидность данного требования, все-таки сформулируем его здесь: необходимо своевременно обновлять антивирусные базы вне зависимости от того, какое антивирусное средство используется.

Как было показано выше, следующим источником угроз является электронная почта. Для минимизации ущерба от этого источника сформулируем еще два правила.

6) Использование надежного пароля для входа в свою учетную запись и, по возможности, настройка на многофакторную аутентификацию (например, дополнительно с помощью одноразовых паролей, передаваемых посредством СМС-сообщений). Ниже мы остановимся более подробно на особенностях выбора и использования паролей.

7) Предотвращение возможных спам, фишинг и т.п. типов атак, предполагающих отправку пользователю под благовидным предлогом (в нашем случае, например, с помощью письма из незнакомого источника) с просьбой перейти на определенный сайт или запуска приложения к письму. Рекомендация здесь вполне понятна – не открывать сообщений от неизвестных абонентов.

Для источника угроз компьютерной безопасности – уязвимости в ПО - также можно сформулировать определенные правила.

8) Проверять соответствие адреса в адресной строке браузера и адреса целевого ресурса (во избежание переадресации на сайт-клон, контролируемый злоумышленниками).

9) Поскольку создатели распространенного ПО (текстовые редакторы, проигрыватели мультимедиа, браузеры, ОС и прочее) регулярно выпускают обновления, устраняя уязвимости предыдущих версий, то установка таких обновлений является обязательной для обеспечения кибербезопасности.

Многие упомянутые выше правила так или иначе направлены на снижение риска заражения компьютера, возникающего в связи с неправильными действиями пользователя, сформулируем это правило отдельно.

10) Не загружать ПО из недостоверных источников (как правило, сайты, предлагающие различные ключи и кейгены для платного ПО, буквально насквозь поражены различными зловредами, также опасность представляет скачивание «бесплатных» электронных книг, фильмов и т.п.), не оставлять в открытом доступе информацию о параметрах аутентификации на сетевых и локальных ресурсах.

Как было обещано выше, остановимся подробнее на вопросах выбора и использования паролей. Здесь также сформулируем ряд базовых правил.

а) Крайне нежелательно использование одного и того же пароля для доступа к разным ресурсам.

б) Пароль для доступа к различным ресурсам должен быть сложным. Желательно, чтобы он был длиной от 10 символов и выше и содержал в себе символы из разных групп. В идеале, пароль должен быть случайным, чтобы затруднить потенциальным злоумышленникам возможность его подбора из списка наиболее популярных паролей (например, по данным, приведенным в [8], наиболее употребимыми паролями являются «12345», «password», «default»).

в) Для упрощения процесса выполнения первых двух требований удобно воспользоваться так называемыми менеджерами паролей (см., например, программное средство KeePass [9]), которые обеспечат надежное хранение в зашифрованном виде паролей пользователя на компьютере. Выгода от использования указанных менеджеров состоит в том, что пользователю требуется запомнить всего один сложный пароль (для доступа к хранилищу паролей в менеджере), ввод которого позволит достать остальные пароли к другим целевым системам.

Рассмотрим далее способы противостояния угрозам, возникающим в результате использования съёмных носителей информации. Под этим термином имеется в виду, прежде всего, флеш-накопители, которые довольно легко заражаются при подключении к ранее зараженному компьютеру. Впоследствии диапазон манипуляций со стороны злоумышленника может быть весьма широким: от заражения как можно большего числа компьютеров до получения конфиденциальной информации (данные по счетам и банковским картам, коммерческая и государственная тайна и т.д.). Причем следует отметить, что для получения такой информации целевой компьютер может быть не подключен к сети Интернет (при подключении зараженной флешки к такому компьютеру запускается процесс поиска потенциально интересной информации, а скопированные данные размещаются в секторах устройства, недоступных пользователю; передача скопированных данных «хозяину» выполняется при подключении данной флешки к компьютеру, подключенному к сети Интернет). Исходя из этого, сформулируем следующие правила кибербезопасности.

11) Свести к минимуму подключения к своему компьютеру посторонних флеш-накопителей.

12) Использовать на компьютере специальное ПО (типа USB Security), контролирующее процесс записи информации с/на флешку.

13) По возможности отказаться от использования флеш-памяти (для переноса данных использовать CD или DVD).

**4. Заключение**

В работе рассмотрены основные угрозы компьютерной безопасности с позиции конечного пользователя. В зависимости от источника угроз приведена их классификация. Для всех типов угроз сформулированы правила для повышения уровня компьютерной безопасности. Суммарно сформулировано 13 правил, а также еще дополнительно 3 правила для работы с парольной информацией. Выполнение пользователем этих несложных правил если и не позволит обеспечить абсолютную безопасность, то, по крайней мере, позволит существенно сократить риски. В первую очередь, это будет происходить вследствие того, что злоумышленникам проще найти другую жертву, не обладающую столь эшелонированной обороной.

**Список литературы**

[1] <https://habrahabr.ru/cmpany/panda/blog/283000/> Дата обращения: 04.12.17

[2] Статья в электронной энциклопедии «Википедия» https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F\_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C

[3] <https://support.kaspersky.ru/614>

[4] <http://ftp.drweb.com/pub/drweb/mac/doc/wks/ru/dw_mac_threat_types.htm>

[5] https://support.kaspersky.ru/789#block1

[6] https://www.cvedetails.com/top-50-products.php?year=2016

[7] https://www.anti-malware.ru/malware\_treatment\_test\_2015

[8] https://xakep.ru/2015/09/15/ashley-madison-passwords-2/

[9] https://habrahabr.ru/post/225053/

1. На первый взгляд, кажется, что такая постановка вопроса ставит конкретного пользователя в очень сложное положение. Действительно, как может один человек, возможно, не обладающий серьезными навыками в области компьютерных технологий, делать то, чем занимаются коллективы профессионалов на коммерческом и государственном уровне. Однако при ближайшем рассмотрении окажется, что с одной стороны, даже коллективы профессионалов не гарантируют неуязвимость защищаемой системы, а с другой стороны, пользователь, выполняя несложную последовательность действий, может значительно обезопасить свою деятельность в открытой сети от чужого вмешательства. Дело тут, на мой взгляд, в том, что в большинстве случаев конкретный пользователь становится жертвой киберпреступников, действующих, что называется, «широким бреднем», т.е. сканирующих диапазоны ip-адресов компьютеров, проверяя при этом каждый компьютер на наличие известной уязвимости, или рассылающих «спам» пользователям, почтовые адреса которых стали доступны тем или иным способом. При этом, например, банки становятся целенаправленными объектами кибернападений, в том числе со стороны превосходно подготовленный хакерских объединений. [↑](#footnote-ref-1)
2. Одна из основных проблем, связанных с использованием старых ОС семейства Windows, состоит в том, что в них достаточно просто повысить права доступа (например, с пользователя до администратора), что существенно облегчает жизнь злоумышленникам. [↑](#footnote-ref-2)