УДК 004.49
DOI 10.33764/2618-981X-2022-6-170-178

Безопасность домашнего компьютера

Е. Б. Маркелова[1]*, *Г. В. Попков*[2]
[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[2] Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск, Российская Федерация
*e-mail: Markelova-EB2021@sgugit.ru

Аннотация. Наша жизнь прочно связана с информационными технологиями: мессенджеры, социальные сети, интернет-магазины – все эти средства коммуникации и связи мы используем ежедневно. Именно поэтому информационная безопасность играет важную роль. Учитывая быстрое развитие информационных технологий, все сложнее становится защита информации, именно поэтому необходимость защиты компьютера от несанкционированного доступа, кражи конфиденциальной информации, воздействия вредоносных программ является приоритетным направлением в сфере компьютерных технологий и информационной безопасности. В данной статье представлены основные угрозы безопасности домашнего компьютера, приведены результаты сравнительного анализа способов защиты домашнего компьютера от вирусных, шпионских, хакерских, рекламных и спам-атак, а также от несанкционированного доступа к информации, хранящейся на компьютере личного пользования.

Ключевые слова: вирусы, конфиденциальность, защита

Home Computer Security

E. B. Markelova[1]*, *G. V. Popkov*[2]
[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[2] Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation
* e-mail: Markelova-EB2021@sgugit.ru

Abstract. Our life is firmly connected with information technologies: messengers, social networks, online stores - we use all these means of communication and communication on a daily basis. That is why information security plays an important role. Taking into account the rapid development of information technologies, it is becoming increasingly difficult to protect information, which is why the need to protect a computer from unauthorized access, theft of confidential information, exposure to malware is a priority in the field of computer technology and information security. This article presents the main threats to the security of a home computer, presents the results of a comparative analysis of ways to protect a home computer from virus, spyware, hacker, advertising and spam attacks, as well as from unauthorized access to information stored on a personal computer.

Keywords: viruses, privacy, protection

Введение

В современном мире большинство людей имеют электронно-вычислительные машины, а то и несколько (планшеты, гаджеты, домашние компьютеры). Главным отличием домашнего компьютера от автоматизированного рабочего места является его многофункциональность. Если в организациях техника при-

обретается с какой-то определенной целью, то домашний компьютер используется не только для работы во внерабочее время, но и для личной переписки, компьютерных игр, просмотра информации в сети Интернет, а также для просмотра фильмов и воспроизведения музыки. При этом среди пользователей существует мнение, что домашний компьютер не может интересовать злоумышленников и зачастую уделяется недостаточное внимание рискам, которые возникают при работе в сети Интернет.

Угрозы безопасности информации можно условно разделить на две основные группы:

– угрозы нарушения конфиденциальности, целостности и доступности информации;

– угрозы нарушения требований к содержательной части информации, размещенной в сети Интернет [1, 2].

Взломанный домашний компьютер злоумышленники могут использовать как плацдарм для своих дальнейших действий (например, для DoS-атак). Просмотр новостных сайтов, развлекательных каналов, фильмов онлайн, посещение социальных сетей – всё это несёт в себе реальные угрозы, хотя для обычного пользователя они и неочевидны. Мало кто воспринимает «подвисания» домашнего компьютера и нежелательную рекламу за серьёзную проблему и угрозу как конфиденциальным данным, находящимся на компьютере, так и самому «железу». Шпионские программы и вирусы могут повредить операционную систему без возможности её восстановления, а личные данные попасть к злоумышленникам.

В современном мире защита домашнего компьютера в большинстве случаев производится собственными силами хозяина, поэтому очень важно иметь достаточный уровень знаний о мерах безопасности, применяемых для компьютеров.

Цель данной статьи заключается в проведении сравнительного анализа способов защиты домашнего компьютера от вирусных, шпионских, хакерских, рекламных и спам-атак, а также от несанкционированного доступа к информации, хранящейся на компьютере личного пользования.

Методы и материалы

Для обеспечения компьютерной безопасности в данной статье рассмотрены следующие способы защиты компьютера от несанкционированного доступа, кражи конфиденциальной информации и воздействия вредоносных программ:

– проведение идентификации и аутентификации;

– применение программ для защиты вредоносного воздействия.

Результаты

Идентификация и аутентификация

Основой применения программно-технических средств обеспечения компьютерной безопасности можно считать идентификацию и аутентификацию, что позволяет ограничить доступ к системе [3].

Идентификация – это процедура присвоения субъектам (объектам доступа) идентификаторов и/или сравнение предъявляемого идентификатора с перечнем присвоенных ранее идентификаторов.

Аутентификация – это действия системы по проверке подлинности субъекта доступа (объекта доступа), а также по проверке принадлежности субъекту доступа (объекту доступа) предъявленного идентификатора и аутентификационной информации.

Другими словами, идентификация и аутентификация предполагает подтверждение личности пользователя, сравнение введенных данных с данными, хранящимися в системе с последующим предоставлением пользователю возможности работы в системе с определенными полномочиями. При этом в качестве идентификаторов при обеспечении компьютерной безопасности можно использовать пароли, криптографические ключи, электронные подписи, а также физиологические параметры человека: отпечатки пальцев, сетчатку глаза или, например, стиль работы на клавиатуре (рис. 1).

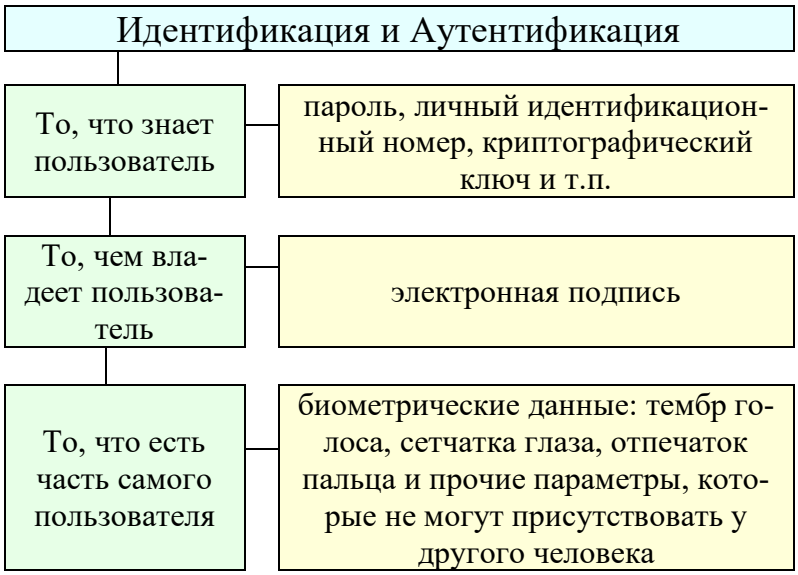

Рис. 1. Виды идентификации и аутентификации

Наиболее распространенным и привычным методом при пользовании домашнего компьютера является метод парольной аутентификации, эффективность которого во многом определяется сложностью пароля. Поэтому при составлении пароля необходимо выполнять ряд требований:

– оптимальная длина пароля – не менее 14 символов;

– сочетание букв верхнего регистра, букв нижнего регистра, цифр и символов;

– не должен содержать личные данные пользователя (имя, фамилия, дата рождения и т.д.);

– отличается от всех предыдущих паролей.

Создав надёжный пароль, необходимо следовать инструкциям для обеспечения его безопасности:

– никому нельзя сообщать свой пароль;

– не отправлять пароли в мгновенном сообщении, по электронной почте или любыми другими средствами связи, в надежности которых пользователь не уверен;

– необходимо использовать уникальный пароль для каждого сайта. Если злоумышленники получат доступ к учетной записи одного сайта, они непременно попытаются использовать полученные данные и для других сайтов, таких как социальные сети и банковские счета;

– можно использовать менеджер паролей. Менеджер паролей – это компьютерная программа, которая позволяет пользователям хранить, генерировать и управлять своими паролями для локальных приложений и онлайн-сервисов. Менеджер паролей помогает генерировать и извлекать сложные пароли, хранить такие пароли в зашифрованной базе данных или вычислять их по требованию;

– можно записать пароли, но хранить их нужно в безопасном месте; ни в коем случае не рядом с компьютером или ноутбуком;

– необходимо использовать многофакторную проверку подлинности. Для многофакторной работы используется несколько данных для входа в учетную запись. Например, пароль и одноразовый код, сгенерированный приложением.

Современные ноутбуки позволяют осуществлять идентификацию и аутентификацию с помощью биометрических данных.

Помимо парольной защиты компьютера не стоит пренебрегать и, например, быстрой блокировкой компьютера. Оставляя работающий компьютер или ноутбук без присмотра, нажмите сочетание клавиш «Alt-Ctrl-Del» и выберите пункт «Блокировка компьютера». Система окажется заблокированной до ввода пароля.

Средства аутентификации и идентификации относятся к категории классических средств по управлению информационной безопасностью. Главным их достоинством является простота и привычность. При правильном использовании пароли могут обеспечить приемлемый уровень безопасности. Тем не менее, по совокупности характеристик, идентификация и аутентификация не может обеспечить безопасность компьютера в полной мере (например, при проникновении в компьютер вредоносных программ).

Защита от вредоносного воздействия

Основной угрозой компьютерной безопасности являются вредоносные программные обеспечения – компьютерные вирусы: вредоносные программы, которые попадают в компьютер несанкционированно, обманным путем либо по неосторожности пользователя. Создают свои копии и внедряют их в загрузочные сектора носителей данных, документы и распространяются по каналам связи. Они представляют собой серьёзную угрозу для безопасности компьютеров. К самым распространённым можно отнести следующие [4]:

– постоянные сбои в работе компьютера (например, опадание букв, искажение внешнего вида элементов управления программ (кнопок, меню и пр.), а также появление дефектов при отображении содержимого окон программ;

– изменение содержимого информации, хранящейся в файле, а также атрибуты файла (имя, дата создания, размер, режим доступа и т.д.). Файлы могут быть удалены или переименованы;

– изменение содержимого жесткого диска, а также частичное или полное удаление файлов с жесткого диска;

– неожиданное значительное увеличение количества файлов на диске;

– существенное уменьшение размера свободной оперативной памяти;

– блокирование работы компьютера;

– реклама и всплывающие окна (очень часто с порнографической информацией), появляющиеся при каждом запуске браузера;

– шантаж и вымогательство денег с угрозами выложить ваши фото, видео в интернет;

– кража персональной информации: логины, пароли, номера банковских карт;

– рассылка спама и вирусные атаки с вашего устройства на другие компьютеры [5, 6].

Вредоносные программы распространяются по следующим каналам и объектам [7]:

– файлы программ;

– загрузочные секторы дисков;

– файлы офисных документов;

– драйверы операционной системы;

– сообщения электронной почты;

– пиринговые (файлообменные) сети;

– интрасеть или Интернет.

Большая угроза проникновения вредоносных программ существует при подключении компьютера к сети либо к внешним носителям.

Идеально защитить компьютер от вредоносных программ невозможно. Но можно снизить риск заражения и повысить уровень безопасности.

Для эффективной защиты домашних компьютеров от вредоносного воздействия можно выделить три типа программ.

1. Программы для защиты от несанкционированного доступа и сетевых хакерских атак. Данную задачу решает брандмауэр (фаерволл) – системная утилита (сетевой экран) для контроля и фильтрации входящего/исходящего трафика. Утилита бывает встроенной в операционную систему и устанавливаемой отдельно, программное обеспечение маршрутизаторов также включает встроенный фаерволл (рис. 2).

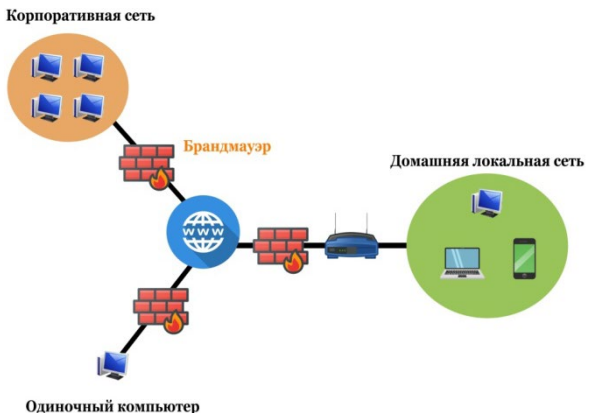

Рис. 2. Принцип работы брэндмауэра

2. Фильтры нежелательной корреспонденции. Спам начинает приходит на тот почтовый ящик, адрес которого попадает в список рассылки злоумышленников. Поэтому отправка на домашний электронный адрес таких писем может означать следующее:

– электронный адрес попал в руки компании, рассылающей спам. Это может произойти в тех случаях, когда пользователь оставляет свои координаты на сайтах, форумах, чатах;

– компьютер, на котором хранился e-mail (например, в адресной книге), был заражен почтовым червем, имеющим процедуру поиска электронных адресов, или трояном, ворующем конфиденциальную информацию, в том числе адреса. Это может быть компьютер друга, коллеги, дальнего знакомого, интернет-магазина или другого сайта, на рассылку писем с которого подписан пострадавший.

Существуют почтовые программы, которые содержат встроенные фильтры. Но при этом для полноценной защиты необходимо регулярное обновление баз. Поэтому установка отдельной, самостоятельной антиспамовой программы – самое лучшее решение для домашних пользователей.

3. Антивирусное программное обеспечение – главный помощник, основной и обязательный элемент защиты, который отвечает за проверку файлов и иных объектов файловой системы на наличие вирусов. В случае их обнаружения предпринимает определенные пользователем действия. Идеально защититься от данной проблемы невозможно, но можно снизить риск заражения и повысить уровень безопасности. С этим пользователю и могут помочь антивирусные программы, которых в настоящее время достаточно немало, их выбор велик. Существуют такие антивирусные программы как: Антивирус Касперского, AVAST, Dr. Web, NOD32 и т. п. Так же стоит отметить, что существует возможность перед приобретением лицензионной версии программы протестировать пробную версию программы, т. к. у каждой антивирусной программы есть множество видов.

К задачам антивирусных программ можно отнести следующие:

- сканирование файлов и программ в режиме реального времени;
- восстановление поврежденных файлов (лечение);
- сканирование интернет-трафика;
- сканирование электронной почты;
- сканирование компьютера по требованию;
- защита от атак враждебных веб-узлов.

Антивирусная защита помогает:

- проанализировать код исполняемых файлов для обнаружения в нем разных типов вредоносного программного обеспечения, не определяемых с помощью антивирусных баз;
- обнаружить и защитить персональный компьютер от всех типов вирусов (включая макро-вирусы, вирусы резидента памяти, вирусы загрузочных секторов, вирусы троянских коней, червей и других вредоносных вирусов);

– обнаружить набор вредоносных приложений, скрывающих свое присутствие на компьютере и позволяющих злоумышленнику действовать незаметно;

– предотвратить распространение любой как известной, так и неизвестной (написанной после появления блокиратора) вредоносной программы, предупреждая пользователя до того, как она заразит другие файлы или нанесет какой-либо вред компьютеру;

– кроме того, антивирусные программы имеют возможность автоматически обновлять свои базы [8].

На первый взгляд антивирусное программное обеспечение давно стало потребительским продуктом, которое устанавливают на каждом персональном устройстве, а пользователь, в свою очередь, выбирает программное обеспечение не за его технические данные, а за удобство или потому, что увидел его в рекламе.

Однако выбор пользователя должен зависеть не от дизайна и внешних элементов программы, а именно от технической части, которая у большинства антивирусных программ значительно отличается.

И без того огромное количество вирусных программ растёт каждый год всё больше и больше. В результате чего антивирусные лаборатории не успевают справиться с такой волной вирусов. Тем самым, при выборе антивирусного программного обеспечения возникает вопрос – от каких именно вирусов защищает данная система и насколько её можно считать надёжной. Сама антивирусная программа должна распознавать и удалять как можно больше вредоносных компонентов.

В таблице ниже (табл. 1) приведен сравнительный анализ функций и возможностей следующих бесплатных антивирусных программ [9]:

1. Avast free antivirus – бесплатная антивирусная программа и простой антишпион. Он может удовлетворить все потребности пользователя. Удобный интерфейс, быстрая и качественная проверка программного обеспечения, приятный дизайн.

2. AVG AntiVirus FREE – еще одна бесплатная антивирусная программа, которая обеспечит базовую защиту компьютера на довольно высоком уровне. Считается одним из лучших продуктов в свободном доступе.

3. Антивирус ESET NOD32 Smart Security – мощное средство для надежной защиты компьютера от различных вирусов. Благодаря встроенному фаерволу, обеспечивает безопасную работу в интернете.

4. Бесплатный Антивирус Касперского создан для надежной защиты персонального компьютера от любых вредоносных программ и веб-сайтов в режиме реального времени. Антивирусный сканер имеет несколько режимов работы.

5. Dr. Web – мощная антивирусная программа для комплексной защиты компьютера от вирусов, троянов, руткитов, шпионского ПО, хакерских атак и прочих вредоносных объектов. Отличается высокой скоростью работы, приятным интерфейсом и простым управлением.

Таблица 1.

Сравнительный анализ функций и возможностей антивирусных программ

	Avast Free Antivirus	**AVG Anti-Virus Free**	**ESET NOD32 Smart Security**	**Antivirus Kaspersky Free**	**Dr.Web Antivirus**
Общий рейтинг	9.2	8	7.7	7.3	5
Общие сведения:					
Лицензия	бесплат-ная	бесплатная	пробная	бесплатная	бесплат-ная
Русский язык	+	+	+	+	+
Поддержка	+	+	+	+	+
Функции и возможности:					
Сканирование по запросу	+	+	+	+	+
Постоянная защита	+	+	+	+	+
Сканирование во время загрузки	+	+	+	+	–
Эвристический алгоритм	+	+	+	+	–
Работа в облаке	+	–	+	–	–
Встроенный firewall	+	–	+	–	–
Система обнаружения вторжений	+	–	+	–	–
Система предотвращения вторжений	–	–	+	–	–
E-mail защита	+	–	+	+	–
Антиспам	+	–	+	–	–
Веб-защита	+	+	+	+	–
Онлайн обновления	+	+	+	+	–
Результаты тестов:					
Время загрузки системы с антивирусом	> 1 мин	> 1 мин	> 1 мин	< 3 мин	> 3 мин
Время сканирования системных папок	> 10 мин	> 10 мин	> 10 мин	> 20 мин	> 15 мин
Использование процессора	3%	17%	10%	6%	19%
Использование памяти	40 Mb	130 Mb	110 Mb	147 Mb	115 Mb

Из приведенной таблицы можно выделить две антивирусных программы, которые максимально удовлетворяют потребностям пользователя: Avast free antivirus (бесплатная) и пробная версия Антивирус ESET NOD32 Smart Security.

Заключение

В данной статье были рассмотрены основные способы защиты компьютера от несанкционированного доступа, кражи конфиденциальной информации, воздействия вредоносных программ, что является приоритетным направлением в сфере компьютерных технологий и информационной безопасности.

Способ, заключающийся в аутентификации и идентификации позволяет установить лицо, которое получает доступ к компьютеру, но не может обеспечить защиту в полной мере. Поэтому так же необходимо использовать способы, позволяющие защитить компьютер от воздействия вредоносных программ.

В результате сравнительного анализа можно сделать вывод, что для оптимальной защиты необходимо использовать комплекс мер, включающий проведение идентификации и аутентификации, а так же применение программ для защиты от несанкционированного доступа, спам-атак и воздействия вредоносных программ.

Кроме того необходимо иметь в виду, что одним из важных моментов является повышение грамотности пользователей в области информационной безопасности [10]. Демонстрация уязвимостей и последствий воздействия вредоносного программного обеспечения способна заинтересовать пользователя и позволит не стать ему лёгкой целью для злоумышленников.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Михайлов В.А. Проблемы современных антивирусных систем / В.А. Михайлов [Электронный ресурс]: статья Студенческий научный форум – 2021 – Режим доступа: https://scienceforum.ru/2021/article/2018025240
2. Напханенко Е.О. Понятие и классификация угроз информационной безопасности в сети Интернет / Е.О. Напханенко – ЮП. 2011. №4.
3. ГОСТ Р 58833-2020. Национальный стандарт Российской Федерации. Защита информации. Идентификация и аутентификация. Общие положения. Дата введения 2020-05-01. – М.: Стандартинформ, 2020.
4. Современная антивирусная индустрия [Электронный ресурс]: https://securelist.ru/sovremennaya-antivirusnaya-industriya/711/.
5. Эндрю Конри-Мюррей. Защита конечных пользователей от атак // LAN. 2002. № 11.
6. Исаков Д.А. Уязвимости домашнего сетевого оборудования [Электронный ресурс]: статья Научно-практический журнал Информационная безопасность регионов, 2015 № 1(18) – Режим доступа: https://cyberleninka.ru.
7. Грошева Е.К., Невмержицкий П.И. Информационная безопасность [Электронный ресурс]: современные реалии статья Бизнес-образование в экономике знаний, 2017 № 3 – Режим доступа: https://cyberleninka.ru/.
8. Башкирова Л. А. Компьютерная безопасность в современном мире / Л. А. Башкирова – Казань: Международный научный журнал, № 14 (148) / 2017 – ISSN 2072-0297.
9. Рейтинг антивирусов [Электронный ресурс]: https://softcatalog.info/ru/obzor/reyting-antivirusov (дата обращения 04.04.2022).
10. Солдатова Г.У. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г. У. Солдатова, Т. А. Нестик, Е. И. Рассказова, Е. Ю. Зотова. – М.: Фонд Развития Интернет, 2013.