Published in the Slovak Republic
Vestnik policii
Has been issued since 2014.
ISSN: 2409-3610
E-ISSN: 2414-0880
2017, 4(1): 19-24

DOI: 10.13187/vesp.2017.1.19
www.ejournal21.com

Technical Means

UDC 681.3

Some Aspects of Cybersecurity of the Personal Computers, connected to the Internet

Yuri F. Katorin [a, *], Artem A. Gonchar [b]

[a] Admiral Makarov State University of Maritime and Inland Shipping, Russian Federation
[b] St. Petersburg University of the Russian Interior Ministry, Russian Federation

Abstract

This article is dedicated to the description of a number of the simple means, with the aid of which it is possible to stop attempts at the penetration to the information of the computer, connected into the network, it is noted, that safety of computer with the work in the Internet depends on many factors, and first of all – from the observance by the user of entire complex of rules and precautions, are given recommendations regarding raising safety level, if there is no possibility to create the complex protective system.

Keys words: the threat of computer safety, the Internet, computer viruses, providing data security, spyware, the unsanctioned access.

1. Введение

Большинство людей, использующих компьютерные технологии и Интернет, в настоящее время осознали значимость разрешения проблемы защиты компьютерных данных от злоумышленников. Немало тому способствовали скандальные судебные разбирательства, связанные с взломом корпоративных компьютерных сетей, с целью промышленного шпионажа, воровства, или нарушения производственного процесса. Угрозы компьютерной безопасности могут быть разнообразными: различные компьютерные вирусы, уязвимости почтовых интернет программ, хакерские взломы и атаки, шпионские модули, короткие пароли, пиратское программное обеспечение, посещение различных вредоносных сайтов, отсутствие антивирусных программ и многое другое (Бармен Скотт, 2002; Борисов, 2013).

В современных условиях любая деятельность сопряжена с оперированием большими объемами информации, которое производится широким кругом лиц. Защита данных от несанкционированного доступа является одной из приоритетных задач при проектировании любой информационной системы. Следствием возросшего в последнее время значения информации стали высокие требования к конфиденциальности данных. Системы управления базами данных (СУБД), в особенности реляционные стали доминирующим

* Corresponding author
E-mail addresses: katorin@mail.ru (Y.F. Katorin), gonchar.tema@yandex.ru (A.A. Gonchar)

инструментом в этой области. К сожалению, злоумышленники постоянно ищут и находят в операционной системе слабые места, так называемые «дыры», через которые они могут проникнуть в Windows. Мошенники с каждым разом придумывают все новые и новые системы кражи информации (Каторин и др., 2012: 99).

2. Материалы и методы

Материалами для исследования послужила российская и зарубежная специализированная историография и справочная литератур, а также официальные государственные, ведомственные, нормативные правовые акты России.

В ходе анализа источников и литературы, а также в выводах, являющихся итогом исследования, автор, использовав метод историко-сравнительного анализа, стремится к научной объективности, непременным условием которой выступает фундаментальный методологический принцип историзма, а также широко применен историко-описательный метод. Методологическую основу исследования составляют общенаучные (анализ и синтез, диалектический, системный, логический) методы.

3. Обсуждение

Компьютерная система абсолютно защищена тогда, когда она выключена, разобрана, заперта в бункере и единственный ключ от этого бункера уничтожен. Любое отклонение от этого состояния делает компьютер потенциально уязвимым. Кибербезопасность — процесс использования мер безопасности для обеспечения конфиденциальности, целостности и доступности данных. Она обеспечивает защиту активов, включая данные локальной сети компьютеров, серверов. Кроме того, под охрану берутся непосредственно здания и, самое главное, персонал. Целью обеспечения кибербезопасности является защита данных (как в процессе передачи и/или обмена так и находящихся на хранении). В целях обеспечения безопасности данных могут быть применены и контрмеры. Некоторые из этих мер включают (но не ограничиваются) контроль доступа, обучение персонала, аудит и отчетность, оценку вероятных рисков, тестирование на проникновение и требование авторизации (Галицкий и др., 2004: 236-238).

Основная угроза компьютерной безопасности – это компьютерные вирусы. Вирус – это достаточно продуманная программа, которая самостоятельно записывается на ваш компьютер и выполняет определенные действия, которые были заданы ранее хакерами при создании. Обычно происходит так, что компьютерные вирусы на компьютере стараются скрывать свое присутствие и выполняют определенные операции. Вирусы действуют с большой скоростью, начинают искать различные уязвимости на компьютере! Чтобы обезопасить себя от разных вирусов, следует установить программное обеспечение, называемое антивирус. Он предназначен для защиты компьютеров. Большинство антивирусных программ являются платными, но есть также и довольно много бесплатных антивирусов. Антивирусы стоят не дорого, поэтому для полноценной защиты лучше приобрести лицензию (Петренко, 2004: 28-31).

Кроме вирусов есть программы, которые называются программы-шпионы. Такие программы очень редко обнаруживаются антивирусами. Это связано с тем, что шпионы самовольно не распространяются, не вредят компьютеру и не совершают никаких действий. Эти программы просто следят за нажатием клавиш на компьютере и при подключении к интернету отсылают все данные на сервер хакеров. Также шпионы позволяют вирусам проникать в системы компьютеров, тем самым создавая уязвимости в операционных системах. Обычные антивирусы здесь уже вам не помогут (Петренко, 2004: 228).

Чтобы обезопасить себя от шпионов, нужно устанавливать специальное программное обеспечение – анти-шпионы. Как правило, такие программы называются фаерволы. Они следят за всеми соединениями компьютера в сети, и принимают решение о доступе в сеть каждой программы. Часто в станицах есть элементы кода, которые на экране не отображаются. Такие элементы кода могут нести в себе угрозу для пользователей. Фаервол может отключать такие элементы кодов, угрожающие безопасности компьютера (Борисов и др., 2013: 186).

4. Результаты

Безопасность компьютера при работе в интернете зависит от множества факторов, и в первую очередь — от соблюдения пользователем всего комплекса правил и предосторожностей, а также от настроек, как пользовательских, так и по умолчанию, установленных патчей и антивирусов, средств защиты на интернет-шлюзе и многого другого (Вихров и др., 2015: 82, ГОСТ, 2005).

Существует ряд простых средств, с помощью которых можно остановить попытки проникновения в ваш компьютер или в сеть, к ним относятся:

- обеспечение защищенного хранения информации на носителях;
- защита данных, передаваемых по каналам связи;
- оперативная установка исправлений для программ, работающих в интернете.
- антивирусные программы по обнаружению различного рода взломов и вирусов незаменимы для повышения безопасности любой сети. Они наблюдают за работой компьютеров и выявляют на них вредоносные программы;
- следует использовать наиболее надежные пароли, менять их как можно чаще и чтобы их длина была максимальной. Это может предотвратить кражу секретной и не секретной информации;
- соединения с удаленными компьютерами должны быть защищены с помощью паролей, чтобы избежать проникновения в сеть с помощью прослушивания сетевого трафика в наиболее важных местах и выделения из него имен пользователей и их паролей;
- при установке новой операционной системы обычно разрешаются все сетевые средства, что является не безопасным. Кроме вышеперечисленных средств защиты информации, существует еще множество способов предотвращения взломов и краж информации. Для избегания неприятных ситуаций необходимо изучать рекомендации по безопасности и придерживаться необходимых средств защиты (Ныркov и др., 2015: 56-58).

Если риски не велики и нет необходимости тратиться на создание специальной системы зажиты, то следует помнить, что при прочих равных условиях:

1. Браузеры Opera 28 и Firefox 36 безопаснее, чем Opera и Firefox предыдущих версий. Microsoft Internet Explorer 11 существенно безопаснее предыдущих версий Microsoft Internet Explorer.

2. Если в операционной системе установлен и включен антивирус — работать в ней безопаснее, чем без антивируса. Высокие оценки AV Comparatives в 2014 получили антивирусы Kaspersky, ESET, BitDefender, Avast! Free Antivirus, AVIRA, Panda Cloud Antivirus, F-Secure, G DATA. Некоторые антивирусы из этого списка являются бесплатными, например: Kaspersky, Avast! Free Antivirus и Panda Cloud Antivirus.

При этом следует помнить, что обновление и доступ к интернету являются для большинства современных антивирусов критически важными, без этого эффективность их защиты быстро снижается.

3. Если в операционной системе включен и правильно настроен файрволл, она безопаснее. Правильная настройка заключается в том, чтобы в брандмауэре была разрешена только та сетевая активность, в которой есть необходимость. Брандмауэр можно включить так:

Microsoft Windows XP: Пуск → Панель управления → Центр обеспечения безопасности → Брандмауэр Windows → Включить → ОК.

Microsoft Windows 7: Пуск → Панель управления → Система и безопасность → Брандмауэр Windows → Включение и отключение брандмауэра Windows → Включение брандмауэра Windows в доменных, домашних и рабочих, а также в общественных сетях.

4. Работать под учетной записью с ограниченными полномочиями существенно безопаснее, чем под учетной записью с правами локального, а тем более доменного системного администратора. Кроме того, рекомендуется, чтобы:

- полномочия учетной записи соответствовали компьютерной грамотности и ответственности тех, кто под ней работает;

- вход под учетной записью системного администратора был возможен только после ввода пароля, причем не формального «qwerty» или «111», а полноценного: минимум 11 букв в разных регистрах, цифр и специальных символов.

5. Microsoft Windows 7 безопаснее предыдущих операционных систем компании Microsoft для рабочих станций, в том числе Microsoft Windows XP. UNIX-подобные операционные системы (в том числе Linux, BSD, «промышленные» UNIX) безопаснее остальных распространенных ОС.

6. Если программное обеспечение, в том числе операционная система, обновляются, они безопаснее. Обновление можно включить так:

Microsoft Windows XP: Пуск → Панель управления → Центр обеспечения безопасности → Автоматическое обновление → Автоматически → ОК.

Microsoft Windows 7: Пуск → Панель управления → Система и безопасность → Центр обновления Windows: Включение и выключение автоматического обновления → Важные обновления: Устанавливать обновления автоматически.

7. Неофициальные сборки, а также образы программных продуктов, распространяемые неофициально (в том числе на контрафактных дисках, с помощью торрентов и «неофициальных» зеркал сайтов) часто менее безопасны, чем официальные.

8. Делайте резервные копии наиболее ценных для вас данных, так как вредоносные программы могут блокировать доступ к системе, шифровать данные на дисках, а иногда и безвозвратно их портить. При этом платить деньги злоумышленникам за восстановление доступа к собственным данным означает финансировать разработку и распространение новых, еще более изощренных вредоносных программ. Желательно, чтобы копии хранились отдельно от компьютера, например на переносных устройствах

9. Если на вашем компьютере хранится очень важная информация, ее следует хранить в отдельных папках, а если основная информация хранится на флешке, то следует также сделать резервные копии. Такие носители часто портятся, теряются, глючат.

10. Если с вашего носителя была удалена важная информация, не стоит сразу же отчаиваться. Существует множество программ, которые восстанавливают удаленные файлы почти на 100 процентов. Принцип работы таких программ в том, что они видят все файлы, которые были на флешке. Если вы не видите файлов, и система пишет что носитель пустой, это еще не говорит о том, что информация полностью удалена (Шушков, Сергеев, 2016: 72-75).

6. Выводы

Удобство почти всегда противоречит безопасности. Система с полностью отключенной безопасностью «не мешает» пользователю ограничениями, вопросами, необходимостью дополнительных подтверждений и действий. Работа антивируса часто снижает быстродействие системы, авторизация и переключение учетных записей — отнимает время.

Но потеря данных часто стоит дороже, ведь среди них могут быть результаты работы и хобби, фотографии, архивы, коллекции, данные для авторизации в платежных системах, системах обмена сообщениями, социальных сетях, онлайн-играх. Даже если учитывать только потери времени, то на однократное восстановление данных и работоспособности системы его обычно уходит больше, чем на соблюдение правил техники безопасности работы с интернетом в течение нескольких лет.

Сейчас в некоторых странах планируется обучение кибербезопасности уже со школьной скамьи. Так, в Великобритании школьникам предлагаются уроки по кибербезопасности, на которых они будут обучаться навыкам, позволяющим обеспечить безопасность британских компаний и организаций от сетевых атак хакеров.

Однако эти программы не смогут защитить ваш компьютер от физических контактов с другими людьми, то есть любой ваш сотрудник или друг может сесть за компьютер и просмотреть вашу личную информацию. Но это уже тема для совсем другой статьи.

7. Благодарности

Публикация подготовлена при финансовой поддержке Минобрнауки России (соглашение № 02.a03.21.0008).

Литература

Бармен Скотт, 2002 – *Бармен Скотт*. Разработка правил информационной безопасности. М.: Вильямс, 2002. 208 с.

Борисов и др., 2013 – *Борисов М.А., Заводцев И.В., Чижов И.В.* Основы программно-аппаратной защиты информации. Изд.2 М.: Книжный дом «ЛИБРОКОМ», 2013. 376 с.

Вихров и др., 2015 – *Вихров Н.М., Ныркoв А.П., Каторин Ю.Ф., Шнуренко А.А., Башмаков А.В., Соколов С.С., Нурдинов Р.А.* Анализ информационных рисков. Морской вестник. 2015. № 3 (55). С. 81-85.

Галицкий и др., 2004 – *Галицкий А.В., Рябко С.Д., Шаньгин В.Ф.* Защита информации в сети — анализ технологий и синтез решений. М.: ДМК Пресс, 2004. 616 с.

ГОСТ, 2005 – ГОСТ ИСО/МЭК 27000 — серия стандартов по менеджменту информационной безопасности. 2005.

Каторин и др., 2012 – *Каторин Ю.Ф., Коротков В.В., Ныркoв А.П.* Защищенность информации в каналах передачи данных в береговых сетях автоматизированной идентификационной системы // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. 2012. № 1. С. 98-102.

Ныркoв и др., 2013 – *Ныркoв А.П., Каторин Ю.Ф., Соколов С.С., Ежгуров В.Н.* Основные принципы построения защищенных информационных систем автоматизированного управления транспортно-логическим комплексом. Проблемы информационной безопасности. Компьютерные системы. 2013. № 2 (2). С. 54-58.

Петренко, 2004 – *Петренко С.А.* Управление информационными рисками. М.: Компания АйТи; ДМК Пресс, 2004. 384 с.

Шушков, Сергеев, 2016 – *Шушков Г.М., Сергеев И.В.* Концептуальные основы информационной безопасности Российской Федерации / Актуальные вопросы научной и научно-педагогической деятельности молодых ученых: сборник научных трудов III Всероссийской заочной научно-практической конференции (23.11.2015 – 30.12.2015 г., Москва) / под общ. ред. Е.А. Певцовой. М.: ИИУ МГОУ, 2016. С. 69-76.

Щербаков, 2009 – *Щербаков А.Ю.* Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный мир, 2009. 352 с.

References

Barmen Skott, 2002 – *Barmen Skott* (2002). Razrabotka pravil informatsionnoi bezopasnosti [Development of the rules of information safety]. M.: Vil'yams, 208 s. [in Russian]

Borisov i dr., 2013 – *Borisov M.A., Zavodtsev I.V., Chizhov I.V.* (2013). Osnovy programmno-apparatnoi zashchity informatsii [Bases of the firmware protection of information]. Izd.2 M.: Knizhnyi dom «LIBROKOM», 376 s. [in Russian]

Galitskii i dr., 2004 – *Galitskii A.V., Ryabko S.D., Shan'gin V.F.* (2004). Zashchita informatsii v seti — analiz tekhnologii i sintez reshenii [Protection of information in the network — the analysis of technologies and the synthesis of the solutions]. M.: DMK Press, 616 s. [in Russian]

GOST, 2005 – GOST ISO/MEK 27000 — seriya standartov po menedzhmentu informatsionnoi bezopasnosti [ALL-UNION STATE STAN. ISO/MEK 27000 — a series of standards on the management of information safety]. 2005.

Katorin id r., 2012 – *Katorin Yu.F., Korotkov V.V., Nyrkov A.P.* (2012). Zashchishchennost' informatsii v kanalakh peredachi dannykh v beregovykh setyakh avtomatizirovannoi identifikatsionnoi sistemy [Protection of information in data links in coast networks of the automated identification system]. *Vestnik gosudarstvennogo universiteta morskogo i rechnogo flota im. admirala S.O. Makarova*. № 1. S. 98-102. [in Russian]

Nyrkov i dr., 2013 – *Nyrkov A.P., Katorin Yu.F., Sokolov S.S., Ezhgurov V.N.* (2013). Osnovnye printsipy postroeniya zashchishchennykh informatsionnykh sistem avtomatizirovannogo upravleniya transportno-logicheskim kompleksom [Basic principles of the construction of the protected information systems of automated management by transport-logical complex]. *Problemy informatsionnoi bezopasnosti. Komp'yuternye sistemy*. № 2 (2). S. 54-58. [in Russian]

Petrenko, 2004 – *Petrenko S.A.* (2004). Upravlenie informatsionnymi riskami [Control of information risks]. M.: Kompaniya AiTi; DMK Press, 384 s. [in Russian]

Shcherbakov, 2009 – *Shcherbakov A.Yu.* (2009). Sovremennaya komp'yuternaya bezopasnost'. Teoreticheskie osnovy. Prakticheskie aspekty [Contemporary computer safety. Theoretical bases. Practical aspects]. M.: Knizhnyi mir, 352 s. [in Russian]

Shushkov, Sergeev, 2016 – *Shushkov G.M., Sergeev I.V.* (2016). Kontseptual'nye osnovy informatsionnoi bezopasnosti Rossiiskoi Federatsii [The conceptual bases of information safety of the Russian Federation]. Aktual'nye voprosy nauchnoi i nauchno-pedagogicheskoi deyatel'nosti molodykh uchenykh: sbornik nauchnykh trudov III Vserossiiskoi zaochnoi nauchno-prakticheskoi konferentsii (23.11.2015 – 30.12.2015 g., Moskva). pod obshch. red. E.A. Pevtsovoi. M.: IIU MGOU, 2016. S. 69-76. [in Russian]

Vikhrov id r., 2015 – *Vikhrov N.M., Nyrkov A.P., Katorin Yu.F., Shnurenko A.A., Bashmakov A.V., Sokolov S.S., Nurdinov R.A.* (2015). Analiz informatsionnykh riskov [Information risk analysis]. *Morskoi vestnik*. № 3 (55). S. 81-85. [in Russian]

УДК 681.3

Некоторые аспекты кибербезопасности персональных компьютеров, включенных в сеть Интернет

Юрий Федорович Каторин [a, *], Артем Александрович Гончар [b]

[a] Государственный университет морского и речного флота имени адмирала С.О. Макарова, Российская Федерация
[b] Санкт-Петербургский Университет МВД, Российская Федерация

Аннотация. Данная статья посвящена описанию ряда простых средств, с помощью которых можно остановить попытки проникновения к информации компьютера, подключенного в сеть, отмечено, что безопасность компьютера при работе в интернете зависит от множества факторов, и в первую очередь – от соблюдения пользователем всего комплекса правил и предосторожностей, даны рекомендации по повышению уровня безопасности, если нет возможности создать сложную систему защиты.

Ключевые слова: угрозы компьютерной безопасности, Интернет, компьютерные вирусы, обеспечение безопасности данных, программы-шпионы, несанкционированный доступ.

[*] Корреспондирующий автор
Адреса электронной почты: katorin@mail.ru (Ю.Ф. Каторин), gonchar.tema@yandex.ru (А.А. Гончар)