Научная статья
Original article
УДК 004.056.53.

СПОСОБЫ ЗАЩИТЫ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

WAYS TO PROTECT AGAINST MALWARE

Смирнов Виталий Михайлович, к.т.н., старший преподаватель кафедры информатики и математики Московского университета МВД имени В.Я. Кикотя. (Россия 117997, г. Москва, ул. Академика Волгина, д. 12.)

Матвеев Станислав Павлович, курсант Московского университета МВД имени В.Я. Кикотя. (Россия 117997, г. Москва, ул. Академика Волгина, д. 12)

Smirnov Vitaly Mikhailovich, Candidate of Technical Sciences, Senior Lecturer at the Department of Computer Science and Mathematics of the Moscow University of the Ministry of Internal Affairs named after V.Ya. Kikot. (12 Akademika Volgina str., Moscow, 117997, Russia)

Matveev Stanislav Pavlovich, cadet of the V.Ya. Kikot Moscow University of the Ministry of Internal Affairs. (12 Akademika Volgina str., Moscow, 117997, Russia)

Аннотация: в статье мы хотим раскрыть сущность понятия вредоносного программного обеспечения и более подробно рассмотреть вопросы, связанные с видами компьютерных угроз, что, в свою очередь, обязывает изучить способы борьбы с вредоносным программным обеспечением.

Annotation: In this article we want to reveal the essence of the concept of malicious software and consider in more detail the issues related to the types of computer threats, which, in turn, obliges us to study ways to combat malicious software.

***Ключевые слова*:** вредоносное программное обеспечение, информация, способы, защита, меры безопасности.

***Keywords**:* malware, information, methods, protection, security measures.

В эпоху развития информационного общества и плотного внедрения современных компьютерных технологий в жизнь человека, сложно представить, что хотя бы один пользователь не сталкивался с таким явлением, как вредоносное программное обеспечение.

В соответствии с государственным стандартом, вредоносное программное обеспечение или вредоносная программа – это программа, которая служит для реализации несанкционированного доступа к информации и/или оказания разрушающего воздействия на информацию, элементы информационной системы в целом, а также для нарушения ее конструктивной целостности и/или доступности[1].

Проникновение современных модифицированных технологий во все сферы жизни общества имеет 2 стороны. С одной стороны, данное явление позволяет человеку участвовать в обмене информацией, помогает в трудовой деятельности и в целом упрощает жизнь общества. Но есть и обратная сторона. Из-за активного внедрения информационных технологий стали рождаться новые угрозы, а именно: заражения многочисленными видами компьютерных вирусов, каждый из которых имеет уникальный побочный эффект, а обнаружить его не так просто; модификация, блокирование или уничтожение информации с ее носителя; ограничение доступа пользователей ПК; информационное подавление обмена данными в сети и многое другое.

По данным официальной статистики, представленной Генеральной прокуратурой РФ в структуре преступности киберпреступления занимают более четверти (26,7 %, 494 тыс.). Более чем в 60 тыс. случаев от таких преступлений пострадали пенсионеры, в 6 тыс. – несовершеннолетние, в 2,5 тыс. – инвалиды.

[1] ГОСТ Р 53113.1-20008

Таким образом, подтверждаем актуальность выбранной нами темы. В период вступления современного общества в Индустрию 4.0, виртуальное является самым распространенным, что несет за собой риски и обязывает разрабатывать и использовать различные способы защиты от программ, зараженных компьютерными вирусами, созданного злоумышленниками.

Если рассматривать компьютерные вирусы, то мы можем проследить некую общую закономерность – скрытое проникновение, закрепление и последующее заражение устройства, но несмотря на огромный массив разновидностей вредоносного программного обеспечения, в лице вирусов, троянов, червей, выводятся общие способы и методы указанных выше проблем:

1. Воспрепятствование самостоятельному запуску вредоносной программы. Это можно сделать следующим образом, отключить обработку файла автоматическим запуском, которая априори включена. Положительной стороной данного метода служит безопасная деятельность конкретных рабочих станций от носителя заражения, но негативным последствием такого способа служит то, что появляется необходимость отключения автоматического запуска на рабочих станциях.

2. Аппаратное блокирование записи новой информации на электронный носитель. Оно регулируется посредством переключателя на корпусе устройства. Главным минусом указанного способа служит блокировка всей информации, поступающей на ПК, в том числе легальной.

3. Следующий способен актуален лишь для устройств, которые поддерживают файловую систему NTFS. Механизм работы защиты заключается в том, что очищается устройство, после чего в «сердце» диска создаются папки, затем осуществляется запрет записи информации в корне устройства, т.е. вирус не имеет возможности записи в корневой каталог устройства.

Также мы предлагаем еще один комплекс способов защиты информации от злоумышленников:

- Межсетевые экраны – данный способ считаем одним их наиболее важных, так как он представляет целую систему, которая образует защитную преграду для исключения явлений несанкционированного доступа к информации;
- Посредством программ образовать «барьер» для завладения данными пользователя третьими лицами;
- Кодирование информации или шифрование;
- Резервное копирование;
- Установка такого программного обеспечения, которое позволит защитить данные от незаконного доступа;
- Аутентификация и идентификация владельца или пользователя.

В эпоху развития информационного общества и развития высоких технологий, информация приобрела огромное значение, и именно ее безопасность подвергается угрозам и «нападениям», что является серьезной проблемой, которая может достичь международного уровня. Похищение, распространение или разглашение сведений, представляющих личную, коммерческую, государственную или военную тайну могут служить необратимыми последствиями. Именно поэтому важно в полном мере осуществлять защиту своих данных, проявлять особую бдительность к подозрительным сайтам, ссылкам или звонкам, что обеспечит минимизацию угроз информационной безопасности.

Библиографический список:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 01.07.2020 N 11-ФКЗ) // Собрание законодательства РФ. .2020. N 31. ст. 4398.
2. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ.
3. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ.

4. Арутюнова В.И. Классификационная характеристика угроз воздействия вредоносных программ на информационные процессы в компьютерных системах / В.В. Киселев, Д.А. Голубков, В.И. Арутюнова // Вестник Воронежского института ФСИН России. - 2016. - № 2. - С.49-56.
5. Статистические данные Генеральной Прокуратуры РФ [Электронный ресурс]: URL: https://genproc.gov.ru/stat/data/1557476/ (дата обращения: 28.02.2022).

List of references used:

1. Constitution of the Russian Federation (adopted by popular vote on 12.12.1993) (with amendments made by the RF Laws on amendments to the RF Constitution dated 30.12.2008 N 6-FKZ, dated 30.12.2008 N 7-FKZ, dated 05.02.2014 N 2-FKZ, dated 01.07.2020 N 11-FKZ) // Collection of Russian Federation Laws. N 31. art. 4398.
2. Federal Law "On Information, Information Technologies and Information Protection" of 27.07.2006 N 149-FZ.
3. Federal Law "On personal data" 27.07.2006 N 152-ФЗ.
4. Arutyunova V.I. Classification characteristics of threats to the impact of malicious programs on information processes in computer systems / V.V. Kiselev, D.A. Golubkov, V.I. Arutyunova // Bulletin of the Voronezh Institute of the Federal Penitentiary Service of Russia. - 2016. - № 2. - C.49-56.
5. Statistical data of the General Prosecutor's Office of the Russian Federation [Electronic resource]: URL: https://genproc.gov.ru/stat/data/1557476/ (access date: 28.02.2022).

© Матвеев С.П.,Смирнов В.М. 2022 Научно – образовательный журнал для студентов и преподавателей «StudNet» 3/2022

Для цитирования: Матвеев С.П., Смирнов В.М. Способы защиты от вредоносного программного обеспечения // *Научно – образовательный журнал для студентов и преподавателей «StudNet» 3/2022*