ИНЖЕНЕРНОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

Научная статья
УДК 681.3; DOI: 10.61260/2307-7476-2024-1-16-23

МОНИТОРИНГ ОПЕРАЦИОННОЙ СИСТЕМЫ КАК СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ

✉**Лабинский Александр Юрьевич.**
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉***labynsciy@yandex.ru***

Аннотация. Рассмотрен один из методов защиты информации на ЭВМ – мониторинг операционной системы.

Анализ вредоносных программ для ЭВМ показывает, что увеличивается количество их разновидностей, повышается вредоносность и прослеживается коммерческое применение. Разработчики вредоносных программ все чаще применяют «экзотические» методы их внедрения в операционную систему ЭВМ. Некоторые вредоносные программы применяют вирусные технологии.

Решением проблемы защиты информации на ЭВМ от вредоносных программ является использование специальных программ, выполняющих исследование (мониторинг) операционной системы ЭВМ.

Подробно рассмотрены утилиты для мониторинга операционной системы, установленной на персональном компьютере: File Monitor (мониторинг операций с файлами), которая позволяет осуществлять мониторинг всех файловых операций в реальном времени; Registry Monitor (мониторинг операций с реестром); TCP View (мониторинг сетевой активности), особенностью которой является привязка прослушиваемого порта или открытого соединения к использующему его процессу; утилита управления автозапуском приложений Auto Runs, которая анализирует десятки различных методов автозапуска, в том числе классические методы автозапуска, расширения проводника разных видов, задания планировщика, службы и драйверы, библиотеки печати и провайдеры; утилита – диспетчер процессов Process Explorer, которая позволяет изменить приоритет процесса, приостановить процесс и все его потоки, принудительно завершить процесс.

Ключевые слова: вредоносная программа, защита информации, мониторинг операционной системы, персональный компьютер, мониторинг операций с файлами, мониторинг операций с реестром, мониторинг сетевой активности, управление автозапуском, диспетчер процессов

Для цитирования: Лабинский А.Ю. Мониторинг операционной системы как средство защиты информации // Природные и техногенные риски (физико-математические и прикладные аспекты). 2024. № 1 (49). С. 16–23. DOI: 10.61260/2307-7476-2024-1-16-23.

Scientific article

THE MONITORING OF OPERATING SYSTEM AS THE MEANS OF THE INFORMATION PROTECTION

✉**Labinskiy Alexander Yu.**
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉***labynsciy@yandex.ru***

Abstract. The article considers one of the methods of information protection on the computer – monitoring of the operating system.

Malicious software for computers are numerous, they are constantly updated and new programs with new principles of malicious work appear. Therefore, the use of antivirus and anti-spyware is often ineffective, as they work on the principle of signature search (sample search) and therefore cannot detect new varieties of malware.

The solution to this problem is the use of various utilities (service programs) for monitoring (research) of the operating system installed on the computer.

The article describes in detail the utilities for monitoring the operating system installed on the PC. This is a monitoring utility of the operating system: File Monitor (monitoring file operations), which allows you to monitor all file operations in real time; Registry Monitor (monitoring registry operations); TCP View (monitoring network activity)a feature of which is the binding of the listening port or open connection to the process that uses it; the auto run application control utility Auto Runs, which analyzes dozens of different autorun methods, including classic autorun methods, extensions of different types of explorer, scheduler jobs, services and drivers, print library and providers; Process Explorer utility, which allows you to change the priority of the process, stop the process and all its threads, force the process to end.

Keywords: malware, information protection, operating system monitoring, personal computer, file operations monitoring, registry operations monitoring, network activity monitoring, autostart management, process manager

For citation: Labinskiy A.Yu. The monitoring of operating system as the means of the information protection // Prirodnye i tekhnogennye riski (fiziko-matematicheskie i prikladnye aspekty) = Natural and man-made risks (physico-mathematical and applied aspects). 2024. № 1 (49). P. 16–23. DOI: 10.61260/2307-7476-2024-1-16-23.

Введение

ЭВМ широко используются в системах управления многих важных и опасных технологических объектов, например, в таких, как атомные электростанции. Выход из строя таких ЭВМ связан с риском больших материальных потерь и может привести, при определенных условиях, к гибели людей.

Несмотря на огромные усилия по созданию технологий защиты информации их уязвимость в современных условиях не только не уменьшается, а постоянно возрастает. Поэтому актуальность проблемы защиты информации постоянно увеличивается [1], и методам обеспечения защиты информации на ЭВМ посвящается много работ [2–10]. В данной статье рассматривается один из методов защиты информации на ЭВМ – мониторинг операционной системы.

Вредоносные программы для ЭВМ многочисленны, они постоянно обновляются, появляются новые программы с новыми принципами вредоносной работы. Поэтому применение антивирусных и антишпионских программ часто является малоэффективным, так как они работают по принципу сигнатурного поиска (поиска по образцу) и поэтому не могут выявлять новые разновидности вредоносных программ.

Решением этой проблемы является применение различных утилит (сервисных программ) для мониторинга (исследования) операционной системы, установленной на ЭВМ. Большинство из них, как правило, не могут выявлять вредоносные программы, но позволяют обнаруживать на ЭВМ подозрительные объекты, требующие последующего анализа и изучения, в том числе с помощью антивирусных и антишпионских программ. Такие утилиты обычно не требуют особой квалификации и специальных знаний, могут использоваться рядовыми пользователями, и большинство из них распространяется бесплатно.

Сформулируем постановку задачи, результаты решения которой представлены в данной статье. Нужно произвести обзор утилит мониторинга операционной системы, установленной на ЭВМ. Тема статьи актуальна, так как важность вопросов защиты информации на ЭВМ не вызывает сомнений.

Новизна исследования, отражающая личный вклад автора, заключается в том, что с целью обеспечения защиты информации на ЭВМ в статье обобщена информация по применению различных утилит для мониторинга операционной системы, установленной на ЭВМ.

Далее будут рассмотрены утилиты, которые распространяются бесплатно и могут работать без инсталляции.

Утилиты мониторинга операционной системы

Основная задача утилит мониторинга операционной системы состоит в наблюдении за операционной системой и регистрации различных событий в протоколах. Обычно в процессе поиска подозрительных объектов применяются три вида мониторинга:

– мониторинг операций с файлами и дисковых операций;
– мониторинг операций с реестром;
– мониторинг сетевой активности приложений.

Утилита File Monitor

В процессе мониторинга следует учитывать, что некоторые антивирусные программы, установленные на исследуемом компьютере, могут принимать данные средства мониторинга как инструменты, используемые вредоносными программами. При этом антивирусные программы могут либо активно противодействовать работе программ мониторинга, либо блокировать работу защищаемых приложений. Подобное поведение иногда можно принять за проявления вредоносной программы.

Интерфейс утилиты File Monitor представлен на рис. 1.

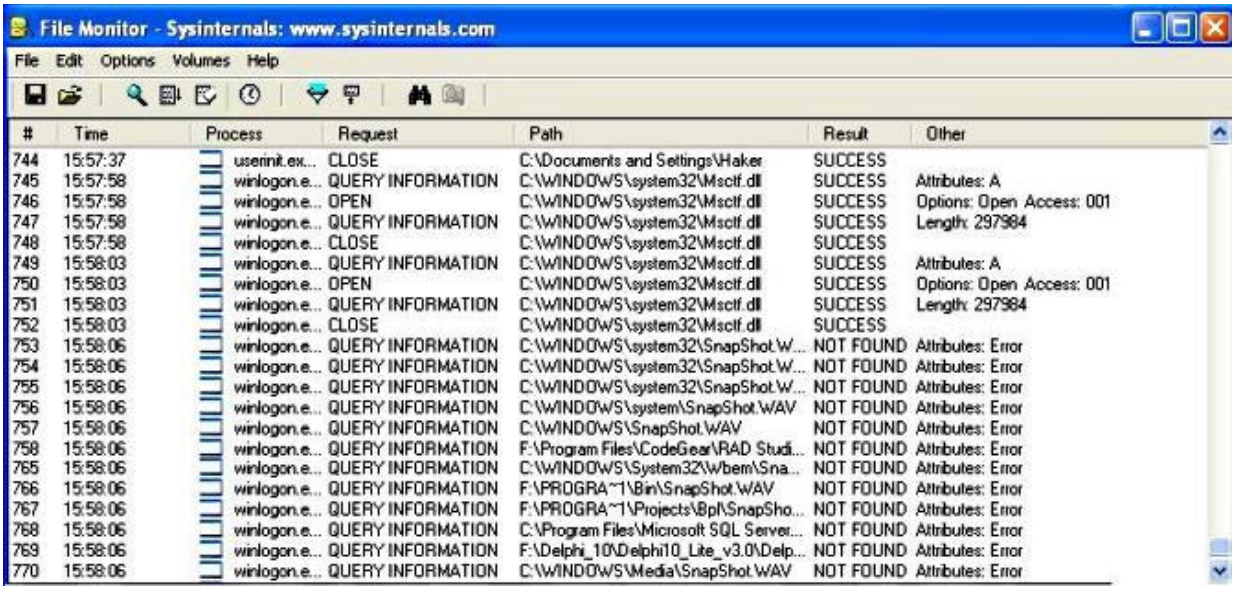

Рис. 1. **Утилита File Monitor**

Утилита File Monitor позволяет осуществлять мониторинг всех файловых операций в реальном времени. Она распространяется бесплатно, не требует инсталляции, имеет сравнительно небольшой размер (150 Кбайт) и может функционировать в операционной системе Windows 2000, XP, 2003 и более поздних. Кроме файловых операций утилита позволяет осуществлять мониторинг сетевых операций и производить настраиваемую фильтрацию регистрируемых событий.

Утилита Registry Monitor

Данная утилита позволяет осуществлять мониторинг всех операций с реестром в реальном времени. Она распространяется бесплатно. Принцип работы программы основан на перехвате функций ядра операционной системы путем правки адресов в таблице KiSST (Kernel interface Service System Table).

Возможности утилиты мониторинга операций с реестром следующие.

Двойной щелчок мышью на строке протокола приводит к открытию редактора реестра и автоматическому позиционированию на соответствующий ключ реестра, что удобно для детального анализа. Протоколы утилиты могут быть сохранены в текстовом файле.

Интерфейс утилиты Registry Monitor представлен на рис. 2.

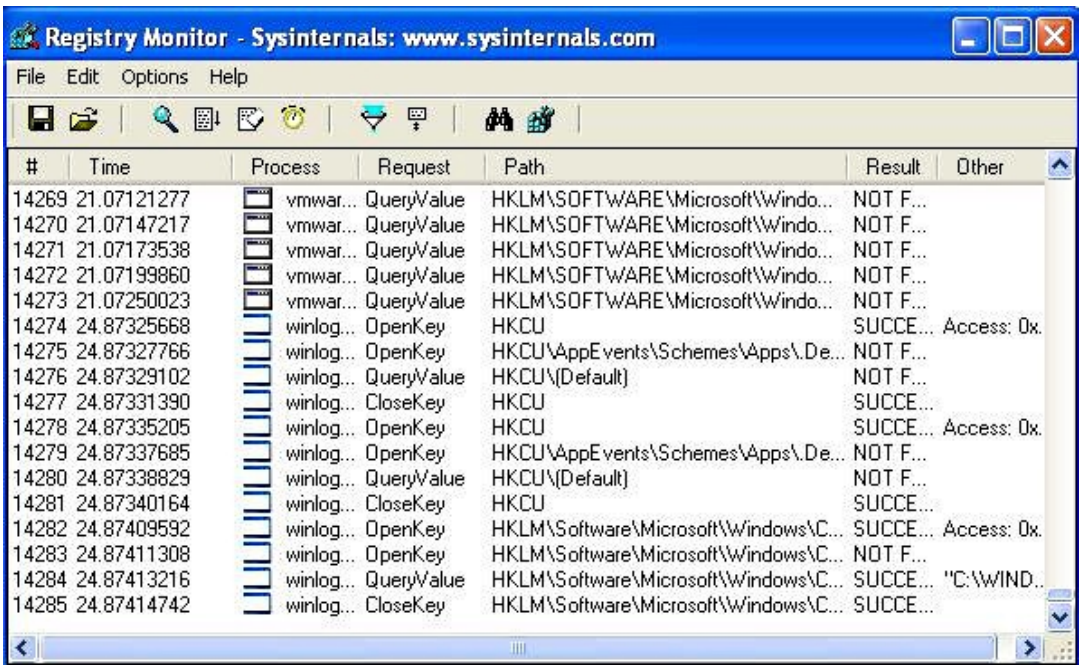

Рис. 2. **Утилита Registry Monitor**

Утилита TCP View

Данная утилита позволяет отображать список прослушиваемых портов TCP (Transmission Control Protocol – протокол управления гарантированной передачей данных) и UDP (User Datagram Protocol – протокол негарантированной доставки дейтаграмм), а также списка установленных соединений по протоколу TCP. Утилита не требует инсталляции и имеет размер 100 Кбайт.

Особенностью программы является привязка прослушиваемого порта или открытого соединения к использующему его процессу.

Список портов и соединений автоматически обновляется с настраиваемой скоростью, новые и удаляемые записи выделяются цветом для удобства наблюдения.

Так как утилита TCP View не имеет защиты от вредоносных руткитов, получаемые данные могут быть искажены в результате работы руткита.

Интерфейс утилиты TCP View представлен на рис. 3.

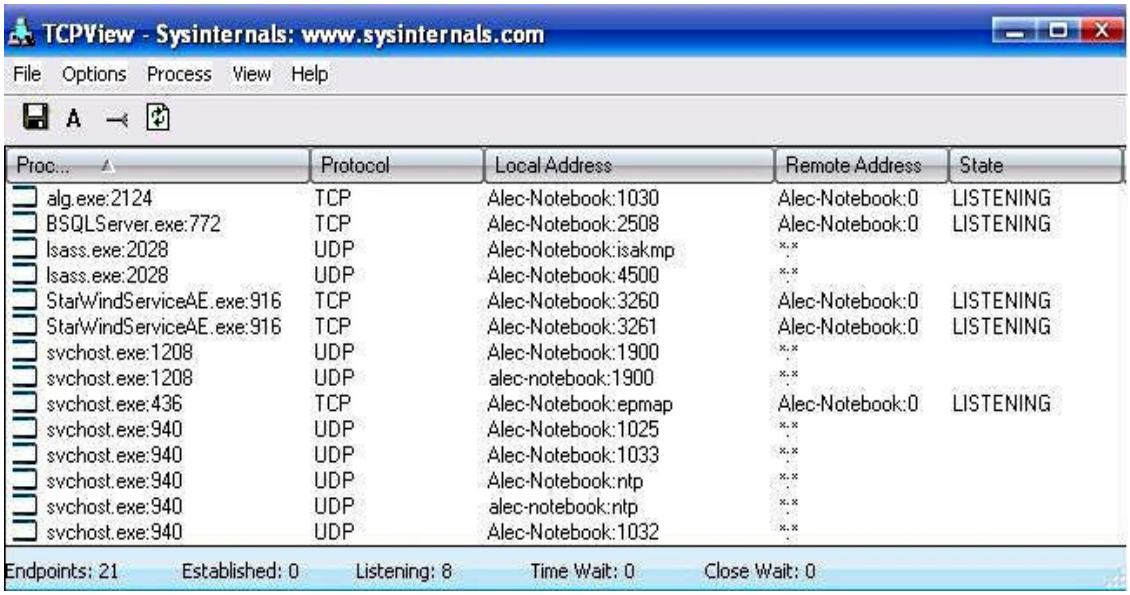

Рис. 3. **Утилита TCP View**

Утилиты для управления автозапуском

Основное назначение утилит данного класса заключается в поиске программ и библиотек, зарегистрированных в автозапуске (данные программы автоматически запускаются при загрузке операционной системы). Штатная утилита MsConfig, служащая для этих целей, анализирует небольшое количество документированных ключей автозапуска. Обычно разработчики вредоносных программ применяют неподдерживаемые утилитой MsConfig методики автозапуска.

Утилита AutoRuns

Данная утилита имеет объем 260 Кбайт, не требует инсталляции и может работать на любой версии операционной системы Windows. Утилита анализирует десятки различных методов автозапуска, в том числе классические, расширения проводника разных видов, задания планировщика, службы и драйверы, библиотеки печати, провайдеры, различные расширения и т.п.

Интерфейс утилиты AutoRuns представлен на рис. 4.

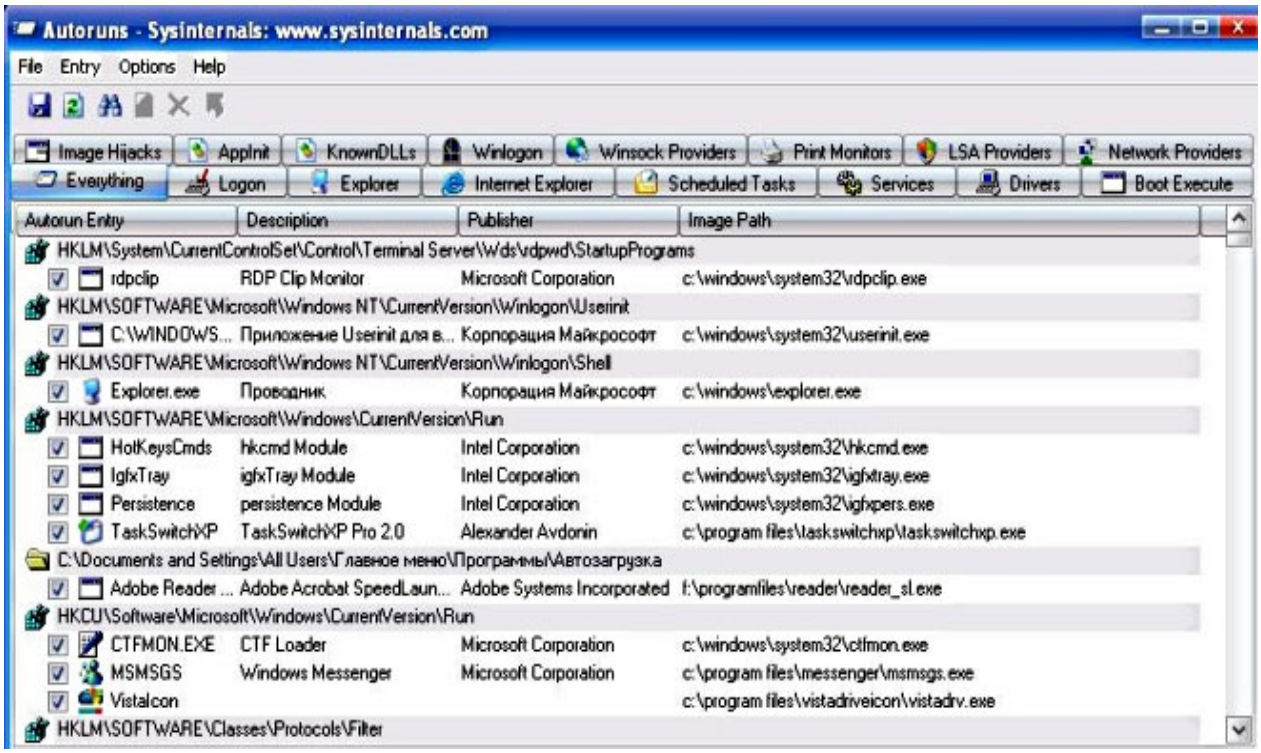

Рис. 4. **Утилита AutoRuns**

Двойной щелчок мышью на любом элементе автозапуска приводит к открытию редактора реестра и автоматическому позиционированию на соответствующий ключ и параметр, соответствующий элементу автозапуска.

Необходимо отметить, что многие вредоносные программы успешно защищаются от удаления из автозапуска с помощью периодической проверки и пересоздания ключей реестра.

Утилиты – диспетчеры процессов

Стандартный системный диспетчер процессов операционной системы Windows отображает минимум информации о запущенных процессах и чаще всего становится объектом атаки со стороны вредоносных программ.

Утилита Process Explorer имеет размер 1300 Кбайт (размер дистрибутива 640 Кбайт), распространяется бесплатно, не требует инсталляции и может замещать стандартный системный диспетчер процессов.

Интерфейс утилиты Process Explorer представлен на рис. 5.

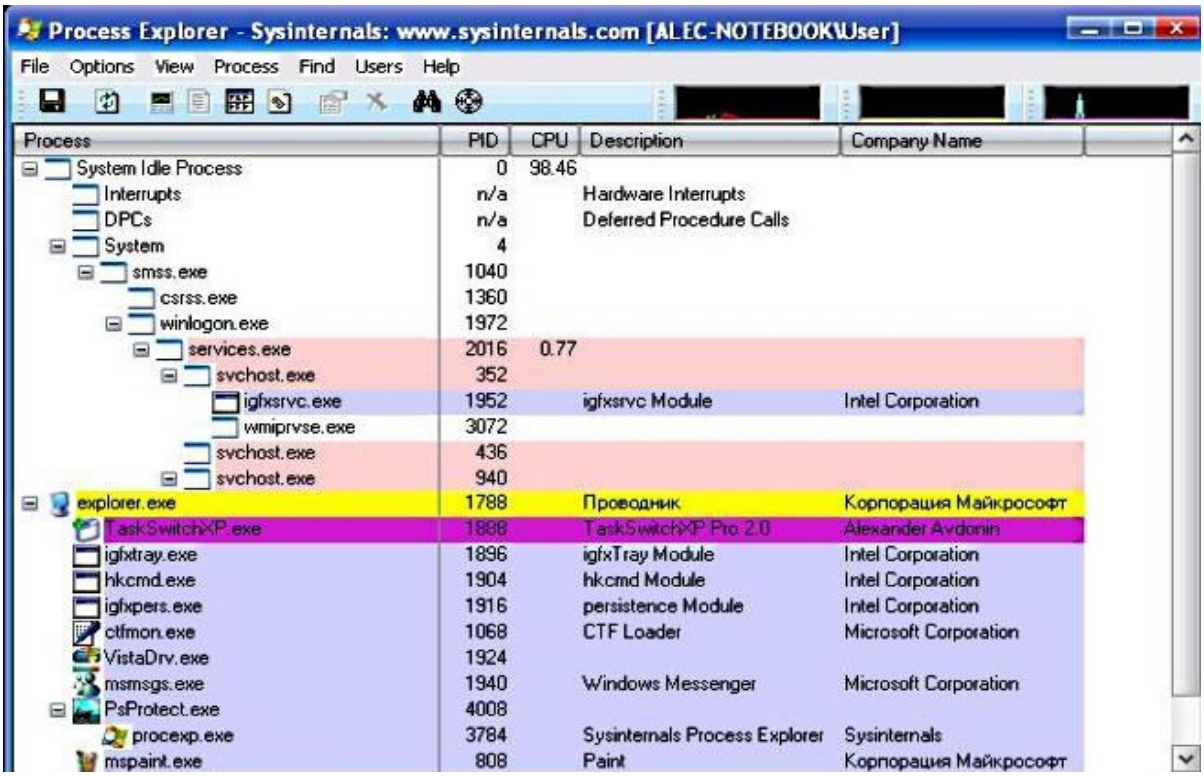

Рис. 5. **Утилита Process Explorer**

В верхней части окна программы отображается обновляемый древовидный список процессов, в нижней части окна отображается список загруженных библиотек текущего процесса. Для каждого запущенного процесса может быть вызвано окно свойств с дополнительной информацией о запущенном процессе и исполняемом файле.

Окно программы имеет несколько вкладок:

Вкладка **Image** – сведения об исполняемом файле и текущем каталоге.

Вкладка **Performance** – счетчики производительности и информация об использовании памяти, а также графики производительности процесса.

Вкладка **Threads** – информация о потоках (таблица потоков).

Вкладка **TCP/IP** – данные о TCP и UDP-портах и TCP-соединениях.

Вкладка **Security** – данные о привилегиях процесса и правах пользователей.

Вкладка **Environment** – список переменных окружения процесса и их значений.

Вкладка **Strings** – текстовые строки, найденные в файле.

Утилита Process Explorer позволяет изменить приоритет процесса, приостановить процесс и все его потоки, принудительно завершить процесс. Кроме этого, утилита Process Explorer может производить поиск библиотеки по имени, производить проверку цифровых подписей файлов и запускать процесс от имени другого пользователя.

Недостатком утилиты Process Explorer, как и других утилит, является отсутствие защиты от вредоносных программ.

Выводы

Рассмотрены утилиты для исследования операционной системы, установленной на персональном компьютере, а именно: утилита мониторинга операций, осуществляемых операционной системой с реестром; утилита регистрации операций с файловой системой; утилита фиксации активности компьютера в сети Интернет, утилита контроля запуска программ и утилита управления процессами.

Кроме рассмотренных специальных программ, для исследования компьютера могут использоваться специализированные программы, которые выполняют проверки подозрительных объектов в online режиме.

Список источников

1. Безопасность информационных систем и защита информации в МЧС России: учеб. пособие / Ю.И. Синещук [и др.]; под ред. В.С. Артамонова. СПб.: С.-Петерб. ун-т ГПС МЧС России, 2012.

2. Пальцев Д.А. Обнаружение и защита от вредоносного ПО. СПб.: БХВ-Петербург, 2016.

3. Скляров Д. Искусство защиты и взлома информации. СПб.: БХВ-Петербург, 2011.

4. Яковлев А.В., Израилов К.Е. Обзор существующих методов обнаружения дубликатов исходного кода // Национальная безопасность и стратегическое планирование. 2023. № 1 (41). С. 86–92. DOI: 10.37468/2307-1400-2023-1-86-92. EDN OLRBOK.

5. Лабинский А.Ю., Ильин А.В. Фракталы и защита информации // Природные и техногенные риски (физико-математические и прикладные аспекты). 2016. № 1 (17). С. 82–86. EDN WKBIDP.

6. Лабинский А.Ю., Толстов А.П. Нейронные сети и защита информации // Проблемы управления рисками в техносфере. 2019. № 1 (49). С. 68–73. EDN EKGDPM.

7. Лабинский А.Ю. Организация защиты информации в операционной системе Linux // Природные и техногенные риски (физико-математические и прикладные аспекты). 2021. № 1 (37). С. 4–9. EDN UVURYZ.

8. Andress J. The Basics of Information Security. Syngpress, 2014.

9. Stewart J.M. Certified Information Systems Security Study Guide. Canada: John Wiley & Sons Inc., 2015.

10. Ramzan Z. Handbook of Information Security. Springer Science, 2017.

References

1. Bezopasnost' informacionnyh sistem i zashchita informacii v MCHS Rossii: ucheb. posobie / Yu.I. Sineshchuk [i dr.]; pod red. V.S. Artamonova. SPb.: S.-Peterb. un-t GPS MCHS Rossii, 2012.

2. Pal'cev D.A. Obnaruzhenie i zashchita ot vredonosnogo PO. SPb.: BHV-Peterburg, 2016.

3. Sklyarov D. Iskusstvo zashchity i vzloma informacii. SPb.: BHV-Peterburg, 2011.

4. Yakovlev A.V., Izrailov K.E. Obzor sushchestvuyushchih metodov obnaruzheniya dublikatov iskhodnogo koda // Nacional'naya bezopasnost' i strategicheskoe planirovanie. 2023. № 1 (41). S. 86–92. DOI: 10.37468/2307-1400-2023-1-86-92. EDN OLRBOK.

5. Labinskij A.Yu., Il'in A.V. Fraktaly i zashchita informacii // Prirodnye i tekhnogennye riski (fiziko-matematicheskie i prikladnye aspekty). 2016. № 1 (17). S. 82–86. EDN WKBIDP.

6. Labinskij A.Yu., Tolstov A.P. Nejronnye seti i zashchita informacii // Problemy upravleniya riskami v tekhnosfere. 2019. № 1 (49). S. 68–73. EDN EKGDPM.

7. Labinskij A.Yu. Organizaciya zashchity informacii v operacionnoj sisteme Linux // Prirodnye i tekhnogennye riski (fiziko-matematicheskie i prikladnye aspekty). 2021. № 1 (37). S. 4–9. EDN UVURYZ.

8. Andress J. The Basics of Information Security. Syngpress, 2014.

9. Stewart J.M. Certified Information Systems Security Study Guide. Canada: John Wiley & Sons Inc., 2015.

10. Ramzan Z. Handbook of Information Security. Springer Science, 2017.

Информация о статье:
Поступила в редакцию: 18.01.2024
Принята к публикации: 10.02.2024
The information about article:
Article was received by the editorial office: 18.01.2024
Accepted for publication: 10.02.2024

Информация об авторах:
Лабинский Александр Юрьевич, доцент кафедры прикладной математики и информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), кандидат технических наук, доцент, e-mail: labynsciy@yandex.ru, https://orcid.org/0000-0001-2735-4189, SPIN-код: 8338-4230
Information about the authors:
Labinsky Alexander Yu., associate professor of the department of applied mathematics and information technologies of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), candidate of technical sciences, associate professor, e-mail: labynsciy@yandex.ru, https://orcid.org/0000-0001-2735-4189, SPIN: 8338-4230