Научная статья
УДК 681.3; DOI: 10.61260/2307-7476-2023-3-56-64

ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ ВРЕДОНОСНЫХ ПРОГРАММ, ИСПОЛЬЗУЮЩИХ ROOTKIT-ТЕХНОЛОГИИ

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

Аннотация. Рассмотрены особенности защиты информации на персональных компьютерах. Представлены классификационные признаки, и дана классификация вредоносных программ по методике заражения и наносимому ущербу. Приведены основные разновидности вредоносных программ. Рассмотрены шпионское программное обеспечение, троянские программы, сетевые и почтовые черви, программы загрузки спама и программы скрытой загрузки программного обеспечения.

Рассмотрены принципы работы вредоносных программ, использующих технологии RootKit, а также клавиатурные шпионы и технологии слежения за пользователем. Основное внимание уделено технологии RootKit. Рассмотрены разновидности технологий RootKit, работающих в режиме пользователя, в режиме ядра и в режиме как ядра, так и пользователя. Подробно рассмотрены особенности работы технологии RootKit в пользовательском режиме и в режиме ядра операционной системы.

Подробно рассмотрены методы перехвата системных функций динамических библиотек операционной системы Windows. Представлены таблицы системных функций, перехватываемых вредоносными программами.

Ключевые слова: вредоносная программа, классификация вредоносных программ, разновидности вредоносных программ, принципы работы вредоносных программ, технология RootKit, разновидности технологии RootKit, пользовательский режим, режим ядра операционной системы

Для цитирования: Лабинский А.Ю. Особенности защиты информации от вредоносных программ, использующих RootKit-технологии // Природные и техногенные риски (физико-математические и прикладные аспекты). 2023. № 3 (47). С. 56–64. DOI: 10.61260/2307-7476-2023-3-56-64.

Scientific article

THE SPECIAL FEATURE OF INFORMATION PROTECTION FROM MALWARE USING ROOTKIT TECHNOLOGIES

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

Abstract. The article considers the features of information protection on personal computers. The classification features are presented and the classification of malicious programs on the methodology of infection and damage is given. The main types of malware are given. Spyware, trojan programs, network and mail worms, spam downloaders and hidden software downloads were considered.

The article considers the principles of malware using RootKit technologies, as well as keyloggers and user tracking technologies.

The focus is on RootKit technology. Varieties of RootKit technologies operating in user mode, in kernel mode and in both kernel and user mode are considered. Features of RootKit technology in user mode and in kernel mode of operating system are considered in detail.

The methods of capturing system functions of dynamic Windows libraries are considered in detail. Tables of system functions intercepted by malware are presented.

Keywords: malware, malware classification, malware varieties, malware operating principles, RootKit technology, RootKit technology varieties, user mode, operating system kernel mode

For citation: Labinskiy A.Yu. The special feature of information protection from malware using RootKit technologies // Prirodnye i tekhnogennye riski (fiziko-matematicheskie i prikladnye aspekty) = Natural and man-made risks (physico-mathematical and applied aspects). 2023. № 3 (47). P. 56–64. DOI: 10.61260/2307-7476-2023-3-56-64.

Введение

Процессы управления различными подразделениями МЧС России и обработки значительных объемов информации подразумевают использование большого количества персональных компьютеров (ПК). В этих условиях особую важность приобретают вопросы защиты информации [1–3]. Вопросам обеспечения защиты информации уделяется большое внимание [4–6].

В настоящее время известно множество методик классификации вредоносных программ [7–9]. В качестве классификационных признаков обычно используются следующие признаки [10–11]:

– методика заражения персонального компьютера;

– ущерб, наносимый в результате деятельности вредоносной программы;

– технические признаки (например, платформа функционирования: Windows, Linux, Mac OS, Java и т.п.).

Исследования в данной статье посвящены выявлению особенностей защиты информации на ПК с точки зрения возможных угроз со стороны вредоносного программного обеспечения (ПО). Для этого необходимо дать классификацию вредоносных программ, рассмотреть основные их разновидности и представить подробное описание технологии работы вредоносных программ, включая Rootkit-технологии, работающие в двух режимах работы операционной системы (ОС): в режиме пользователя (UserMode) и в режиме ядра (KernerMode). Тема статьи актуальна, так как важность решения вопросов защиты информации в настоящее время не вызывает сомнений.

Новизна исследования заключается в подробном рассмотрении принципов работы Rootkit-технологии в режиме пользователя и в режиме ядра, включая методики и схемы перехвата системных функций в динамических библиотеках операционной системы и таблицы системных функций, перехватываемых UserMode-руткитами и KernerMode-руткитами.

Классификация вредоносных программ

По методике заражения можно выделить следующие категории:

Компьютерные вирусы – вредоносные программы, обладающие способностью заражения других программ (заражение – внедрение машинного кода вируса в тело программы и модификация программы так, что машинный код вируса получает управление в момент запуска программы или в процессе ее работы). Лечение компьютера сводится к удалению кода вируса из тела программы и восстановление её работоспособности.

Сетевые и почтовые черви – вредоносные программы, заражающие другие приложения и имеющие механизм рассылки своих копий на другие компьютеры. Лечение компьютера сводится к поиску компонентов червя на жестком диске и их удалению.

Троянские программы не могут заражать другие программы и рассылать свои копии, но могут передавать конфиденциальные данные злоумышленнику, уничтожать информацию и нарушать работу других программ. Лечение компьютера сводится к удалению файлов троянской программы.

Шпионские программы и программы рассылки спама (AdWare и SpyWare программы) аналогичны троянским программам, но не наносят видимого вреда. Такие программы могут следить за работой пользователя и передавать конфиденциальные данные на другой компьютер. Наличие таких программ замедляет работу компьютера, происходит чрезмерный расход интернет-трафика. Лечение компьютера сводится к удалению файлов этих программ.

Следует отметить, что массу вредоносных программ можно отнести сразу к нескольким категориям одновременно.

По наносимому ущербу можно выделить следующие категории:

Безопасные – не причиняют видимого ущерба ОС и данным пользователя (некоторые шпионские программы и программы рассылки спама).

Программы, уничтожающие и повреждающие данные, – компьютерные вирусы и троянские программы.

Программы, собирающие и передающие третьим лицам конфиденциальную информацию, – обычно это троянские программы, собирающие пароли пользователя.

Программы, организующие брешь в безопасности компьютера, – хакерские и троянские программы, выполняющие создание посторонних учетных записей, что позволяет злоумышленнику получить доступ к компьютеру пользователя.

Программы, нейтрализующие или повреждающие программное обеспечение, предназначенное для защиты компьютера.

Многие из вредоносных программ можно отнести к нескольким категориям одновременно.

Основные разновидности вредоносных программ

Шпионские (SpyWare) программы – ПО, собирающее и передающее кому-либо информацию о пользователе, включая персональные данные, конфигурацию компьютера и операционной системы, статистику работы в сети Интернет.

Шпионское ПО может попасть на ПК пользователя двумя основными путями:

– в ходе посещения сайтов сети Интернет;

– в результате установки бесплатных (условно-бесплатных) программ.

Шпионские программы обычно выполняют следующие действия:

– программа скрытно устанавливается на ПК пользователя;

– программа скрытно загружается в память в процессе загрузки ПК и использует технологии, затрудняющие ее удаление;

– программа выполняет некоторые операции без ведома пользователя, например, принимает или передает информацию с помощью сети Интернет;

– программа загружает и устанавливает свои обновления, дополнения, модули расширения и иное ПО без ведома пользователя;

– программа модифицирует системные настройки;

– программа модифицирует информацию, например, расширения для программы Outlook Express, которые при отправке письма приписывают к нему свою информацию.

Троянские программы типа Trojan и Hijacker – собирают и передают злоумышленнику конфиденциальную информацию о пользователе, перенастраивают параметры браузера, электронной почты или других приложений без разрешения пользователя.

Программы и модули загрузки спама (AdWare) – загрузка на ПК пользователя информации рекламного характера. Существуют две категории таких программ:

– программы, распространяемые по лицензии (воспроизведение рекламы является неявной оплатой за использование программы);

– программы, маскирующие свое присутствие и затрудняющие свое удаление.

Программы скрытной несанкционированной загрузки ПО (Trojan-Downloader) – загрузка ПО с хакерских сайтов сети Интернет. Применяется в основном для загрузки вирусов, троянских и шпионских программ. Все программы данной категории можно условно разделить на два типа:

– универсальные загрузчики, способные загружать любое ПО с любого сервера;

– специализированные загрузчики, загружающие строго определенные троянские и шпионские программы.

Принципы работы вредоносных программ

В настоящее время существует три наиболее распространенных технологии работы вредоносных программ:

– технология RootKit, используемая для защиты вредоносных программ от обнаружения и удаления, а также для шпионажа за пользователем;

– клавиатурные шпионы и сопутствующие им технологии скрытого слежения за пользователем;

– прочие технологии, включая методики защиты программ от удаления, программы Trojan-Downloader и Trojan-Dropper, методики обхода Firewall и слежения за сетевой активностью.

Термин RootKit пришел из ОС Unix, где root – пользователь с наивысшими полномочиями, kit – набор инструментов, rutkit – набор программ для контроля над компьютером. RootKit – это не шпион и не вирус, он не размножается. Главным компонентом rutkit являются программы, скрывающие присутствие на компьютере постороннего кода. В ОС Windows под Rootkit подразумевают программу, которая внедряется в ОС и перехватывает системные функции или производит замену системных библиотек. Перехват и модификация API-функций (API – Application Programm Interface – интерфейс прикладных программ) позволяет решить несколько задач:

– маскировка присутствия руткита в ОС путем маскировки запущенных процессов, открытых портов, ключей реестра и файлов на диске;

– защита от обнаружения и удаления антивирусными программами, предназначенными для исследования ОС, путем блокировки модификации ключей реестра, защита файлов от открытия на чтение и удаление;

– слежение за действиями пользователя.

Условно Rootkit-технологии можно разделить на три разновидности:

– работающие в режиме пользователя (UserMode) и основанные на перехвате функций библиотек пользовательского режима работы ОС;

– работающие в режиме ядра (KernerMode) и основанные на перехвате функций ядра ОС или установке драйвера-фильтра;

– работающие как в режиме пользователя, так и в режиме ядра.

Пример работы Rootkit-технологии, работающей как в режиме пользователя (UserMode), так и в режиме ядра (KernerMode), – перехватчик функций библиотек, работающий в режиме ядра (KernerMode), который реагирует на запуск процесса или загрузку библиотеки и производит её модификацию или установку в режиме пользователя (UserMode).

Сама технология вмешательства в работу функций библиотек может применяться для решения полезных задач, например, для мониторинга операционной системы, решения задач отладки программ и профилирования, обеспечения безопасности и ряда других задач.

Рассмотрим принципы работы UserMode Rootkit (пользовательский режим). Функции ОС Windows размещены в системных библиотеках, находящихся в файлах динамических библиотек Kernel32.dll и Ntdll.dll.

Схема вызова функции динамической библиотеки представлена на рис. 1.

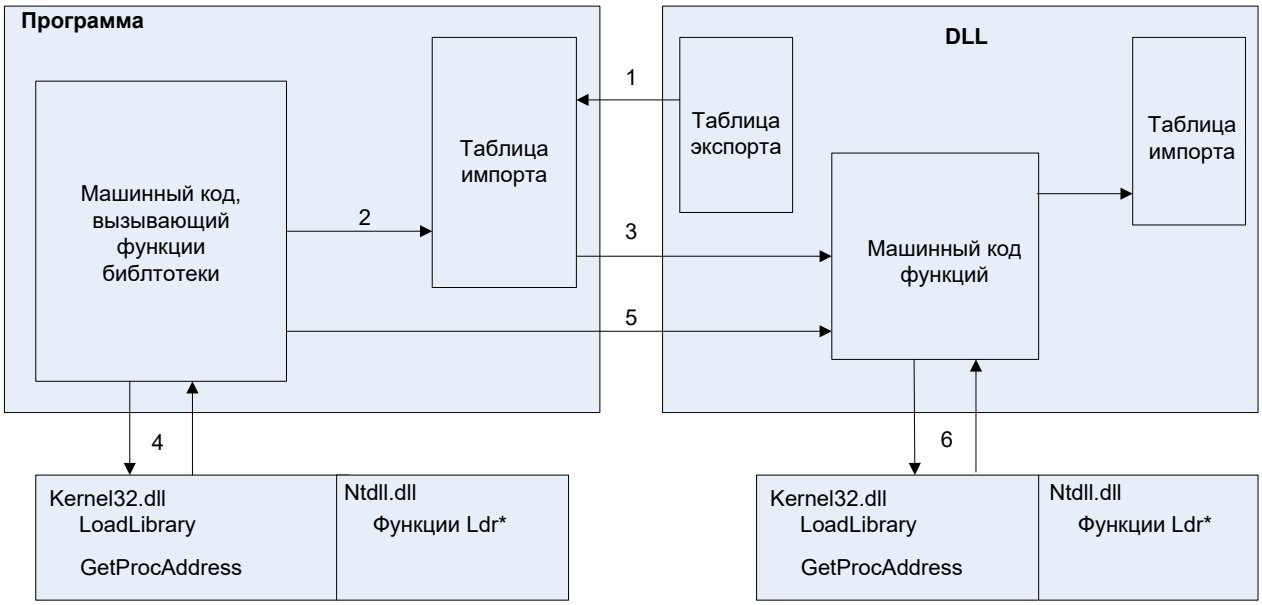

Рис.1. **Схема вызова функции динамической библиотеки**

Сначала вызывающая программа заполняет таблицу импорта. Затем определяются адреса нужных функций в библиотеке *.DLL. Далее производится вызов нужной функции из библиотеки.

Существует два способа вызова системных функций:

– раннее связывание (статически импортируемые функции), вызов до начала работы программы;

– позднее связывание (динамически импортируемые функции), вызов во время работы программы.

Рассмотрим принципы работы KernelMode Rootkit (режим ядра ОС). В этом режиме вредоносная программа может получить контроль над всей ОС компьютера, вызов системных функций производится следующими способами:

– с помощью редактирования адресов функций в таблице KiSST (Kernel interface Service System Table);

– с помощью модификации машинного кода ядра ОС;

– путем установки в ОС драйвера-фильтра, подменяющего адреса функций;

– путем создания собственной таблицы KiSST.

Существует несколько методик перехвата системных функций:

– перехват модификацией машинного кода программы, вызывающего функцию (схема перехвата модификацией кода представлена на рис. 2);

– перехват подменой адресов функций (схема перехвата подменой адреса функции представлена на рис. 3).

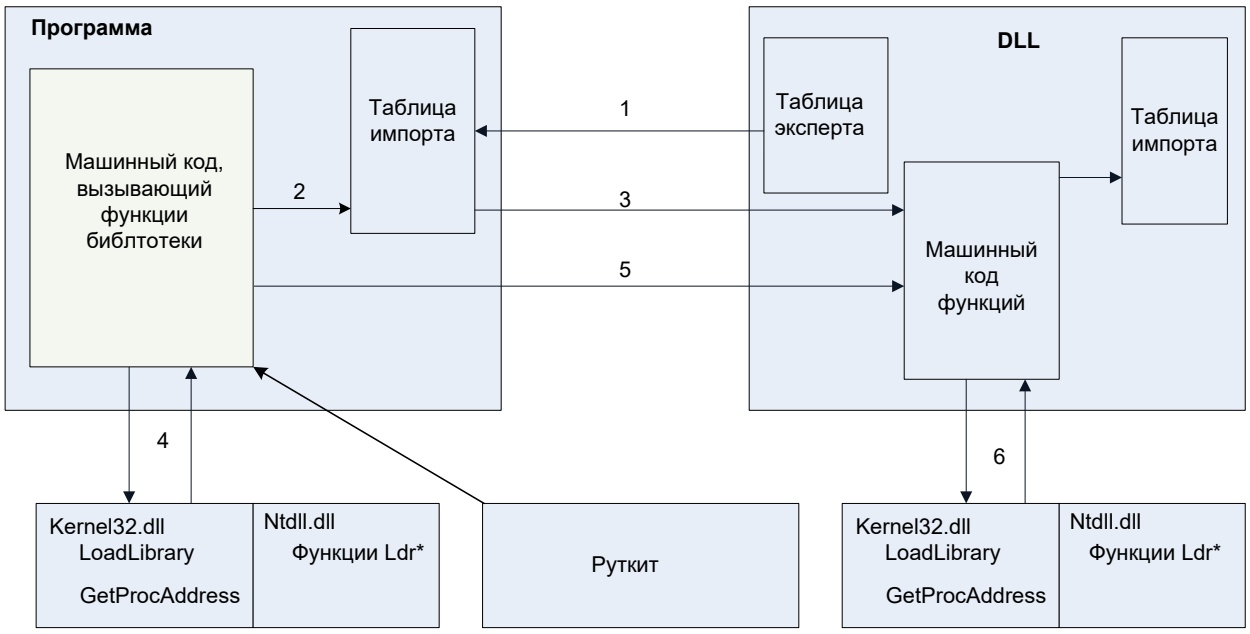

Рис. 2. **Схема перехвата модификацией машинного кода программы**

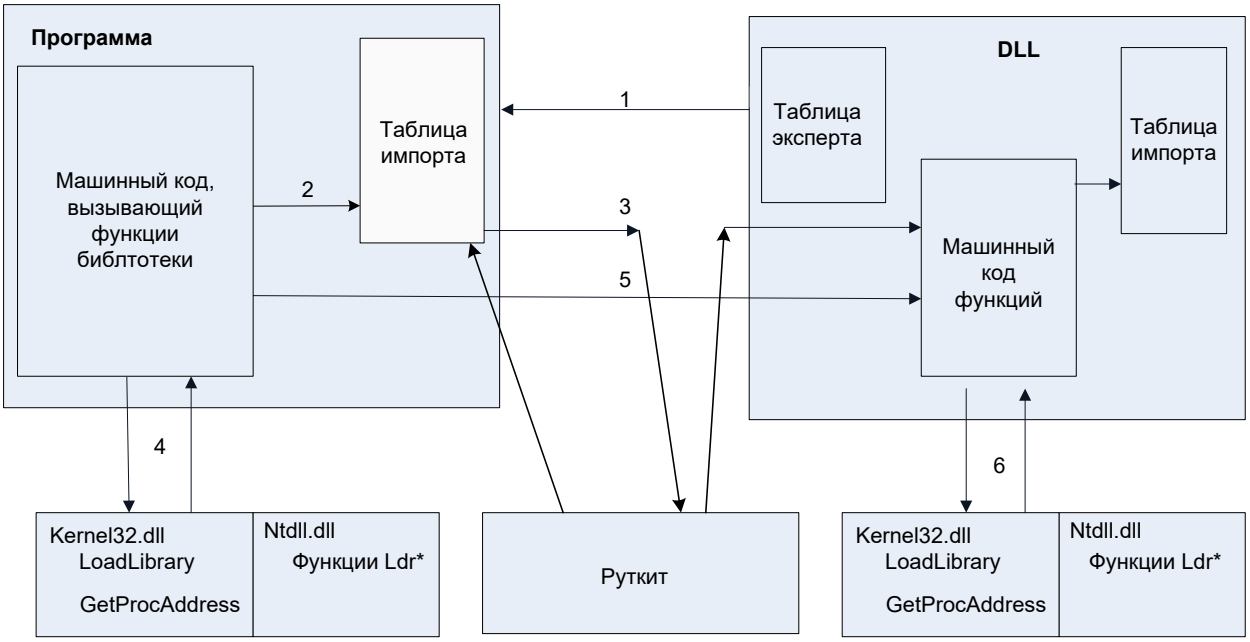

Рис. 3. **Схема перехвата подменой адреса функции**

Чаще всего UserMode-руткитами перехватываются системные функции, представленные в табл. 1.

Таблица 1

Функция	Библиотека	Назначение
LoadLibrary	Kernel32.dll	Отслеживание загрузки библиотек
GetProcAdress	Kernel32.dll	Подмена адресов функции
NtEnumerateKey NtEnumerateValueKey	Ntdll.dll	Маскировка ключей и значений реестра
RegEnumKey RegEnumKeyEx	Advapi32.dll	Маскировка ключей и значений реестра

Функция	Библиотека	Назначение
NtOpenProcess NtOpenThread	Ntdll.dll	Защита процессов и потоков от анализа и остановки
Process32Next	Kernel32.dll	Маскировка процессов
NtQueryDirectoryFile NtQueryVolumeInformationFile NtOpenFile; NtCreateFile	Ntdll.dll	Маскировка файлов и каталогов. Блокировка доступа к файлам
FindNextFile	Kernel32.dll	Маскировка файлов и каталогов
NtQuerySysyemInformation RtlGetNativeSystemInfornation	Ntdll.dll	Искажение системной информации
EnumServiceGroupW EnumServiceStatusA EnumServiceStatusEx	Advapi32.dll	Маскировка служб, блокировка их запуска и остановки
NtReadVirtualMemory NtWriteVirtualMemory	Ntdll.dll	Перехват операции чтения памяти процесса
HttpSendRequest InternetConnect	Wininet.dll	Шпионаж за обменом с сетью Интернет

В режиме KernelMode вредоносная программа может осуществлять мониторинг загрузки исполняемых файлов и производить маскировку файлов и папок файловой системы. Чаще всего KernelMode-руткитами перехватываются системные функции, представленные в табл. 2.

Таблица 2

ZwCreateKey ZwOpenKey	Операции с реестром: блокировка создания и открытия ключей
ZwSetValueKey ZwDeleteValueKey	Операции с реестром: блокировка модификации и удаления параметров реестра
ZwEnumerateKey ZwEnumerateValueKey	Операции с реестром: маскировка ключей и параметров реестра
ZwCreateFile; ZwOpenFile ZwCreateDirectoryObject ZwOpenDirectoryObject	Блокировка доступа к файлам и каталогам по заданным условиям
ZwOpenProcess	Блокировка открытия заданных процессов
ZwQuerySystemInformation	Искажение системной информации
ZwQueryInformationFile ZwQueryDirectoryFile ZwQueryDirectoryObject	Маскировка файлов, искажение информации о файлах и каталогах

Вмешательство в работу компьютера может осуществляться без перехвата системных функций с использованием технологии DKOM (Direct Kernel Object Manipulation) – путем маскировки процессов и драйверов, а также с помощью изменения уровней привилегий процессов. Такое вмешательство, в отличие от перехвата функций, сложнее обнаружить.

Выводы

Применяемые разработчиками вредоносных программ технологии постоянно развиваются и прогрессируют [12]. Поэтому при «лечении» компьютера следует использовать специальные программы-антивирусы и пользоваться специализированными Интернет-ресурсами (virusinfo.com, viruslist.ru, virustotal.com, virusscan.org и т.д.).

Опытным пользователям рекомендуется периодически пользоваться утилитами мониторинга ОС, выполняющими следующие функции:

– мониторинг операций с файлами (например, утилита FileMon);

– мониторинг операций с реестром (например, утилита RegMon);

– мониторинг сетевой активности (например, утилита TDI Mon);

– мониторинг запуска процессов (например, утилита Process Explorer);

– мониторинг программ и библиотек, зарегистрированных в автозапуске при загрузке ОС (например, утилита AutoRuns).

При этом нужно учитывать, что вредоносные программы могут обнаруживать присутствие на компьютере утилит мониторинга ОС.

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. Буйневич М.В., Матвеев А.В., Смирнов А.С. Актуальные проблемы подготовки специалистов в области информационной безопасности МЧС России и конструктивные подходы к их решению // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2022. № 3. С. 1–17. EDN OGPXZX.

4. Фленов М. Компьютер глазами хакера. СПб.: БХВ-Петербург, 2010.

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. Распознавание компьютерных вредоносных программ с использованием нейронных сетей // Природные и техногенные риски (физико-математические и прикладные аспекты). 2017. № 3 (23). С. 10–15. EDN ZUFYPF.

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

8. Лабинский А.Ю. Организация защиты информации в операционной системе Linux // Природные и техногенные риски (физико-математические и прикладные аспекты). 2021. № 1 (37). С. 4–8. EDN UVURYZ.

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

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

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

12. Метельков А.Н. О криптографических мерах защиты информации при внедрении информационных технологий в решение задач управления в социальных и экономических системах // Национальная безопасность и стратегическое планирование. 2020. № 4 (32). С. 68–78. DOI: 10.37468/2307-1400-2021-2020-4-68-78. EDN XZNNXX.

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. Bujnevich M.V., Matveev A.V., Smirnov A.S. Aktual'nye problemy podgotovki specialistov v oblasti informacionnoj bezopasnosti MCHS Rossii i konstruktivnye podhody k ih resheniyu // Nauch.-analit. zhurn. «Vestnik S.-Peterb. un-ta GPS MCHS Rossii». 2022. № 3. S. 1–17. EDN OGPXZX.

4. Flenov M. Komp'yuter glazami hakera. SPb.: BHV-Peterburg, 2010.

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. Raspoznavanie komp'yuternyh vredonosnyh programm s ispol'zovaniem nejronnyh setej // Prirodnye i tekhnogennye riski (fiziko-matematicheskie i prikladnye aspekty). 2017. № 3 (23). S. 10–15. EDN ZUFYPF.

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

8. Labinskij A.Yu. Organizaciya zashchity informacii v operacionnoj sisteme Linux // Prirodnye i tekhnogennye riski (fiziko-matematicheskie i prikladnye aspekty). 2021. № 1 (37). S. 4–8. EDN UVURYZ.

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

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

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

12. Metel'kov A.N. O kriptograficheskih merah zashchity informacii pri vnedrenii informacionnyh tekhnologij v reshenie zadach upravleniya v social'nyh i ekonomicheskih sistemah // Nacional'naya bezopasnost' i strategicheskoe planirovanie. 2020. № 4 (32). S. 68–78. DOI: 10.37468/2307-1400-2021-2020-4-68-78. EDN XZNNXX.

Информация о статье:
Поступила в редакцию: 04.08.2023
Принята к публикации: 22.09.2023
The information about article:
Article was received by the editorial office: 04.08.2023
Accepted for publication: 22.09.2023

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