3. Tyazhev A.I. *Optimization of digital detectors in receivers at a minimum of computing costs*. Samara: PIIRS Publishing House, 1994, 256 p. (In Russian.)
4. Tyazhev A.I., Mishin D.V. Comparative evaluation of computing costs in the implementation of OFDM digital modems based on KSG and FFT. *Prilozhenie k zhurnalu «Infokommunikacionnye tehnologii»*, 2011, no. 8, pp. 32–38. (In Russian.)
5. Widrow B., Stearns S. *Adaptive signal processing*. Moscow: Radio i svyaz', 1989. 440 p. (In Russian).
6. Sergienko A.B. *Digital signal processing*. Saint Petersburg: Piter, 2006, 751 p. (In Russian.)
7. Karjakin V.L. *Digital TV*: textbook for universities. Moscow: Solon – Press, 2013, 448 p. (In Russian.)
8. Mishin D.V., Tyazhev A.I. Digital simulation of a multipath communication channel. *Infokommunikacionnye tehnologii*, 2019, vol. 17, no. 4, pp. 368–373. DOI: 10.18469/ikt.2019.17.4.02. (In Russian.)
9. Ivanova V.G., Tyazhev A.I. *Digital Signal Processing and Signal Processors*. Ed. by A.I. Tyazheva. Samara: OFORT, 2008, 264 p. (In Russian.)
10. *Other Radio Receivers*. Textbook for high schools. Ed. by N.N. Fomina. Moscow: Goryachaya liniya – Telekom, 2007, 516 p. (In Russian.)

Received 17.03.2020

ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 004.725.5

ОСОБЕННОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ FLASH-НАКОПИТЕЛЕЙ

Василенко К.А.[1], Золкин А.Л.[2], Абрамов Н.В.[3], Курганов Д.О.[3]
[1] Владивостокский государственный институт экономики и сервиса, Владивосток, РФ
[2] Волжский государственный университет водного транспорта (Самарский филиал), Самара, РФ
[3] Дальневосточный федеральный университет, Владивосток, РФ
E-mail: k2857@mail.ru, alzolkin@list.ru, nikolay.abramov1990@mail.ru, kurganov_vl@mail.ru

Рассматриваются угрозы информационной безопасности flash-накопителей, проведен анализ файловых систем FAT32 и NTFS flash-накопителей и их уязвимостей перед вредоносными программами; выделены особенности алгоритма действия вирусов на flash-накопителях. Вопрос безопасности flash-накопителей все еще остается весьма открытым. Существует достаточно много действенных способов, позволяющих существенно снизить возможность заражения flash-накопителей. Проведя анализ недостатков системы NTFS, стоит отменить, что для данной системы необходим гораздо больший объем оперативной памяти по сравнению с системой FAT32, фрагментация данных также затрудняет работу системы с каталогами файлов средних размеров. Кроме того, по сравнению с системой FAT32, система NTFS имеет относительно низкую скорость производительности. Если flash-накопитель используется чаще на домашнем компьютере, то в качестве рабочего выбирается именно домашний компьютер и ему предоставляется полный доступ. Для всех остальных устанавливается запрет на запись. На сегодняшний день существует множество способов и методов защиты flash-накопителей, но специфика их применения зависит от расположения хранилища информации и ее ценности.

Ключевые слова: *информационная безопасность, flash-накопители, рабочая станция, вирус, информация, файловые системы, компьютер*

Введение

По статистике на сегодняшний день основным «рассадником» вирусов является Internet, а второе место прочно удерживают съемные запоминающие устройства. И лидируют среди них с большим отрывом флеш-накопители (USB, «флешки»), обладающие возможностью многократной перезаписи и пополнения файлов без каких-либо дополнительных усилий. Кроме того, флешки имеют больший объем памяти, по сравнению с известными ранее и используют более

совершенные алгоритмы управления данными, поэтому они и представляют такой интерес для злоумышленников [1].

Особенности алгоритма действия вирусов на flash-накопителях

И, кроме того, иногда пользователь не может даже вспомнить, где и когда подключал flash-накопитель, чтобы скачать ту или иную картинку или программу. Однако, когда пользователь компьютера вставляет в системный блок данного устройства flash-накопитель, и антивирусная программа может выдавать целый список подхваченных вредоносных программ, которые нередко можно удалить только после полного форматирования накопителя.

Алгоритм действия вируса ведется по следующему пути: электронное вычислительное устройство или рабочая станция, подвергнутая заражению, эксплуатируется злоумышленником с целью хищения чужих кодов доступа и паролей к основным и сервисным службам сайта, имеющим возможность миграции, данная ситуация касается также USB-коннекторов и flash-накопителей. В данной ситуации заражение ведется последовательно от рабочей станции к подсоединенному к ней flash-накопителю [1].

Если вирусом будет обнаружена возможность присоединения к глобальной сети, то тут же им будет выполнена операция по передаче в Internet зафиксированной ранее информации с кодами доступа и паролями, в дальнейшем заражая другие элементы сетевого окружения [2]. Чтобы включить операцию по старту рассылки вируса при подключении flash-устройства, вредоносная программа производит или ведет перезапись на указанном накопителе «Аутранеров» (специальных файлов под заглавием «autorun.inf»), где ведется описание текущих приложений, которые являются соединительным звеном для старта автозагрузки при соединении носителя.

В «Аутранере» ведется описание направления к вредоносной программе, а именно к коду, который должен быть исполнен, как правило, это определенный файл («EXE»), имеющий конкретное имя [3]. Как правило, файл «Аутранер» и EXE-файл не имеют визуального отражения в оптимальных настройках операционных систем, в том числе Windows, поскольку их атрибутика имеет статусы «системный» или «скрытый».

Вопрос безопасности flash-накопителей все еще остается весьма открытым. Существует достаточно много действенных способов, позволяющих существенно снизить возможность заражения flash-накопителя.

Один из вариантов – отключить автозагрузку, так как некоторые вирусы прописываются только тогда, когда система пытается автоматически открыть съемный носитель. Отсутствие автозапуска в данном случае не активирует вирус, и он не «обоснуется» на flash-накопителе [4]. Другой еще более радикальный вариант – создание скрытых файлов с «нулевым» размером. Обычно вирусы, которые распространяются через флешки, создают скрытый файл с определенным именем, которое не вызывает у пользователя подозрений [5]. Например, *autorun.ini*, *autorun.inf*, *recycler* и т. д. И если заранее «застолбить» файлы с такими именами, то вирусу просто некуда будет прописываться, и он «отцепится» от вас.

Третий возможный вариант защиты – поставить запрет на запись в корень, а для записи файлов использовать отдельную папку (папки). Однако такой вариант напрямую возможен только для файловой системы NTFS [6]. Если недостаточно серьезно отнестись к этой проблеме, то существует риск заразить подхваченным вирусом и свой компьютер, что является куда более серьезной проблемой.

Итак, в первую очередь, для защиты собственного компьютера от вирусов, попавших на флешноситель необходимо отключить автозагрузку (автозапуск) на всех дисках, подключаемых к компьютеру.

Файловые системы FAT32 и NTFS flash-накопителей и их уязвимости перед вредоносными программами

Вторым аспектом безопасности компьютера является задача непосредственной защиты флеш-накопителя от заражения [7]. Поскольку флеш-карта – это собственно контейнер для передачи файлов с одного компьютера на другой, то с уверенностью можно сказать, что заражение флеш-носителя происходит только через уже зараженный компьютер, при передаче файлов через этот контейнер [7]. Для работы с внешними накопителями можно использовать одну из двух возможных систем: FAT32 и NTFS. Рассмотрим их более подробно.

Как известно, стандартом для флеш-накопителей является использование системы FAT32, которая ориентирована на работу с различными версиями операционных систем Windows [8; 9]. Особенностью этой системы является ограничение, накладываемое на размер файла – не более 4 Гб.

Сама по себе система FAT32 имеет невысокие требования, особенно это проявляется в необхо-

димости использования небольшого объема ОЗУ, при этом скорость работы данной системы весьма высока, как и эффективность работоспособности с файлами больших размеров [10]. Кроме того, при данной системе также невысок износ носителей информации, поскольку головки чтения-записи жесткого диска производятся в меньшем количестве.

Система FAT32 имеет также и недостатки, они проявляются в уязвимости системы безопасности от существующих сбоев, в снижении эффективности работы с файлами огромных размеров; установление пределом по объему файлов и соответствующих размеров, отсутствие нормальных скоростей обработки информации при выполнении операции фрагментации, медленная синхронизация при взаимодействии с каталогами, хранящими весомое количество информации [11].

Таким образом, высокий уровень сохранности файлов небольших размеров является наиболее подходящим для системы FAT32, это связано с тем, что в системе не имеется лишних составляющих, при этом преобладает достаточно высокая и производительная скорость обработки информации, и работы с файлами. Минимальный риск существующего износа дисков также является преимуществом указанной системы.

Описывая характеристики NTFS, стоит отметить, что достоинствами данной системы являются относительно высокая скорость доступа к информации небольшого размера, отсутствие границ и препятствий на емкость хранилища данных, отсутствие влияния фрагментации данных на файловую систему, высокая сохранность информации и структуры системы, высокие характеристики производительности при обработке информации большого размера [12].

Говоря о недостатках системы NTFS, стоит отметить, что для данной системы необходим гораздо больший объем оперативной памяти (ОЗУ) по сравнению с системой FAT32, фрагментация данных также затрудняет работу системы с каталогами файлов средних размеров. Кроме того, по сравнению с системой FAT32, система NTFS имеет относительно низкую скорость производительности.

При использовании системы NTFS, мы имеем целый ряд дополнительных возможностей, так как в рамках самой файловой системы предусмотрены параметры безопасности, то есть у нас имеется возможность просто запретить запись в корень нашей флеш-карты, создав при этом отдельную папку (или папки), куда можно записывать все данные. Сравнение файловых систем FAT32 и NTFS приведено в таблице.

Таблица. Сравнение файловых систем FAT32 и NTFS

Комментарий	FAT32	NTFS
Максимальная длина имени файла	255	255
Максимальный размер файла	4 Гбайт	Теоретический максимум 16 Эбайт
Максимальный размер тома	2 Тбайт	2 Тбайт
Совместимость с гибкими дисками	Да	Нет
Несколько дисков в одном томе	Нет	Да
Безопасность на уровне файлов и каталогов	Нет	Да
Проверка доступа на уровне файлов и каталогов	Нет	Да

Таким образом, имеется два возможных варианта: оставить носитель на родной файловой системе FAT32 или перейти на файловую систему NTFS. В первом случае необходимо использовать специфику системы FAT32. Задача следующая – запретить вирусу создавать на флешке файл *autorun.inf*. Раньше эта проблема решалась достаточно просто – нужно было создать каталог с именем *AUTORUN. INF*, выставив ему атрибуты «*Read only*» и «*Hidden*». Так мы препятствовали созданию файла с таким же именем. Современный вирус, легко может изменить права, удалить файл и записать новый.

Существует несколько более изощренный путь, который большинство вирусов обходить пока не научились. Идея здесь следующая: создаем каталог *AUTORUN.INF.* Если каталог не пустой, то удалить его можно, лишь расправившись со всем содержимым. И это очень просто, однако, в том случае, когда в каталоге имеются файлы с некорректными для FAT32 именами, задача для современных вирусов становится неразрешимой. Именно этот принцип защиты и положен в основу нашего алгоритма, программная реализация которого создает на флешке папку *AUTORUN. INF* с некорректными локальными *UNC*-путями.

UNC – это формат для записи пути к файлу, расположенному на удаленном компьютере. Он имеет вид *\\server\share\path*, где *server* – это название удаленного хоста. Такой способ доступа к файлам можно использовать и для локальной машины, в этом случае вместо *server* нужно подставлять «?» или «.», а путь к файлу указывать вместе с буквой диска [13].

Например, так: *\\?\C:\ folder\file.txt.* Идея заключается в том, что при использовании *UNC*-путей и стандартных консольных команд можно создавать файлы даже с запрещенными файловой системой именами.

Создадим несложный bat-файл, алгоритм которого создает некорректную папку *autorun.inf* и еще несколько некорректных папок в ней. Далее он создает файл конфигурации в самой папке и помещает туда свою иконку, которая будет служить идентификатором, то есть папку, которая будет выглядеть как иконка, а в файле конфигурации прописан путь к ней, со скрытыми атрибутами. С помощью данного способа мы можем знать при каждом открытии флешки, изменен ли наш файл *autorun.inf* или нет (если изменен, то это свидетельствует о заражении носителя) [14].

Недостатком этого способа является то, что хоть папку и невозможно удалить, однако ее возможно переименовать, а это дает шанс злоумышленникам записать на флешку свой *autorun*, но и это предусмотрено – если вы зашли на свою флешку и не увидели своей иконки, это означает, что на вашей флешке со 100% гарантией поселился вирус.

Следующий шаг: для защиты компьютера от уже зараженной флешки необходимо отключить автозагрузку. Самый удобный, на наш взгляд, способ делать это через реестр. По своей сути, этот способ подменяет содержимое файла *autorun.inf* значением из реестра, которое специально задается пустым/неверным. Это приводит к тому, что если на диске и прописан файл *autorun.inf*, то он воспринимается как пустой.

Кроме того, для подстраховки в ветке *autoplayhandlers* в реестре прописывается запрет автостарта всех типов файлов (за исключением автостарта, обработки двойного клика и контекстного меню). Последнее означает, что будет появляться хорошо нам известное всплывающее окно, которое предлагает открыть флешку, прослушать музыку и так далее, но никакие файлы запуститься в автоматическом режиме не смогут [15]. Другой, более кардинальный вариант – полностью забить флешку пустыми файлами и тогда напрямую на нее не удастся записать ни один байт информации.

Если нам требуется что-то записать на флешку, то это реализуется посредством обращения к специальной программе, которая автоматически запишет файл на флешку, не удалив при этом нужную нам информацию, и кроме того проверит и в случаи необходимости заполнит весь объем флешки.

Если рассматривать файловую систему NTFS, то здесь одним из способов защиты будет программная установка на запрет: изменения и запись файлов; удаления всех файлов; создания или копирования файлов или папок в корень флешки.

Заключение

Таким образом, учитывая, что flash-накопители достаточно часто используются на сторонних компьютерах, то рациональным видится следующий алгоритм: отформатировать указанный накопитель; создать папку в корне, в которой в дальнейшем будут осуществляться все операции над файлами и каталогами; запретить всем доступ в корень. Если flash-накопитель используется чаще на домашнем компьютере, то в качестве рабочего выбирается именно домашний компьютер и ему предоставляется полный доступ. Для всех остальных устанавливается запрет на запись. Кроме того, можно, комбинируя этими двумя способами, создать, например, такой flash-накопитель, для которого доступ в корень присутствует только на домашнем компьютере, а на всех остальных разрешено пользоваться папкой, созданной предварительно в корне.

Литература

1. Ильин С. Защита USB флеш-накопителей от вирусов. URL: http://www.windxp.com.ru/articles61.htm (дата обращения: 22.02.2020).
2. Уничтожение вирусов «Форум фан-клуба лаборатории Касперского». URL: http://forum.kasperskyclub.ru/index.php?showtopic=8920 (дата обращения: 22.02.2020).
3. Берёза Н.В. Современные тенденции развития мирового и российского рынка информационных услуг // Инженерный вестник Дона. 2012. № 2. URL: http://ivdon.ru/ru/magazine/archive/n2y2012/758 (дата обращения: 22.02.2020).
4. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. М.: Изд-во МГТУ им. Н.Э. Баумана, 2017. 255 с.
5. Золкин А.Л. Разработка информационно-управляющей системы для сбора, обработки и передачи данных о техническом состоянии коллекторов электродвигателей // Научно-технические аспекты инновационного развития транспортного комплекса: сб. трудов V МНПК. Донецк: ДАТ, 2019. С. 48–53.
6. Панкратов С.А. Использование графической информации для защиты программного и информационного обеспечения // Инженерный вестник Дона. 2012. № 2. URL: http://ivdon.

ru/ru/magazine/archive/n2y2012/792 (дата обращения: 22.02.2020).
7. Уилсон Э. Мониторинг и анализ сетей. Методы выявления неисправностей / пер. с англ. М.: Лори, 2016. 480 с.
8. Золкин А.Л. Разработка информационно-управляющей системы для контроля износа коллекторов тяговых электродвигателей // Вестник Донецкой академии автомобильного транспорта. 2019. Вып. 2. С. 65–74.
9. Аладышев О.С., Овсянников А.П, Шабанов Б.М. Развитие корпоративной сети Межведомственного суперкомпьютерного центра. URL: http://vbakanov.ru/metods/1441 (дата обращения: 22.02.2020).
10. Гайдук А.Р. Теория и методы аналитического синтеза систем автоматического управления: (полиномиальный подход). М.: Физматлит, 2020. 264 с.
11. Khalil H.K. Nonlinear Systems. 3rd ed. Upper Saddle River: Prentice Hall, 2016. 766 p. URL: http://en.bookfi.net/book/1417228 (дата обращения: 22.02.2020).
12. Melin P., Castillo O. Modeling, Simulation and Control of Non-linear Dynamical Systems: An Intelligent Approach Using Soft Computing and Fractal Theory. Boca Raton: Taylor & Francis, 2017. 265 p.
13. Смирнов А.В. Руководство по захвату сетевого трафика. URL: http://blog.packet-foo.com/2016/11/the-network-capture-playbook-part-3-network-cards (дата обращения: 22.02.2020).
14. Perlman R. Interconnections: Bridges & Routers. Boston: Addison-Wesley, 2016. 245 p.
15. Oggerino C. High Availability Network Fundamentals. Indianapolis: Cisco Press, 2017. 327 p.

Получено 12.03.2020

Василенко Константин Александрович, преподаватель колледжа сервиса и дизайна Владивостокского государственного университета экономики и сервиса. 690092, Российская Федерация, Приморский край, г. Владивосток, ул. Добровольского, 20. Тел. +7 964 453-06-36. E-mail: k2857@mail.ru

Золкин Александр Леонидович, к.т.н., преподаватель кафедры естественнонаучных и общепрофессиональных дисциплин Волжского государственного университета водного транспорта (Самарский филиал). 443099, Российская Федерация, г. Самара, ул. Молодогвардейская, 62-64. Тел. +7 960 825-68-49. E-mail: alzolkin@list.ru

Абрамов Николай Викторович, студент Дальневосточного федерального университета (ДВФУ). 690920, Российская Федерация, Приморский край, г. Владивосток, ул. Суханова, 8. Тел. +7 914 373-91-16. E-mail: nikolay.abramov1990@mail.ru

Курганов Даниил Олегович, студент ДВФУ. 690920, Российская Федерация, Приморский край, г. Владивосток, ул. Суханова, 8. Тел. +7 999 059-37-74. E-mail: kurganov_vl@mail.ru

FEATURES OF FLASH DRIVES INFORMATION SECURITY

Vasilenko K.A.[1], Zolkin A.L.[2], Abramov N.V.[3], Kurganov D.O.[3]
[1] Vladivostok State University of Economics and Service, Vladivostok, Russian Federation
[2] Volga State University of Water Transport (Samara branch), Samara, Russian Federation
[3] Far Eastern Federal University, Vladivostok, Russian Federation
E-mail: k2857@mail.ru, alzolkin@list.ru, nikolay.abramov1990@mail.ru, kurganov_vl@mail.ru

The article provides the review of the threats to information security of flash drives, analyzes the FAT32 and NTFS file systems of flash drives and their vulnerabilities to malware. Features of viruses' action algorithms on flash drives are highlighted in the article. The issue of flash drives security is still open. There are many effective ways to significantly reduce the possibility of infection of flash drives. After analyzing the drawbacks of the NTFS system, it shall be noted that this system requires a much larger amount of RAM compared to the FAT32 system, and that the data fragmentation also complicates the work of the system with medium size file directories. Moreover, the NTFS system has a relatively low performance rate when compared to the FAT32 system. If the flash drive is used more often with the home computer, then the home computer is chosen as the workstation and is

provided with full access. Recording shall be prohibited for other computers. Today, there are many ways and methods of flash drives protecting, but the specifics of their use depend on the information store location and information value.

Keywords: *IT security, flash drives, workstation, virus, information, file systems, computer*

DOI: 10.18469/ikt.2020.18.2.11

Vasilenko Konstantin Alexandrovich, Service and design college of the Vladivostok State University of Economics and Service, 20, Dobrovolskogo Street, Vladivostok, Primorsky Krai, 690092, Russian Federation; Teacher of the Service and design college. Tel. +7 964 453-06-36. E-mail: k2857@mail.ru

Zolkin Alexander Leonidovich, Volga State University of Water Transport (Samara branch), 62-64, Molodogvardeyskaya Street, Samara, 443099, Russian Federation; PhD in Technical Science, Teacher of Natural-science and general professional disciplines sub-faculty. Tel. +7 960 825-68-49. E-mail: alzolkin@list.ru

Abramov Nikolai Viktorovich, Far Eastern Federal University, 8, Sukhanova Street, Vladivostok, Primorsky Krai, 690092, Russian Federation; Student. Tel. +7 914 373-91-16. E-mail: nikolay.abramov1990@mail.ru

Kurganov Daniil Olegovich, Far Eastern Federal University, 8, Sukhanova Street, Vladivostok, Primorsky Krai, 690092, Russian Federation; Student. Tel. +7 999 059-37-74. E-mail: kurganov_vl@mail.ru

References

1. Ilin S. *Protection of USB flash-drives against viruses*. URL: http://www.windxp.com.ru/articles61.htm (accessed: 22.02.2020). (In Russian.)
2. *Viruses elimination «Kaspersky lab fan-club forum»*. URL: http://forum.kasperskyclub.ru/index.php?showtopic=8920 (accessed: 22.02.2020). (In Russian.)
3. Bereza N.V. Current trends in the development of the global and Russian markets of information services. *Inzhenerniy vestnik Dona*, 2012, no. 2. URL: http://ivdon.ru/ru/magazine/archive/n2y2012/758 (accessed: 22.12.2019). (In Russian.)
4. Bondarev V.V. *Introduction to information security of automated system: study guide*. Moscow: Izdatelstvo MGTU im. N.E. Baumana, 2017, 255 p. (In Russian.)
5. Zolkin A.L. Development of the data management system for collection, processing and transmittion of data on the technical condition of electric motor collectors. *Nauchno-tehnicheskie aspekti innovacionnogo razvitiya transportnogo kompleksa: sbornik nauchnih trudov po materialam V Mezhdunarodnoy nauchno-prakticheskoi konferencii*, 2019, pp. 48–53. (In Russian.)
6. Pankratov S.A. Use of graphical information for protection of the software and data intelligence. *Inzhenerniy vestnik Dona*, 2012, no. 2. URL: http://ivdon.ru/ru/magazine/archive/n2y2012/792 (accessed: 25.01.2020). (In Russian.)
7. Willson E. *Network monitoring and analysis. Fault identification methods*. Moscow: Lori, 2016, 480 p. (In Russian.)
8. Zolkin A.L. Development of the data management system for control of traction electric motor collectors wearing. *Vestnik Donetskoi akademii avtomobilnogo transporta*, Donetsk: DAT, 2019, vol. 2, pp. 65–74. (In Russian.)
9. Aladishev O.S., Ovsyannikov A.P., Shabanov B.M. *Development of enterprise network of Interagency supercomputer center*. URL: http://vbakanov.ru›metods/1441 (accessed: 25.01.2020). (In Russian).
10. Gaiduk A.R. *Theory and methods of analytical synthesis of automatic control systems: (polynomial approach)*. Moscow: Izdatelstvo Fizmatlit, 2017, 264 p. (In Russian.)

11. Khalil H.K. *Nonlinear Systems*. 3rd ed. Upper Saddle River: Prentice Hall, 2016, 766 p. URL: http://en.bookfi.net/book/1417228/ (accessed: 25.01.2020).
12. Melin P., Castillo O. *Modeling, Simulation and Control of Non-linear Dynamical Systems: An Intelligent Approach Using Soft Computing and Fractal Theory*. Boca Raton: Taylor & Francis, 2017, 265 p.
13. Smirnov A.V. *Guideline on network traffic capture*. URL: http://blog.packet-foo.com/2016/11/the-network-capture-playbook-part-3-networkcards (accessed: 25.01.2020). (In Russian.)
14. Perlman R. *Interconnections: Bridges & Routers*. Boston: Addison-Wesley, 2016, 245 p.
15. Oggerino C. *High Availability Network Fundamentals*. Indianapolis: Cisco Press, 2017, 327 p.

Received 12.03.2020

ТЕХНОЛОГИИ ЦИФРОВОЙ ЭКОНОМИКИ

УДК 338.2

МЕЖДУНАРОДНЫЙ ОПЫТ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ, СТРУКТУРНЫЙ АНАЛИЗ ФУНКЦИОНАЛЬНЫХ АСПЕКТОВ

Абрамов В.Е., Юкласов К.А.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: vabrta@mail.ru

Статья содержит сравнительный анализ современного состояния цифровой экономики Евросоюза и России по разнонаправленным кластерам, которые, по мнению авторов, являются достаточно информативными и очевидными для специалистов отрасли. Цель данной статьи – аналитическое прогнозирование возможных этапов цифровизации социально-экономических механизмов развития. Авторы предполагают, что средства информационного содержания и манера их репрезентации могут оказаться интересными для специалистов, вовлеченных в цифровое развитие компьютерных технологий, экономики с ее социальными аспектами, которые непосредственно влияют на процессы планирования, стимулирования и регулирования отдельных отраслей. Цифровые выкладки способствуют объективному восприятию излагаемого материала, который статистически обеспечен оригиналами первоисточников. Логика изложения материалов основана на принципах элементарных последовательностей фактов и мнений зарубежных и отечественных экспертов отрасли, что позволяет использовать данные как специалистами, так и всеми заинтересованными лицами. Авторы полагают, что любые замечания и мнения могут оказаться полезными для дальнейшего развития.

Ключевые слова: *цифровизация, цифровая экономика, сетевые эффекты, конкуренция, регуляционные меры*

Введение

В предлагаемой статье анализируется современное состояние цифровой экономики с позиций специалистов этой отрасли. Авторы статьи предпринимают попытку не только дать оценку ее теперешнего состояния по первоисточникам, но и проанализировать возможные перспективы дальнейшего развития одной из моделей европейской экономики в качестве сравнительного образца. Выбор одной из евромоделей представляется целесообразным по ряду причин: цифровая экономика в Европе сравнительно молода и на начальном этапе своего развития использовала образцы уже существующих и действующих моделей, например американскую.

Выстраивая собственные компоненты цифрового структурирования, европейские эксперты использовали опыт уже функционирующих моделей с учетом специфики национального развития и этапного состояния собственной экономики. Компаративные усилия экспертов цифровизации достаточно эффективны, поскольку позволяют позитивно использовать накопленный опыт и избежать негативизма избыточного реинжиниринга. В данном аспекте представляется интересным анализ структурно-аналитического подхода, осуществляемого отечественными учеными и специалистами, так как любая стандартизация дает несомненные преимущества относительно фрагментарных и спорадических изысканий.

Описываемые системы структурного функционирования главным образом ориентированы и практически целенаправлены специфическими потребностями в современных терминах полезности, отрасли или методологическими условиями выполняемых задач. Таким образом, некий