ОСОБЕННОСТИ ОРГАНИЗАЦИИ И ПЛАНИРОВАНИЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

SPECIFICS OF THE ORGANIZATION AND PLANNING OF THE INVESTIGATION OF CRIMES COMMITTED WITH THE MALWARE

DOI: 10.31429/20785836-13-2-51-57

Маркосян Георгий Ашотович
кандидат экономических наук
доцент кафедры криминалистики и правовой информатики
ФГБОУ ВО «Кубанский государственный университет»
ID ORCID: 0000-0002-9749-3387

Markosyan Georgiy Ashotovich
Candidate of Economics
Associate Professor of Criminalistics and Legal Informatics department
Kuban State University

Бондаренко Юрий Алексеевич
кандидат юридических наук
доцент кафедры криминалистики и правовой информатики
ФГБОУ ВО «Кубанский государственный университет»
ID ORCID: 0000-0002-5750-685X
Researcher ID: M-6198-2016

Bondarenko Yuri Alekseevich
Candidate of Legal Sciences
Associate Professor of Criminalistics and Legal Informatics department
Kuban State University

Аннотация: Количество случаев использования вредоносных компьютерных программ в России существенно увеличилось за последние несколько лет. Авторы поставили цель установить особенности организации и планирования расследования преступлений этого вида и провести анализ следственной деятельности, чтобы найти пути дальнейшего совершенствования борьбы с компьютерной преступностью. Целью исследования выступает определение наиболее перспективных направлений организации и планирования расследования преступлений с использованием вредоносных программ. Результаты исследования выражаются в следующем:

1. На стадии проверки заявления о преступлении, где высока вероятность применения вредоносных компьютерных программ виновными лицами, следователь незамедлительно устанавливает полный контроль над компьютерной техникой потерпевшего и доступом к его электронным учетным записям. Производится отбор объяснений от заявителя, осмотр средств компьютерной техники и назначение судебной компьютерно-технической экспертизы с целью установить факт заражения вредоносной программой.

2. Направленность действий следователя обусловлена на выдвижение и проверку версий о наличии преступления, времени его совершения, установлении вреда заявителю, классификации вредоносной компьютерной программы, механизма заражения программного обеспечения потерпевшего и способах нанесения ему вреда. Все эти сведения определены как обстоятельства, подлежащие установлению для возбуждения уголовного дела.

3. Тактическими рисками организации расследования выступают невозможность классификации экспертом программы как вредоносной при наличии вреда, а также применение

комплекса мероприятий по анонимизации виновными лицами своих действий и даже недостоверность сообщаемых самим заявителем сведений о происшествии.

4. Способ заражения вредоносной программой и образовавшиеся следы от этого, зависят от избранной преступниками модели взаимодействия с жертвой. Здесь встречаются как распространение программы под видом служебной, сервисной, дополняющей другие и расширяющие возможности компьютера, так и уведомление потерпевшего, что использования программы незаконно, но принесет ему выгоды от ее использования. В таких случаях следователю приходится иметь дело с организованными, законспирированными группами преступников.

Ключевые слова: вредоносное программное обеспечение, расследование, преступление, организация и планирование.

Annotation: The number of cases of malicious computer programs in Russia has increased significantly over the past few years. The authors set out to establish the features of the organization and planning of the investigation of crimes of this type and to analyze the investigative activities in order to find ways to further improve the fight against computer crime. The purpose of the study is to determine the most promising areas of organizing and planning the investigation of crimes involving malware. The results of the study are expressed as follows:

1. At the stage of checking a crime report, where there is a high probability of malicious computer programs being used by the perpetrators, the investigator immediately establishes full control over the victim's computer equipment and access to his electronic accounts. The selection of explanations from the applicant, the examination of computer equipment and the appointment of a forensic computer-technical examination in order to establish the fact of infection with malware.

2. The focus of the investigator's actions is based on the promotion and verification of versions about the existence of a crime, the time of its commission, the establishment of harm to the applicant, the classification of malicious computer programs, the mechanism of infection of the victim's software and the methods of harming him. All this information is defined as the circumstances to be established for the initiation of a criminal case.

3. The tactical risks of organizing the investigation are the inability of the expert to classify the program as malicious in the presence of harm, as well as the use of a set of measures to anonymize the perpetrators of their actions, and even the unreliability of the information about the incident reported by the applicant himself.

4. The method of malware infection and the resulting traces depend on the model of interaction with the victim chosen by the criminals. Here you can find both the distribution of the program under the guise of a service, service, complementing other and expanding the capabilities of the computer, and the notification of the victim that the use of the program is illegal, but will bring him benefits from its use. In such cases, the investigator has to deal with organized, secret groups of criminals.

Keywords: malware, investigation, crime, organization and planning.

Введение

Статистика преступности в сфере компьютерной информации и информационных систем от года к году показывает неуклонный ежегодный рост как их количества, так и масштабов наносимого ущерба.

По данным Министерства внутренних дел Российской Федерации, в 2020 г. зарегистрирован существенный рост количества преступлений в информационно-телекоммуникационной сфере: более чем на 73,4 % по сравнению с 2019 г. В абсолютных цифрах за 2020 г. – 510396 преступлений зарегистрировано, раскрыто лишь 94942 из них [15]. Распространены хищения, вымогательство, незаконный оборот наркотических средств и психотропных веществ, изготовление и распространение порнографических материалов, неправомерный доступ к компьютерной информации.

Как видно из актуальной статистики, раскрываемость преступлений для этой категории в 2020 г. составила 18,6 %. Такое положение сказывается на восприятии многими пользователями виртуальной среды как нерегулируемой законодательством.

Практика показывает, что наиболее сложными для расследования выступают такие преступления в рассматриваемой сфере, где преступники применяют вредоносные компьютерные программы собственной разработки либо собственные модификации уже распространенных в компьютерных сетях вредоносных программ. Это обусловлено возможностями для виновных скрыть следы преступлений от разоблачения жертвами, и предотвратить их выявление сотрудниками правоохранительных органов. Целью исследования выступает определение наиболее перспективных направлений организации и

планирования расследования преступлений с использованием вредоносных программ.

Методы исследования

Основу методов криминалистического познания составляет метод отражения объектов и явлений в объективной реальности, сознании людей, на цифровых объектах [3].

Методология нашего исследования опирается на методы анализа и сравнения материалов уголовных дел по делам данной категории с дальнейшими обобщениями результатов в виде выводов. Такой подход международно признан, и поэтому использован нами в качестве обоснования новизны исследования. Для этого мы ознакомились с материалами 14 уголовных дел данной категории, расследованных в г. Москве, Краснодарском крае, Ростовской и Московской областях в период 2017–2020 г. Нами проведены сравнение направлений и программ расследования, установление по ним исходного плана следователя, а также логически проистекающей отсюда всей структуры организации расследования.

Для проверки достоверности выводов использован метод анализа части структуры последовательности кода программы, для отнесения ее к группе вредоносных [8], как один из факторов, влияющих на процесс формирования версий и планирования расследования вообще. И хотя организация и планирование расследования преступлений этой категории не затрагивает напрямую вопросы судебной компьютерно-технической экспертизы, однако, именно заключение эксперта на поставленные вопросы существенно влияет на дальнейшие действия и решения в рамках установления обстоятельств происшествия.

Результаты исследования

Результаты исследования выражаются в следующем:

1. На стадии проверки заявления о преступлении, где высока вероятность применения вредоносных компьютерных программ виновными лицами, следователь незамедлительно устанавливает полный контроль над компьютерной техникой потерпевшего и доступом к его электронным учетным записям. Производится отбор объяснений от заявителя, осмотр средств компьютерной техники и назначение судебной компьютерно-технической экспертизы с целью установить факт заражения вредоносной программой.

2. Направленность действий следователя обусловлена на выдвижение и проверку версий о наличии преступления, времени его совершения, установлении вреда заявителю, классификации вредоносной компьютерной программы, механизма заражения программного обеспечения потерпевшего и способах нанесения ему вреда. Все эти сведения определены как обстоятельства, подлежащие установлению для возбуждения уголовного дела.

3. Тактическими рисками организации расследования выступают невозможность классификации экспертом программы как вредоносной при наличии вреда, а также применение комплекса мероприятий по анонимизации виновными лицами своих действий и даже недостоверность сообщаемых самим заявителем сведений о происшествии.

4. Способ заражения вредоносной программой и образовавшиеся следы от этого, зависят от избранной преступниками модели взаимодействия с жертвой. Здесь встречаются как распространение программы под видом служебной, сервисной, дополняющей другие и расширяющие возможности компьютера, так и уведомление потерпевшего, что использования программы незаконно, но принесет ему выгоды от ее использования. В таких случаях следователю приходится иметь дело с организованными, законспирированными группами преступников.

Научная дискуссия

Традиционным поводом для проверки сообщений о преступлениях выступают заявления граждан, пострадавших от незаконных действий; сообщения от уполномоченных лиц или руководителей организаций, которые базируются на результатах внутреннего расследования предприятий; сведения, полученные в результате расследования других преступлений в сфере компьютерной информации, выделенные в отдельное производство; публикации в средствах массовой информации и глобальной сети «Интернет», а также непосредственное обнаружение следователем программного обеспечения, подпадающего под определение вредоносной программы при проведении осмотров, обысков, выемки.

Приступая к рассмотрению сообщения о преступлении в информационно-телекоммуникационных сетях, следователь определяет основные направления проверки и перечень фактов, которые при подтверждении влекут возбуждение уголовного дела. К ним относятся следующие:

− наличие у заявителя прав на цифровой финансовый актив, цифровую валюту или размещение им информации в информационных системах либо в памяти компьютера;

− содержание размещенной информации заявителем, возможность ее использования для нарушения его прав и законных интересов виновными;

− сведения о копировании, изменении, удалении информации заявителя;

− отсутствие воли самого заявителя на копирование, изменение, удаление или другие действия по распоряжению своими информационными ресурсами;

− отсутствие основанной на законе, договоре или условиях использования информационного ресурса, возможности у оператора информационной системы вносить изменения в информацию заявителя, без его уведомления;

− отсутствие права доступа виновных лиц к информации, которая стала предметом преступления;

− причинение имущественного, морального вреда или ущерба деловой репутации пострадавшего в результате действий виновных;

− способ, применявшийся виновными для незаконного собирания, уничтожения, изменения информации потерпевшего;

− способы и средства присвоения и легализации виновными финансового актива, цифровой валюты или иной информации, незаконно полученными от заявителя.

Как видно, ответы на поставленные для проверки сообщения о преступления вопросы, сами по себе образуют существенную часть подлежащих доказыванию обстоятельств, и направлены на формирование системы доказательств по уголовному делу.

Поэтому в преступлениях, совершаемых с использованием вредоносных программ, организация расследования начинается еще на этапе проверки сообщения о преступлении. Это обусловлено тем, что необходимо использовать специальные знания в области компьютерной техники и информационных технологий. Активно используются знания и в области финансов, когда транзакции проводятся цифровыми средствами платежа (криптовалютами), либо в безналичной форме с использованием личных счетов или счетов третьих лиц, обслуживаемых в кредитных организациях.

Такой подход полностью подтверждается практикой расследования, где в 100 % изученных материалов назначалась и производилась судебная экспертиза компьютерной техники и программного обеспечения, а в 35,7 % случаев устанавливалось движение денежных средств по счетам подозреваемых.

Расследованные факты преступлений с использованием вредоносных программ позволяют говорить, что часто преступники создают и реализуют смарт-карты для несанкционированного доступа к услугам провайдеров сети «Интернет», телеканалам с платной подпиской, создают вредоносный код для сбора сведений об учетных записях [5] и паролях пользователей социальных сетей, порталов государственных услуг и компьютерных игр, предполагающих коммерческую реализацию некоторых игровых функций для своих пользователей.

Мы находим несколько вариантов действий следователя для обнаружения и закрепления следов воздействия вредоносного программного обеспечения.

Первое направление предполагает обнаружение вредоносной программы пользователем в ходе взаимодействия с вычислительной машиной. На данный момент, это самый распространенный способ выявления. Это утверждение обосновано, в первую очередь, специфической сущностью и функционированием вредоносной программы. Зачастую она вызывает сбой в компьютерной системе пользователя, препятствует нормальному функционированию вычислительной машины.

При осмотре компьютерных средств можно использовать помощь технических специалистов органов государственной власти, если по каким-либо причинам невозможно обеспечить участие специалистов в области компьютерной техники органов внутренних дел [2]. Однако в нашем исследовании мы не обнаружили участия в осмотре иных, кроме территориального органа внутренних дел, специалистов, содействовавших следователю в обнаружении и изъятии электронных следов.

Однако немаловажен тот факт, что вредоносные программы разнообразны в своих воплощениях и функциональной направленности. В связи с чем возникают ситуации, в которых программное обеспечение работает в латентном режиме. Подобный случай представляет собой действительность, в которой обнаружить те или иные вирусы представляется проблематичным.

Латентность здесь выражается в том, что вредоносная программа маскирует сбои под ошибки, вызванные отдельными компонентами вычислительной машины (зачастую накопителем на жестких магнитных дисках) или же операционной системой.

Помимо прочего, существует разновидность вредоносного программного

обеспечения, обнаружить которую возможно лишь при мониторинге нагрузки центрального процессора и графического адаптера. Подобное явление характерно для программного обеспечения, использующего мощность вычислительной машины в целях осуществления деятельности по созданию новых структур, обеспечивающих функционирование криптовалютных платформ.

Также обнаружение вредоносной программы возможно при использовании компьютерных сетей и обмене информации. В данном случае речь идет о сетевых червях. Основная цель такого вредоносного программного обеспечения заключатся в самостоятельном распространении при помощи различных видов компьютерных сетей.

Как показывает анализ заключений экспертов, заражение может происходить двумя способами: в первом случае червь использует уязвимости программного обеспечения вычислительной машины пользователя; во втором случае, вредоносная программа провоцирует пользователя самостоятельно запустить ее.

Часто установление наличия происходит в результате проверки компьютерной техники специализированными антивирусными программами с актуальными [1]. Средство антивирусной защиты зачастую самостоятельно обнаруживает вредоносную программу и блокирует ее. Это привлекает внимание пострадавшего или системного администратора и служит причиной обращения о совершении преступления.

Любое планирование расследования нельзя осуществить без выдвижения и проверки версий. Именно версия позволяет установить возможные связи между механизмом преступления и подлежащими установлению фактами [4]. В нашем случае необходимо отталкиваться от данных о предполагаемом преступнике, а также от функциональной направленности вредоносной программы, изучить ее особенности и определить пути внедрения в вычислительную машину, а также механизм распространения.

Далее следует определить круг конкретных действий, совершение которых необходимо для получения доказательств по делу. Собирание доказательств осуществляется в результате проведения следственных действий, однако следует отметить, что формирование круга следственных действий производится на основании подлежащих установлению обстоятельств, объективированных в версии. Организация расследования использования вредоносных компьютерных программ не может быть осуществлена без постоянно корректируемого плана расследования.

В процессе выдвижения версий наиболее ценны те из них, которые направляют поисковые устремления следователя на установление личности преступника, основываясь на его навыках в программировании [7]. Данный подход показал свою эффективность в силу объективной корреляции между имеющимися в каждом расследуемом случае следами, способом совершения и личностью преступника.

Мы приходим к выводам, что факт создания вредоносной компьютерной программы выступает предикатным преступлением, то есть необходимой основой для совершения других преступлений в компьютерных сетях и базах данных, где виновный получает запланированный им преступный результат.

Криминалистически такой подход к анализу преступной деятельности, дробит традиционную модель полноструктурного способа преступления «подготовка – совершение – сокрытие». В результате выделяются дополнительные, но необходимые здесь структурные элементы: подготовка – разработка вредоносной программы как предикативное преступление – совершение основного преступления с ее помощью – достижение запланированного преступного результата – овеществление или иное распоряжение преступным результатом – сокрытие.

Такая категория преступлений в целом характеризуется высокой степенью обдумывания плана их совершения и сокрытия, особенно если участвует организованная группа лиц.

Д. Меймон и Э.Р. Лоудербек исследовали взаимозависимые преступления в сфере компьютерных технологий и информации в рамках концепции единой экосистемы киберпреступлений посредством проведения междисциплинарных связей между ее элементами. Это позволило им выявить основных участников взаимосвязей, куда включены посягатели, разработчики вредоносных приложений и программ, их цели и жертвы их преступлений, а также противостоящие преступникам правоохранительные органы, системные администраторы и разработчики программ для выявления несанкционированного доступа к защищаемой информации [12].

В целом, такая структура применяется также и российскими следователями, что упорядочивает организацию борьбы с преступлениями в сфере компьютерной

информации, в том числе и при обнаружении признаков преступлений.

А. Сингх предлагает особую структуру организации компьютерной сети для противодействия программам-вымогателям, назвав ее «цифровой готовностью». Она позволяет фиксировать все цифровые следы в компьютерной сети и немедленно предоставлять их для расследования преступления [14].

Сегодня исследователи занимаются познанием разных подходов к выявлению компьютерных вирусов [15], закономерностей распространения компьютерных вирусов в различных условиях компьютерной среды [11], моделированием нестандартных алгоритмов их внедрения на разные виды носителей компьютерной информации [16], моделированием условий массовых заражений конкретными видами вредоносных компьютерных программ в сети «Интернет» [9], выявлением компьютерных вирусов, перемещающих данные с использованием средств машинного обучения и естественных языков [10]. Эти исследования послужат основой для новых или совершенствования уже существующих методов судебно-экспертных исследований вредоносного программного обеспечения преступной деятельности.

Говоря о разработке прикладных методов вообще, научное познание продвинулось сегодня до анализа «больших данных», где нужная информация преступниками добывается из анализа имеющихся разрозненных сведений о жертве. Исследовательский коллектив под руководством В.Р. Ниведисы по этому поводу указывает на способность компьютерных вирусов к маскировке под видом программ анализа больших данных и использования полученной информации в незаконных целях [13]. Мы видим перспективное направление дальнейшей разработки положений методики расследования именно в работе следователя с такими видами производной из больших данных информации.

Представляется, в эпоху цифровой трансформации общественных отношений количество киберпреступлений продолжит возрастать в силу перехода большой части экономических отношений, взаиморасчетов в удобный пользователям формат. Поэтому выработка направлений расследования преступлений этого вида послужит первым этапом к декриминализации правоотношений в цифровой сфере.

Список использованной литературы:

1. Алиев А.Т. Проактивные системы защиты от вредоносного программного обеспечения // Известия ЮФУ. Технические науки. 2014. № 2. С. 26- 33.

2. Кравец Е.Г., Шувалов Н.В. Комплекс специальных знаний, необходимых при расследовании хищений, совершаемых с использованием вредоносных компьютерных программ // Юридическая наука и правоохранительная практика. 2020. № 3. С. 119-126.

3. Россинская Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2. С. 193-202.

4. Руденко А.В. Содержательная логика доказывания: монография. М., 2016.

5. Ручкин В.Н., Фомин В.В. Современные технологии виртуализации для обеспечения криминальной безопасности в процессе расследования // Информатика и прикладная математика. 2018. № 24. С. 112−118.

6. Состояние преступности в Российской Федерации за январь-декабрь 2020 г. // Официальный сайт Министерства внутренних дел Российской Федерации // URL https://мвд.рф/reports/item/22678184/.

7. Трубчанинов А.В. Особенности возбуждения уголовного дела и планирования на первоначальном этапе расследования преступлений,

References:

1. Aliev A.T. Proactive protection systems against malicious software // News of the Southern Federal University. Technical sciences. 2014. № 2. Pp. 26- 33.

2. Kravets E.G., Shuvalov N.V. Complex of special knowledge necessary in the investigation of theft committed with the use of malicious computer programs // Legal science and law enforcement practice. 2020. № 3. Pp. 119-126.

3. Rossinskaya E.R. Theory of information and computer support of criminalistics activities: concept, system, basic laws // Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2019. № 2. Pp. 193-202.

4. Rudenko A.V. Substantial logic of proof: monograph. M., 2016.

5. Ruchkin V.N., Fomin V.V. Modern technologies of virtualization for ensuring criminal security in the process of investigation // Informatics and Applied Mathematics. 2018. № 24. Pp. 112–118.

6. The state of crime in the Russian Federation for January-December 2020: Official Website of the Ministry of Internal Affairs of the Russian Federation // URL https://мвд.рф/reports/item/22678184/

7. Trubchaninov A.V. Features of criminal case initiation and planning at the initial stage of investigation of crimes

связанных с созданием, использованием и распространением вредоносных компьютерных программ // Вестник Волгоградской академии МВД России. 2019. № 1. С. 153-159.

8. Hiray S., Ranveer S. Comparative Analysis of Feature Extraction Methods of Malware Detection // International Journal of Computer Applications. 2015. № 120 (5) // https://doi.org/10.5120/21220-3960.

9. Iliev A., Kyurkchiev N., Rahnev A., Terzieva T. Some New Approaches for Modelling Large-Scale Worm Spreading on the Internet // Neural, Parallel and Scientific Computation. 2019. № 1. С. 23–34.

10. Karbab E.M.B., Debbabi M. MalDy: Portable, data-driven malware detection using natural language processing and machine learning techniques on behavioral analysis reports // Digital Investigation. 2019. Т. 28. С. S77–S87.

11. MadhuSudanan V., Geetha R. Dynamics of Epidemic Computer Virus Spreading Model with Delays // Wireless Personal Communications. 2020. https://doi.org/10.1007/s11277-020-07668-6.

12. Maimon D., Louderback E.R. Cyber-Dependent Crimes: An Interdisciplinary Review // Annual Review of Criminology. 2019. № 2. С. 191–216.

13. Niveditha V.R., Ananthan T.V, Amudha S., Dahlia S., Srinidhi S. Detect and Classify Zero Day Malware Efficiently In Big Data Platform // International Journal of Advanced Science and Technology. 2020. Т. 29. № 4s. С. 1947–1954.

14. Singh A., Ikuesan A.R., Venter H.S. Digital Forensic Readiness Framework for Ransomware Investigation // ICDF2C 2018: Digital Forensics and Cyber Crime. 2018. С. 91–105.

15. Souri A.A., Hosseini R. State-of-the-art survey of malware detection approaches using data mining techniques // Human-centric Computing and Information Sciences. 2018. № 8 // https://doi.org/10.1186/s13673-018-0125-x.

16. Zhang X., Li Y. Modelling and Analysis of Propagation Behavior of Computer Viruses with Nonlinear Countermeasure Probability and Infected Removable Storage Media // Discrete Dynamics in Nature and Society. 2020. // https://doi.org/10.1155/2020/8814319.

related to the creation, use and distribution of malicious computer programs // Bulletin of the Volgograd Academy of the Ministry of Internal Affairs of Russia. 2019. № 1. Pp. 153-159.

8. Hiray S., Ranveer S. Comparative Analysis of Feature Extraction Methods of Malware Detection // International Journal of Computer Applications. 2015. № 120 (5) // https://doi.org/10.5120/21220-3960

9. Iliev A., Kyurkchiev N., Rahnev A., Terzieva T. Some New Approaches for Modelling Large-Scale Worm Spreading on the Internet // Neural, Parallel and Scientific Computation. 2019. № 1. Pp. 23–34.

10. Karbab E.M.B., Debbabi M. MalDy: Portable, data-driven malware detection using natural language processing and machine learning techniques on behavioral analysis reports // Digital Investigation. 2019. Vol. 28. Pp. S77–S87.

11. MadhuSudanan V., Geetha R. Dynamics of Epidemic Computer Virus Spreading Model with Delays // Wireless Personal Communications. 2020. https://doi.org/10.1007/s11277-020-07668-6.

12. Maimon D., Louderback E.R. Cyber-Dependent Crimes: An Interdisciplinary Review // Annual Review of Criminology. 2019. № 2. Pp. 191–216.

13. Niveditha V.R., Ananthan T.V, Amudha S., Dahlia S., Srinidhi S. Detect and Classify Zero Day Malware Efficiently In Big Data Platform // International Journal of Advanced Science and Technology. 2020. Vol. 29. № 4s. Pp. 1947–1954.

14. Singh A., Ikuesan A.R., Venter H.S. Digital Forensic Readiness Framework for Ransomware Investigation // ICDF2C 2018: Digital Forensics and Cyber Crime. 2018. Pp. 91–105.

15. Souri A.A., Hosseini R. State-of-the-art survey of malware detection approaches using data mining techniques // Human-centric Computing and Information Sciences. 2018. № 8 // https://doi.org/10.1186/s13673-018-0125-x.

16. Zhang X., Li Y. Modelling and Analysis of Propagation Behavior of Computer Viruses with Nonlinear Countermeasure Probability and Infected Removable Storage Media // Discrete Dynamics in Nature and Society. 2020. // https://doi.org/10.1155/2020/8814319.