МЕТОДИКА РАССЛЕДОВАНИЯ НЕПРАВОМЕРНОГО ВОЗДЕЙСТВИЯ НА КОМПЬЮТЕРНУЮ ИНФОРМАЦИЮ ПРИ КОМПЬЮТЕРНОЙ АТАКЕ

А.Е. Фролов, Д.М. Нагаев
Алтайский государственный университет, г. Барнаул
email: frolov@mc.asu.ru

Аннотация. В статье рассмотрены вопросы расследования компьютерных инцидентов, возникающих при неправомерном дистанционном воздействии на компьютерную информацию с использованием вредоносных компьютерных программ. Предложена и апробирована новая методика такого расследования, основанная на анализе дополнительных индикаторов компрометации. Применение новой методики дает возможность устанавливать более детальную картину компьютерных инцидентов и более надежно строить вектор компьютерной атаки.

Ключевые слова: компьютерный инцидент, вредоносное программное обеспечение, защита информации, индикаторы компрометации.

Расследование компьютерных инцидентов, совершенных с применением вредоносного программного обеспечения в операционной системе Windows, требует анализа большого массива данных. Любое событие, записанное операционной системой, свидетельствует о каком-либо воздействии на эту систему. Часть событий напрямую связана с информационной безопасностью. Такие события называются индикаторами компрометации. Появление в операционной системе индикаторов компрометации свидетельствует о совершении вредоносным программным обеспечением каких-либо деструктивных действий, называемых вредоносным воздействием. Результатом успешного вредоносного воздействия является ущерб, нанесенный компьютерным данным или операционной системе [1]. Соответствующие преступные посягательства при этом могут подпадать под различные составы преступлений (например, ст. 272, 233, 159.6 УК РФ [2]).

Большой объем анализируемых при расследовании данных и сложность их обработки, которые возникают вследствие использования механизмов защиты вредоносного программного обеспечения (ПО), способных затруднить исследование кода программы, скрыть следы присутствия в операционной системе (ОС) вредоносного ПО или уничтожить часть индикаторов компрометации, являются одной из главных проблем в расследовании компьютерного инцидента.

Решению данной проблемы способствует систематизация и углубленный анализ индикаторов компрометации с целью восстановления хронологии компьютерного инцидента по прямым или косвенным признакам. Исследование дополнительных индикаторов компрометации сопровождается применением большого набора программных продуктов и методов интерпретации их результата. Подбор необходимых программных продуктов и методов анализа индикаторов является на сегодняшний день весьма актуальной задачей, а постоянное обновление криминалистических комплексов и информационных технологий придает новизну данному направлению исследований [3-5].

Цель настоящей работы заключается в разработке методики расследования неправомерного воздействия на конфиденциальную компьютерную информацию при компьютерной атаке с использованием вредоносного программного обеспечения, действующего на операционную систему (ОС). Для достижения этой цели необходимо решить следующие задачи:

- проанализировать существующие программные продукты;
- апробировать существующие методики на основе анализа практического инцидента;
- разработать и апробировать оптимальную методику.

В основе практического расследования компьютерных инцидентов лежит поиск ключевых индикаторов, которые с определенной долей вероятности являются доказательством совершения каких-либо вредоносных действий в ОС, повлекших за собой ущерб владельцу компьютерной информации. Индикаторы компрометации содержатся в таких файлах ОС, как системный реестр, локальный реестр пользователя, файлах Prefetch, журналах событий ОС, записях главной файловой таблицы (в файловой системе NTFS в качестве такого файла выступает MFT) и других [6]. Сами по себе обнаруженные индикаторы компрометации, за редким исключением, не несут большой смысловой нагрузки, но связки (комбинации) определенных событий [7] позволяют определить вектор развития атаки на компьютерную систему. Примерами подобных комбинаций могут служить:

– удаленное выполнение shell-кода (4648 код в журнале событий, запись запуска powershell.exe в ветке реестра AimCache.hve и файлах Prefetch);

– выполнение кода посредством технологии WMI (4648 код в журнале событий, запись запуска wmic.exe в ветке ShimCache и файлах Prefetch);

– удаленный доступ (1132 код в журнале событий, запись запуска mtsc.exe в ветке UserAssist файла UNUSER.dat и файлах Prefetch, а также записи Jumplists).

Анализ индикаторов компрометации позволяет выстроить «логическую нить» событий компьютерного инцидента. В то же время с развитием технологий ОС растет и объем индикаторов компрометации. Так, если обратить внимание на бесплатные наборы программных продуктов для компьютерной криминалистики (например, Nirsoft, Mitec, TZwork, Eric Zimmerman Tools или SIFT), то, например, программный продукт компании «Nirsoft» NirLauncher насчитывает в своем наборе более 120 программ для анализа индикаторов компрометации ОС Windows. Очевидно, что запуск всех этих программ и сравнение их результатов этих программ может занять огромное количество времени. В связи с этим на рынке существуют программные комплексы, предназначенные непосредственно для использования в криминалистических целях (например, Encase Forensics, AccessData FTK, Magnet Axiom, BelkaSoft, X-Ways Forensics, Autopsy).

Анализ российского рынка программных продуктов, предназначенных для криминалистического исследования компьютерной информацией, свидетельствует о достаточно большом количестве программных и программно-аппаратных комплексов. В такой перечень входят, в частности, такие программные продукты, как Belkasoft, X-Ways, AutoPsy и другие. Исследования этих программных продуктов показало наличие общей схожести в предлагаемом функционале. Однако на практике предлагаемый каждым программным комплексом функционал не охватывает всех категорий индикаторов компрометации. В силу этого для исследования необходимо использовать дополнительный набор программных продуктов, обеспечивающий более детальный разбор отдельных индикаторов компрометации (например, NirSoft, TzWork или Mitec). Применение программных комплексов позволяет существенно сократить время на расследование компьютерного инцидента, частично или полностью автоматизировав анализ отдельных массивов данных.

Условно процесс расследования компьютерного инцидента можно разделить на три этапа: автоматический, полуавтоматический и ручной. Автоматически этап анализа представляет собой сбор, обработку и анализ данных с помощью программных средств. На данном этапе можно применять такие программные решения как Belkasoft и AutoPsy. На этом этапе собирается и анализируется весь массив данных, позволяя быстро переключаться между категориями обнаруженных индикаторов (рисунок 1). Помимо объединения всех индикаторов в единое пространство на автоматическом этапе возможно структурирование индикаторов по

категориям для облегчение анализа или же поиск интересующей информации по ключевым словам (например, поиск слова «AnyDesk» во всех индикаторах).

Полуавтоматический этап анализа отличается от автоматического этапа тем, что необходимо анализировать дополнительные индикаторы компрометации. Для этого необходимо проверять косвенные индикаторы компрометации, например запуск нестандартных программ, установку программ по нестандартному пути (рисунок 2), их расположение в ОС, а также производить ручной поиск индикаторов в директориях программных продуктов, представляющих интерес (например, нестандартное расположение программных продуктов или имена директорий). На данном этапе можно применять такие программные решения как Belkasoft, Autopsy, Mitec или Nirsoft.

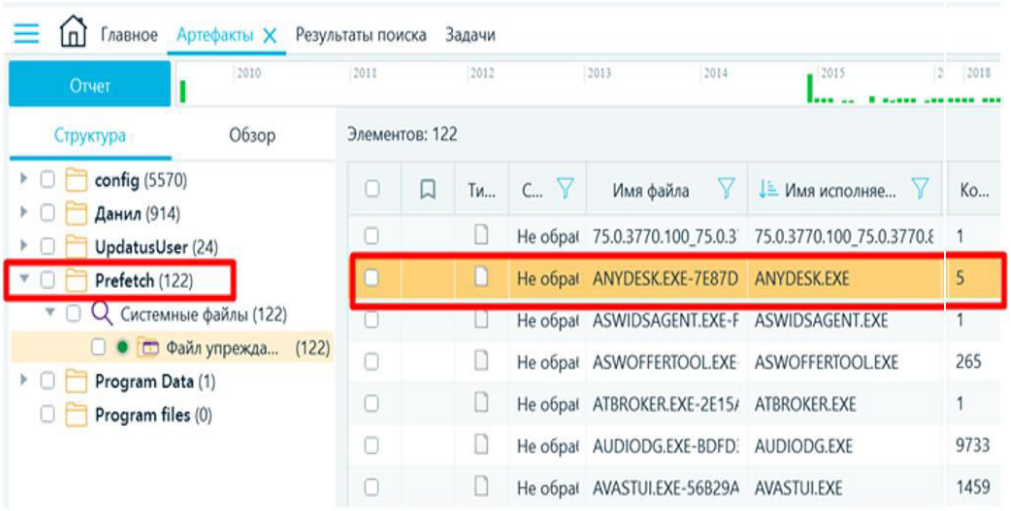

Рисунок 1. Пример результата анализа данных при помощи Belkasoft.

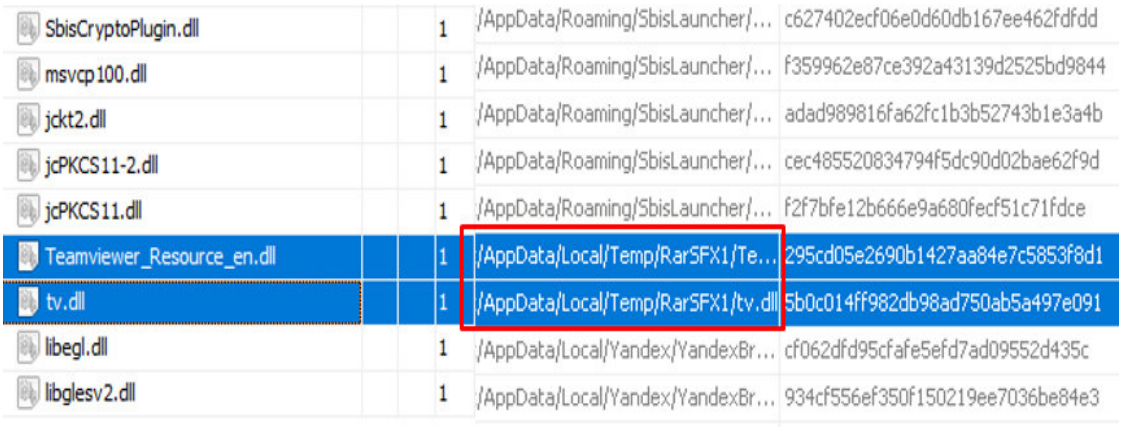

Рисунок 2. Пример анализа дополнительных индикаторов при помощи AutoPsy.

На ручном этапе необходимо проводить анализ, при котором требуется просматривать и сравнивать различные записи журналов, сравнивать и сопоставлять время и т.д., учитывая смещение времени в ОС. На данном этапе требуется детальный анализ всех индикаторов компрометации, в том числе ранее удаленных. Для этого необходимо применять средства для восстановления ранее удаленной информации (например, R-Studio, DMDE или UFS). Применение данных программных продуктов с большой долей вероятности позволяется обнаружить уничтожение необходимых для расследования инцидентов объектов (например, удаление вредоносных файлов антивирусными средствами, или обнаружение дополнительных ip-адресов). Заключительным моментом на данном этапе является построение timeline для восстановления хронологии инцидента (рисунок 3) [8].

-04-16T14:52:57	Last Access Time	/Users/A ›/Downloads/Пример отчета по закупкам/Пример отчета по закупкам.xls.exe Type: file C
-04-16T14:53:51	Content Modification Time	/Windows/System32/Install.cmd Type: file Owner identifier: 0 Group identifier: 0 Mode: 0o777 Number of links: 1
-04-16T14:53:51	Last Access Time	/Windows/System32/Install.cmd Type: file Owner identifier: 0 Group identifier: 0 Mode: 0o777 Number of links: 1
-04-16T14:53:51	Metadata Modification Time	/Windows/System32/Install.cmd Type: file Owner identifier: 0 Group identifier: 0 Mode: 0o777 Number of links: 1
-04-16T14:53:51	Last Access Time	/Windows/System32/32_rdpclip.exe Type: file Owner identifier: 0 Group identifier: 0 Mode: 0o777 Number of links: 2
-04-16T14:53:51	Content Modification Time	/Windows/System32/32_rdpclip.exe Type: file Owner identifier: 0 Group identifier: 0 Mode: 0o777 Number of links: 2
-04-16T14:53:51	Metadata Modification Time	/Windows/System32/32_rdpclip.exe Type: file Owner identifier: 0 Group identifier: 0 Mode: 0o777 Number of links: 2
-04-16T14:53:51	Last Access Time	/Windows/System32/32_termsrv.dll Type: file Owner identifier: 0 Group identifier: 0 Mode: 0o777 Number of links: 2
-04-16T14:53:51	Content Modification Time	/Windows/System32/32_termsrv.dll Type: file Owner identifier: 0 Group identifier: 0 Mode: 0o777 Number of links: 2
-04-16T14:53:51	Metadata Modification Time	/Windows/System32/32_termsrv.dll Type: file Owner identifier: 0 Group identifier: 0 Mode: 0o777 Number of links: 2
-04-16T15:23:46	Content Modification Time	/Windows/System32/runmipko.lnk Type: file Owner identifier: 0 Group identifier: 0 Mode: 0o777 Number of links: 1
-04-16T15:23:46	Content Modification Time	/Windows/System32/runmipko.lnk Type: file Owner identifier: 0 Group identifier: 0 Mode: 0o777 Number of links: 1
-04-16T15:23:46	Last Access Time	/Windows/System32/runmipko.lnk Type: file Owner identifier: 0 Group identifier: 0 Mode: 0o777 Number of links: 1

Рисунок 3. Пример анализа дополнительных индикаторов при помощи AutoPsy.

Построенная при помощи «SIFT» timeline позволяет просмотреть все индикаторы по времени, детально отслеживая все события, произошедшие в ОС. Например, построение timeline анализа накопителя на жестких магнитных дисках (НЖМД) может предоставить информацию о запуске пользователем конкретного исполняемого файла, последующего запуска оболочки командной строки, проведении манипуляций с удаленным доступом, запуском вредоносных библиотек и запуском программы-шпиона. На данном этапе можно применять такие программные решения как FTK Imager, Mitec, Nirsoft или SIFT.

По итогам расследования компьютерного инцидента может быть построен описан вектор атаки злоумышленника и хронология работы вредоносной программы с момента проникновения в ОС до воздействия на компьютерную информацию и нанесения ущерба. Пример конкретного вектора атаки при его наложении на модель cyber kill chain [8] приведен на рисунке 4.

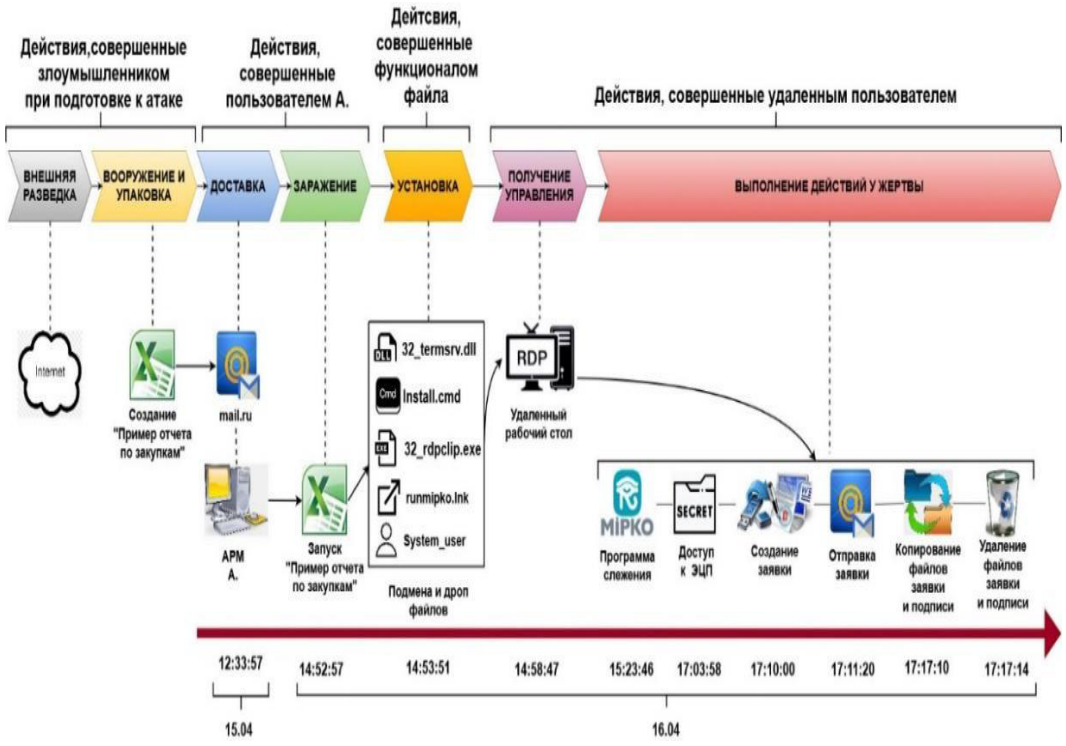

Рисунок 4. Пример построения цепочки атаки.

Методика cyber kill chain дает наглядное представление вектора атаки. Однако на практике часть индикаторов компрометации удаляется вредоносными программами с целью сокрытия следов инцидента. Из-за этого нельзя однозначно связать отдельные блоки событий, тем самым внося в расследование компьютерного инцидента элемент неопределенности.

Для устранения таких неопределенностей и соединения блоков событий в единую логическую цепочку необходимо прибегать к еще одному методу анализа индикаторов компрометации, а именно, к обратной разработке вредоносных файлов (reverse engineering) [9]. Обратная разработка подразумевает исследование программы или исполняемого файла с целью понять принцип его работы. Применение на практике методов обратной разработки совместно с восстановлением хронологии компьютерного инцидента дают более детальное понимание совершенного компьютерного инцидента.

Анализ исполняемых файлов при обратной разработке может производиться статическими или динамическими методами. При анализе файла необходимо обращаться внимание на следующие индикаторы:

- обращение к нестандартным библиотекам;
- импорты и экспорты функций;
- строки;
- ip- адреса;
- вызов оболочки командной строки.

На данном этапе можно применять такие программные продукты как IDA Pro, OllyDbg, x64_dbg, radare2, frida, WinDbg, ghidra. Также возможно примирение онлайн сервисов для ускорения анализа базовыми методами, например VirusTotal, Cuckoo или Anyrun. Применение этих программных продуктов позволяет понять принцип работы вредоносного файла и описать функционал анализируемого файла [10]. Пример наглядного представления функционала приведен на рисунке 5.

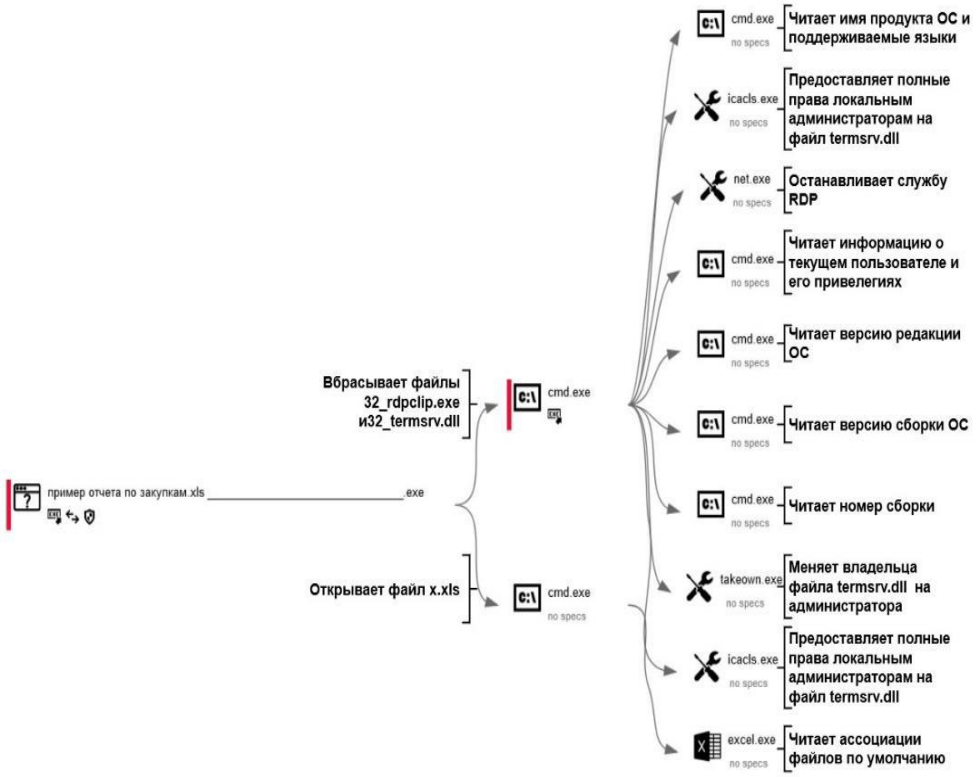

Рисунок 5. Пример представления функционала анализируемого файла.

На основе обобщения практики расследования конкретных компьютерных инцидентов может быть предложена общая методика расследования, включающая в себя следующие последовательные этапы [1-8]:

1. Фиксация доказательств (создание образа или дубликата).
2. Восстановление ранее удаленной информации.
3. Проверка антивирусными средствами.

4. Автоматический анализ памяти (поиск базовых индикаторов компрометации).
5. Поиск дополнительных индикаторов компрометации (журналов событий и браузеров).
6. Построение timeline.
7. Анализ подозрительных файлов автоматизированными средствами (например, онлайн песочницы VirusTotal, Cuckoo, AnyRun).
8. Ручной анализ подозрительных файлов.

На первом этапе производится сбор и анализ основной информации об ОС (платформа, версия, зарегистрированные пользователи, временная зона) и типе файловой системы, выбирается список наиболее важных индикаторов, характерных для ОС. Вторым этапом производится восстановление ранее удаленных данных. Данную процедуру поддерживают все комплексы для криминалистического анализа, но в случае их отсутствия возможно применение узкоспециализированного ПО (например, UFS, R-Studio, DMDE). Третий этап заключается в поиске в памяти объекта (в том числе ранее удаленных данных) программ, детектируемых антивирусными средствами как вредоносные. Четверным этапом производится анализ базового списка индикаторов (системный реестр или локальный реестр пользователя, Prefetch, jumplists, Event Log, Services), символизирующих о присутствии вредоносного ПО. Пятый этап заключается в поиске косвенных индикаторов компрометации, косвенно указывающих на следы присутствия вредоносного ПО в ОС (журнал событий, история браузера, журнал $MFT или $UsnJrnl). Шестым этапом производится анализ всех имеющихся индикаторов компрометации с целью детального восстановления хронологии компьютерного инцидента. На данном этапе происходит построение timeline с целью детального разбора действий, зафиксированных ОС во время вредоносного воздействия. Седьмой этап включает в себя проверку всех подозрительных файлов, которые не были детектированы антивирусными средствами на третьем этапе. Восьмой этап заключается в ручном анализе подозрительных файлов с целью определения их функционала.

Апробация описанной в работе методике показала, что эта методика позволяет наиболее детально выявлять обстоятельства неправомерного воздействия на компьютерную информацию при компьютерной атаке.

Библиографический список.

1. Тушканова О.В. Терминологический справочник судебной компьютерной экспертизы: Справочное пособие. – М.: ЭКЦ МВД России, 2005.
2. Уголовный кодекс Российской Федерации [Текст]: от 13.06.1996 № 63-ФЗ (ред. от 07.04.2020) // Собрание законодательства РФ. – 17.06.1996. – № 25. – Ст. 2954. https://www.securityvision.ru/blog/indikatory-komprometatsii/
3. Windows Artifact Analysis [Электронный ресурс] // URL: https://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf. (Дата обращения 21.03.2022).
4. Индикатор компрометации [Электронный ресурс] // URL: https://encyclopedia.kaspersky.ru/glossary/indicator-of-compromise-ioc/ (Дата обращения 19.04.2022).
5. Индикатор компрометации (Indicator of Compromise, IoC) [Электронный ресурс] // URL: https://encyclopedia.kaspersky.ru/glossary/indicator-of-compromise-ioc/ (Дата обращения 15.03.2022).
6. Windows Forensics Analysis — Windows Artifacts (Part I) [Электронный ресурс] // URL: https://nasbench.medium.com/windows-forensics-analysis-windows-artifacts-part-i-c7ad81ada16c (Дата обращения 23.06.2022).

7. Find Evil – Know Normal [Электронный ресурс] // URL: https://share.ialab.dsu.edu/CAE_Workshops/2019/Incident%20Response/Supplementary%20Material/SANS_Poster_2018_Hunt_Evil_FINAL.pdf (Дата обращения 23.06.2022).
8. Реагирование на инциденты информационной безопасности в РФ [Электронный ресурс] // URL: https://tsarev.biz/stati/rassledovanie-inczidentov-kompyuternoj-bezopasnosti (Дата обращения 26.03.2022).
9. Reverse engineering: обратная разработка приложений для самых маленьких [Электронный ресурс] // URL: https://habr.com/ru/company/pentestit/blog/555590/ (Дата обращения 27.06.2022).
10. ANY.RUN - Interactive Online Malware Sandbox [Электронный ресурс] // URL: https://any.run/. (Дата обращения 19.05.2022).
11. Что такое Cyber-Kill Chain и почему ее надо учитывать в стратегии защиты [Электронный ресурс] // URL: https://habr.com/ru/company/panda/blog/327488/. (Дата обращения 16.05.2022).

METHODOLOGY OF INVESTIGATION OF UNLAWFUL INFLUENCE ON COMPUTER INFORMATION DURING A COMPUTER ATTACK

A.E. Frolov, D.M. Nagaev
Altai state university, Barnaul
email: frolov@mc.asu.ru

Annotation. The article considers the issues of investigation of computer incidents arising from illegal remote exposure to computer information using malicious computer programs. A new method of such investigation based on the analysis of additional indicators of compromise is proposed and tested. The use of the new technique makes it possible to establish a more detailed picture of computer incidents and more reliably build a computer attack vector.

Keywords: computer incident, malicious software, information protection, indicators of compromise.