КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.781
УДК 004.056.57

Чернігівський Іван Андрійович
аспірант
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0009-0003-4568-3212
i.chernihivskiy@gmail.com

Крючкова Лариса Петрівна
доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-8509-6659
l.kriuchkova@kubg.edu.ua

СИСТЕМНИЙ ПІДХІД ДО ВИРІШЕННЯ ЗАДАЧІ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОКОМУНІКАЦІЙНІЙ МЕРЕЖІ ВІД ВПЛИВУ КОМП'ЮТЕРНИХ ВІРУСІВ

Анотація. Сучасна інфокомунікаційна мережа є розподіленою системою, базові елементи якої об'єднані в єдиний інформаційний простір. Задача забезпечення якісного функціонування інфокомунікаційних мереж в умовах впливу комп'ютерних вірусів обумовлює необхідність контролю стану мережі для своєчасного виявлення тривожних подій, під якими розуміється виявлення ознак зараження технічних засобів мережі. Очевидно, що для досягнення необхідного рівня захищеності інформації в мережі мають бути забезпечені вірні і своєчасні управлінські рішення для запобігання небажаних наслідків. Це обумовлює необхідність створення більш досконалих методів захисту інформації від впливу комп'ютерних вірусів на технічні засоби мережі. Мета публікації — формування системного підходу до вирішення задачі захисту інформації в інфокомунікаційній мережі від впливу комп'ютерних вірусів з обґрунтуванням словника ознак, необхідних для виявлення тривожних подій, і забезпечення підтримки цільового стану інфокомунікаційної мережі. Обґрунтовано основні науково-технічні завдання для створення системи захисту інформації від впливу комп'ютерних вірусів, побудованої за принципом керуючої системи. Запропоновано в якості ідентифікаційних ознак стану інфокомунікаційної мережі для виявлення тривожних подій використовувати цифрові артефакти, які залишають шкідливі програмні засоби в результаті впливу. Розглянуто можливість використання Forensic-аналізу з неповним набором цифрових артефактів. Визначено універсальні артефакти, виявлення яких свідчить про стовідсоткову зараженість. Побудова системи захисту інформації у вигляді автоматизованої системи управління, спрямованої на забезпечення підтримки цільового стану інфокомунікаційної мережі, дозволяє забезпечити необхідний рівень захищеності інформації. Зазначений словник ознак для ідентифікації стану інфокомунікаційної мережі є достатнім для прийняття рішень в циклах управління системи захисту інформації. Практичне значення отриманих результатів полягає у можливості їх застосування в різних галузях для вдосконалення методів захисту інформації від впливу комп'ютерних вірусів і більш ефективного використання часу аналітика при проведенні Forensic-аналізу інфокомунікаційної мережі.

Ключові слова: інформація; кібербезпека; віруси; захист; ідентифікаційні ознаки; виявлення тривожних подій; захист інформації; інфокомунікаційні мережі.

ВСТУП

У сучасному світі успіх будь-якого підприємства вирішальною мірою визначається ефективністю його інформаційної інфраструктури. Для вірної оцінки ситуації та прийняття своєчасного обґрунтованого рішення керівнику необхідна інформаційна система, яка забезпечує достовірне і повне відображення поточного стану підприємства.

В сучасних умовах успішним технологічним рішенням може вважатися система, яка має такі характеристики як:

- простота для кінцевого користувача;
- гнучкість в нарощуванні функціональних можливостей;
- масштабованість;
- відкритість;
- можливість розмежування доступу користувачів;
- відмовостійкість.

Забезпечення зазначених вимог під час створення інформаційної системи можливо за умови застосування для її розробки сучасних інструментальних засобів, що реалізують стандартні методи обробки, передачі та зберігання даних.

Сучасні програмні засоби надають розробнику широкий вибір інструментів для створення інформаційних систем будь-якої складності. Основною тенденцією при побудові корпоративних інфокомунікаційних мереж (ІКМ) є використання Internet\Intranet-технологій, які найбільш повно відповідають вищезазначеним вимогам. З появою «візуального програмування» значна кількість задач, рішення яких потребувало залучення професійних програмістів, стало доступним безпосередньо користувачу інформаційної системи. Таким чином, в ролі розробника системи виступає користувач цієї системи, що володіє усіма аспектами її експлуатаційних можливостей і характеристик.

Критично важливим завданням для забезпечення надійного та ефективного функціонування ІКМ є завдання захисту інформації.

У кібербезпеці прийнято загрози поділяти за такими основними ознаками:

- порушення цілісності інформації;
- порушення конфіденційності інформації;
- порушення доступності інформації.

Пошкодження інформаційних систем комп’ютерними вірусами може одночасно призводити до усіх цих порушень.

Основним методом боротьби з вірусами завжди були антивіруси, тому процес розвитку вірусів і антивірусів — це постійна війна технологій. Регулярно у вірусах реалізовуються оригінальні ідеї, що вимагає адекватних дій від розробників антивірусного ПЗ. Для корпоративного сегменту боротьба з вірусами зазвичай забезпечується рішеннями класу Endpoint Detection and Response (EDR), які на додачу до звичайного модулю Endpoint Protection (EPP) мають модулі Next Generation Antivirus (NGAV) та поглиблений поведінковий аналіз. Слід зазначити, що не завжди цих мір буває достатньо, тому потрібно чітко розділяти ПК на заражені\не заражені, на випадок, якщо захисне рішення «пропустило» невідомий вірус.

Постановка проблеми. Узагальнену структуру інфокомунікаційної мережі наведено на рис. 1. Зазвичай структура ІКМ включає головний офіс та додаткові філіали у різних містах, філіали отримують доступ до інтернету та необхідних для функціонування мережі внутрішніх ресурсів (Active Directory, Database File Server, тощо) через головний офіс. В локальних мережах швидкість передачі даних 90–100МБ\сек, між мережами — 20МБ\сек, швидкість доступу в Інтернет коливається в межах 60–90МБ\сек. ПК\сервери мають різну апаратну\програмну конфігурацію (у тому числі оновлення і версії ОС).

Для прикладу, мережа має проблеми з вивантаженням артефактів оскільки має неоднорідну структуру:

Kiev Network — має 300ПК (Win7 100, Win10 170, Win11 30) і 10 серверів (Win2003 1, Win2008 2, Win2016 2, Win2019 5);

Uzhorod Network — має 200ПК (WinXP 5, Win7 75, Win8.1 10, Win10 110) і 3 сервера (Win2016 1, Win2019 2);

Kharkiv Network — має 200ПК (WinXP 5, Win7 70, Win8.1 5, Win10 120) і 3 сервера (Win2016 1, Win2019 2).

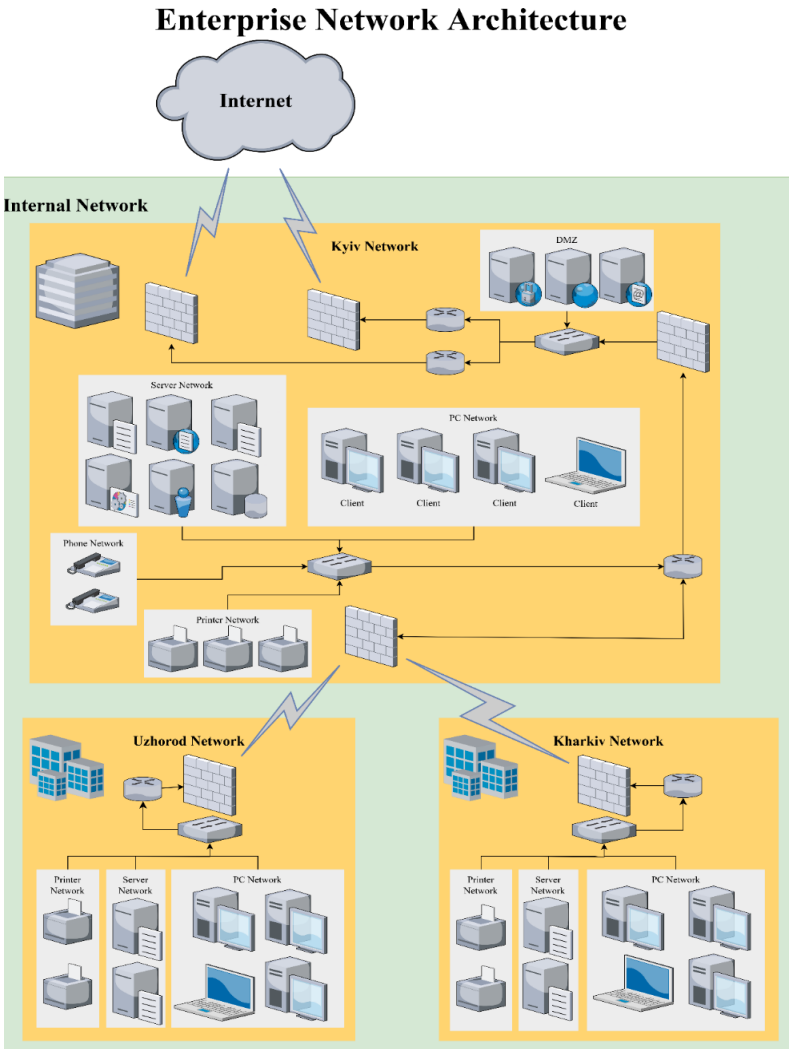


Рис. 1. Узагальнена структура інфокомунікаційної мережі

Зазначена мережа має ряд проблем як в адмініструванні, так і в вивантаженні артефактів:

– різна пропускна здатність локальних мереж, що спричиняє довше завантаження даних з філіалів і неможливість швидко оцінити приблизний час завантаження;
– різний час роботи співробітників (різні вихідні дні, різні робочі години, залишення робочого місця в робочі години), що не дозволяє аналітику інформаційної безпеки (ІБ) достовірно спрогнозувати наявність\відсутність співробітника на робочому місці, адже необхідно щоб ПК був доступний у мережі. При цьому робота аналітика не повинна перешкоджати роботі співробітника;
– неможливість в будь-який час підключитися до ПК та ноутбуків (бо користувачі їх переміщують та підключаються з інших мереж + можуть бути

додаткові помилки), що не дозволяє отримати інформацію про стан ПК і невідомо, коли це можна буде зробити в майбутньому;
- залежність швидкодії від того, з якою конфігурацією апаратного і програмного забезпечення ПК працює користувач;
- різні налаштування доступу до ПК через помилки або неправильну конфігурацію (наприклад, адміністратор віддав недоналаштований ПК користувачу, у якому за замовчуванням закрито ICMP та інші протоколи), що перешкоджає отриманню інформації про стан ПК;
- залежність від користувачів, які вимикають свій ПК замість виходу з акаунту після переривання своєї роботи (своєрідна «економія електроенергії»), що спричиняє ситуацію, коли спочатку не можна підключитись до ПК, бо користувач за ним працює, а пізніше підключитись теж не можна, бо користувач вже не працює. Це не дозволяє аналітику вчасно отримати необхідну інформацію.

Додатково, через війну та часті відключення електроенергії, адміністратор не може спрогнозувати, коли конкретний ПК буде знову відключений від мережі. Це призводить до ситуації, коли навіть почавши завантажувати архів з артефактами, що згенерувала програма для проведення Forensic Triage, відбувається переривання з'єднання і невідомо через який час ПК знову з'явиться в мережі. В результаті архів залишається недозакачаним і аналітик не має жодного уявлення про стан ПК.

Зазначені проблеми обумовлюють необхідність вирішення наступних задач:
- суттєво зменшити кількість часу на обробку інформації та її передачу, порівняно з наявними рішеннями;
- передавати артефакти у текстовому форматі нестиснутими;
- розбирати наявні артефакти на предмет аномалій автоматично.

Для зменшення часу, у випадку коли ми не можемо підвищити швидкість передачі у мережі та вплинути на швидкодію диску\процесора досліджуваного ПК, потрібно зменшити розмір та кількість даних, що підлягають передачі.

Цього можна досягти за рахунок:
- зменшення кількості програм та артефактів, залишивши тільки ті, що будуть корисні (без непотрібних дублікатів);
- оптимізації виводу артефактів (відкинувши варіанти які точно не є шкідливими);
- використання програм-парсерів артефактів, щоб передавати не бінарні, а текстові дані, які будуть суттєво менші;
- виключення зайвих операцій (зтискання\розтискання\передачі програм);
- автоматичного віддаленого запуску програм та завантаження артефактів на заздалегідь заданий сервер;
- розпаралеленого запуску кількох процесів, що вивантажують артефакти;
- передачі за можливості метаданих файлу, а не самого файлу (наприклад, не файли Prefetch, а їх розібраний вигляд у текстовому форматі);
- автоматичної передачі артефакту відразу після вивантаження з ПК, а не очікування вивантаження усіх артефактів з подальшою їх централізованою передачею.

Для передачі артефактів у нестиснутому форматі необхідно:
- потрібно проранжувати артефакти на відповідність\значущість для конкретного сценарію та визначити порядок їх завантажень, що надасть

можливість отримати більше уявлення про стан системи, ніж якби вони завантажувались їх у випадковому порядку;
- використовувати програми-парсери артефактів, щоб передавати не бінарні, а текстові дані, які будуть суттєво менші;
- здійснювати підготовку текстового виводу для машинної обробки, що в деяких випадках забезпечує значне зменшення розміру вихідного файла.

Для автоматичного розбору аномалій потрібен окремий модуль, функціональним призначенням якого є:
- виявлення специфічних даних, які з високою імовірністю вказують на потенційне зараження;
- виконання відповідних додаткових дій над проблемним ПК (наприклад, заблокувати його до вирішення всіх обставин і перевірки інших наявних артефактів);
- формування відповідного повідомлення, який приверне увагу аналітика ІБ.

Аналіз останніх досліджень і публікацій. Щоб відповідати сучасним вимогам безпеки, ІКМ та інформація, яка в ній циркулює, повинна бути захищена від порушення цілісності, конфіденційності, доступності. Функціонування шкідливих програмних засобів (ШПЗ), методи їх виявлення та способи ліквідації розглядали такі відомі вчені, як М. Д. Василенко, В. О. Рачук, В. М. Слатвінська [1], Д. О. Ричка [2]. У дослідженні М. Д. Василенко, В. О. Рачук і В. М. Слатвінська [1] висвітлюється тема виявлення шкідливих програм в контексті вимог комп'ютерної безпеки. У праці Д. О. Ричка [2] розглянуто комплекс заходів щодо захисту бази даних від кіберзагроз і визначено напрямки боротьби із комп'ютерними вірусами.

Автори Muhammad Shamraiz Bashir, Mirwais Khan [3] та Da-Yu Kao, Guan-Jie Wu [4] розглянули можливі рішення для вивантаження артефактів з ПК, проведення Live Computer Forensics та визначення місць розташування цифрових артефактів.

Проте, як свідчить аналіз наукових робіт, потребує подальших досліджень розробка нових підходів до створення сучасного механізму захисту комп'ютерного середовища та інформації від шкідливих програм і кібератак, а також вдосконалення наявних методів ідентифікації ШПЗ на ПК.

Зазначені умови функціонування ІКМ вимагають вірних і своєчасних управлінських рішень для запобігання небажаних наслідків. Це обумовлює необхідність створення більш досконалих методів захисту інформації в ІКМ від впливу комп'ютерних вірусів на технічні засоби мережі.

Завдання забезпечення якісного функціонування інфокомунікаційних мереж в умовах впливу комп'ютерних вірусів обумовлює необхідність контролю стану мережі для своєчасного виявлення тривожних подій під якими розуміється виявлення ознак зараження технічних засобів мережі.

Метою статті є формування системного підходу до вирішення задачі захисту інформації в інфокомунікаційній мережі від впливу комп'ютерних вірусів з обґрунтуванням словника ознак, необхідних для виявлення тривожних подій, і забезпечення підтримки цільового стану інфокомунікаційної мережі.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

ІКМ можна класифікувати як складну динамічну багатопараметричну слабодетерміновану систему з розподіленими параметрами, в якій можуть виникати несподівані емерджентні властивості в результаті впливу комп'ютерних вірусів.

Очевидно, що для досягнення необхідного рівня захищеності інформації має бути забезпечена здатність передбачати та запобігати появі цих властивостей на об'єкті захисту.

Вирішення такої задачі досягається побудовою системи захисту інформації у вигляді *системи управління*, що забезпечує підтримку цільового стану об'єкта управління (ОУ). При цьому мета управління може бути представлена як стабілізація стану ОУ або переведення ОУ в деякий кінцевий (цільовий) стан, при якому забезпечується необхідний рівень захищеності інформації.

Рис.2. Інформаційна структура циклу управління ІКМ

За інформаційною сутністю процес управління формалізується у вигляді замкнутого циклу послідовного звернення до трьох операторів: ідентифікації об'єкта управління (ОУ), прийняття рішень про характер і величину керуючих впливів, що забезпечують досягнення поставленої мети, та здійснення керуючих впливів (рис. 2). При цьому під ідентифікацією ОУ розуміється отримання інформації, необхідної і достатньої для ухвалення рішення в циклі управління.

Мета управління досягається забезпеченням якісного функціонування всіх операторів у кожному циклі управління. Основою ж для прийняття вірних керуючих впливів на ОУ є достатність і достовірність інформації при ідентифікації стану ОУ. Межа між тим, що вважається навколишнім середовищем і тим, що вважається об'єктом управління відносна і визначається можливістю системи управління здійснювати на них вплив.

Основна проблема, яка проявляється при синтезі системи управління складним динамічним об'єктом — невизначеність і недостатність апріорної вхідної інформації про об'єкт управління, наявність невідомих факторів, що суттєво впливають на його поведінку і, як наслідок, проблематичність побудування змістовної аналітичної моделі складного об'єкта управління. Тому, замість параметричного управління вводиться більш широке поняття «управління за станом складного об'єкта управління» [5]. При цьому, в граничному випадку, коли зв'язок вихідних параметрів і станів об'єкта управління має однозначний і детермінований характер, управління за станами зводиться до управління за параметрами.

Згідно з викладеним, основними задачами для створення системи захисту інформації, побудованої за принципом керуючої системи, є:

- визначення цільового стану ОУ, що забезпечує необхідний рівень захисту інформації;
- синтез математичної моделі ОУ, здатної забезпечувати генерацію такого набору керованих факторів, що їх фактичний вплив на ОУ в циклі

управління з максимально можливою вірогідністю переведе його в заздалегідь заданий цільовий стан. При цьому модель повинна враховувати поточний стан ОУ і вплив наявних і прогнозованих неконтрольованих факторів середовища на поведінку ОУ;

– визначення достатнього набору вихідних параметрів ОУ для достовірної ідентифікації його станів. При цьому важливо знати їх імовірнісні характеристики (математичне очікування, кореляційну функцію та ін.) за якими можливо визначати крок квантування контрольованого параметра з урахуванням швидкості затухання інформаційних зав'язків, допустимих втрат інформації, запізнення і частоти послідовного контролю;
– синтез методу прийняття рішень, що забезпечує вибір керуючих дій в контурі управління спрямованих на оперативні локалізацію і нейтралізацію загроз.

Обґрунтування словника ознак для ідентифікації стану ІКМ. Ідентифікаційні ознаки об'єктів прийнято поділяти на детерміновані (логічні) і стохастичні (імовірнісні). Логічні ознаки можна розглядати як елементарні висловлювання, що приймають два значення істинності виду «так», «ні», або «істина» і «неправда» з повною визначеністю.

До числа імовірнісних відносяться ознаки, випадкові значення яких розподілені по всіх класах об'єктів, тому рішення про належність об'єкта до того чи іншого класу може прийматися тільки на основі конкретних значень ознак об'єкта.

Стани C_1 і C_2 ідентифікаційної ознаки не можуть бути достовірно передбачені заздалегідь, тому можна вважати, що вони відповідають гіпотезам H_1 і H_2 про знаходження ідентифікаційної ознаки у станах C_1 і C_2.

Таким чином, завданням є ототожнення кожної конкретної реалізації ідентифікаційної ознаки зі станом C_1 і C_2 ідентифікаційної ознаки, тобто встановлення істинності гіпотези H_1 і H_2.

У двоальтернативній ситуації прийняття рішень завжди супроводжується помилками першого і другого роду [6]:

– помилка першого роду (хибна тривога) — гіпотеза Н1 відкидається тоді, коли насправді вона вірна;
– помилка другого роду (пропуск цілі) — відкидається гіпотеза Н2 тоді, коли вона вірна.

Зазначені помилкові рішення характеризуються відповідно ймовірностями $P_{\text{пом.1}}$ і $P_{\text{пом.2}}$. Ухвалення правильних рішень про стани ідентифікаційної ознаки при знаходженні її в станах C_1 і C_2 характеризується відповідно ймовірностями $P_{\text{в1}}$ і $P_{\text{в2}}$, причому

$$P_{\text{в1}} + P_{\text{пом.1}} = 1 \quad (1)$$

$$P_{\text{в2}} + P_{\text{пом.2}} = 1 \quad (2)$$

оскільки можливі результати, що відповідають кожному із станів ідентифікаційної ознаки, становлять повну групу подій.

Завданням вирішального пристрою є виявлення одного із станів ідентифікаційної ознаки відповідно до введеного в вирішальний пристрій критерію K (правилом прийняття рішення). З двох гіпотез H_1 і H_2 вирішальний пристрій вибирає ту, яка в заданому сенсі краще. Як критерій прийняття рішення може бути обраний критерій «ідеального спостерігача» (критерій Котельникова), який є окремим випадком критерію мінімального середнього ризику Байєса. Зазначений критерій мінімізує можливість сумарної помилки прийняття рішення

$$P_{\text{пом.}} = P_a(\text{C}_1)\int_{U_n}^{\infty} f_1(U)dU + P_a(\text{C}_2)\int_{-\infty}^{U_n} f_2(U)dU \quad (3)$$

де $P_a(C_1)$ и $P_a(C_2)$ — апріорні ймовірності знаходження ідентифікаційної ознаки у станах C_1 та C_2 (присутня чи відсутня конкретна ознака на об'єкті); $f_1(U)$ і $f_2(U)$ — функції густин ймовірностей випадкових значень інформативної ознаки, що відповідають станам C_1 і C_2 ідентифікаційної ознаки (рис. 3); $U_п$ — поріг прийняття рішення вирішального пристрою.

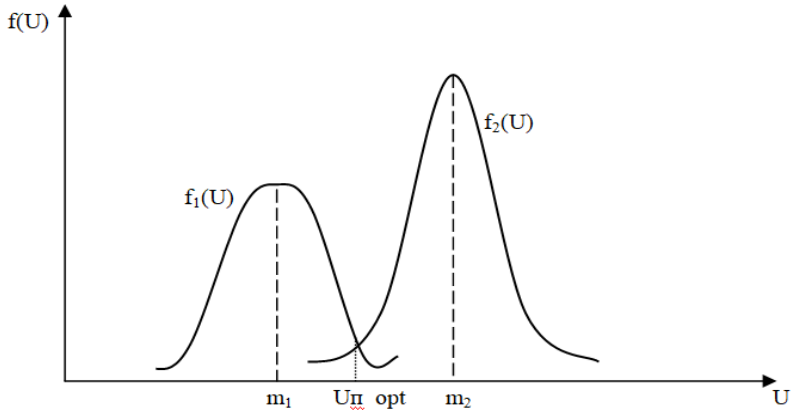


Рис. 3. Графіки умовних густин розподілу інформативної ознаки

Перевагою даного критерію є можливість роздільного обліку імовірностей помилок першого та другого роду, які визначаються виразами

$$P_{\text{пом.1}} = \int_{U_n}^{\infty} f_1(U)dU \quad (4)$$

$$P_{\text{пом.2}} = \int_{-\infty}^{U_n} f_2(U)dU \quad (5)$$

що є дуже важливим, оскільки у загальному випадку імовірності цих помилок можуть істотно відрізнятися. Окрім того, аналітичний вираз для критерію такий, що в нього можуть бути введені величини, які характеризують як параметри випадкових значень інформативної ознаки, так і основні параметри вирішального пристрою, що дозволяє зробити їх раціональний вибір і визначити точні характеристики, що забезпечують максимальну або задану достовірність результатів ідентифікації.

В якості ідентифікаційних ознак стану ІКМ для виявлення тривожних подій доцільно використовувати цифрові артефакти, які залишає шкідливе програмне забезпечення в результаті впливу та методи їх ідентифікації.

Для проведення повноцінного forensic-аналізу необхідно мати повний віртуальний образ диску та оперативної пам'яті досліджуваного комп'ютера, фізичний доступ до нього, а також мати достатню кваліфікацію та час на аналіз, що не завжди є можливим у корпоративному середовищі. Додатково до цього, корпоративні ПК мають невизначений термін підключення до мережі, а до аналітика зазвичай ставиться конкретний перелік питань, які не завжди потребують збору усіх наявних артефактів. У цьому випадку функціонал програм Forensic Triage (частковий збір артефактів з активного ПК) не є оптимальним для вирішення завдань аналітика [7].

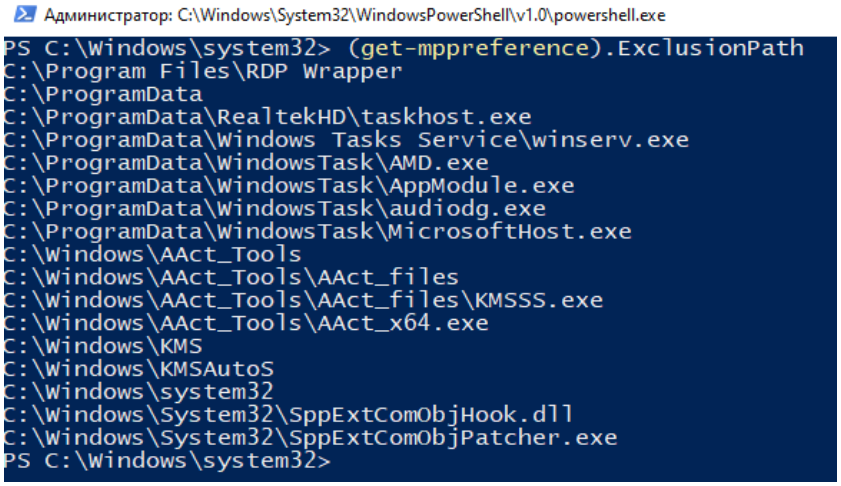
Викладене обумовлює необхідність пришвидшення збору необхідних артефактів з ОС Windows ІБ-спеціалістами та ІТ-адміністраторами для проведення Forensic Triage в умовах, де неможливо отримати повний віртуальний образ диску і оперативної пам'яті досліджуваного комп'ютера, або фізичного доступу до нього, на відміну від ситуацій, де у аналітика є вичерпний час на підключення до досліджуваного ПК [7].

Обґрунтування словника ознак, необхідних для виявлення тривожних подій, здійснено на прикладі характерних ознак, які після себе залишив наступний вірус:

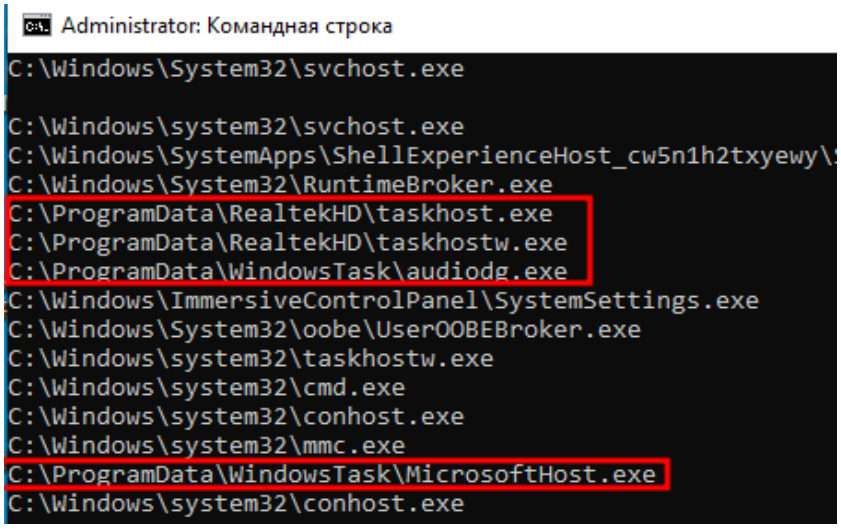
VT 60\72 Trojan[Packed]/Win64.Themida, Trojan[dropper]:Win/Tiggre, Trojan.Barys https://www.virustotal.com/gui/file/fa86dd3ccd8ca63f2fa214f43c4d90e09d9e108798952d855b75220e1f207592

Після запуску вірусу і залишення ПК «як є» впродовж 3-х годин, виявлено наступні сліди:

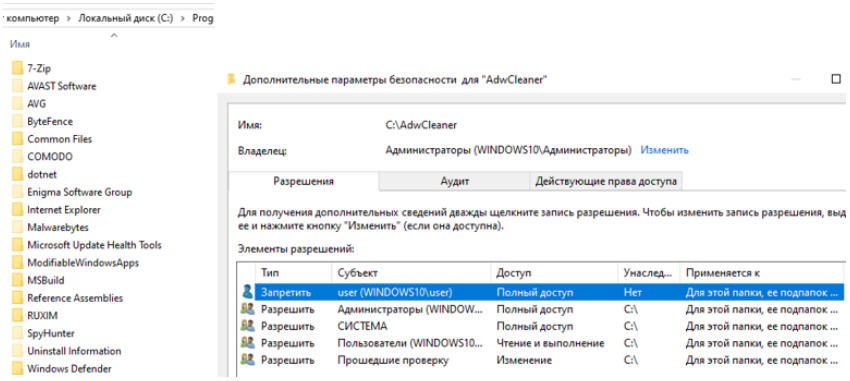
1. Інформація про вірусні файли\каталоги у списку виключень Windows Defender (Regedit – HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths
Powershell – (Get-MpPreference).ExclusionPath) [8].



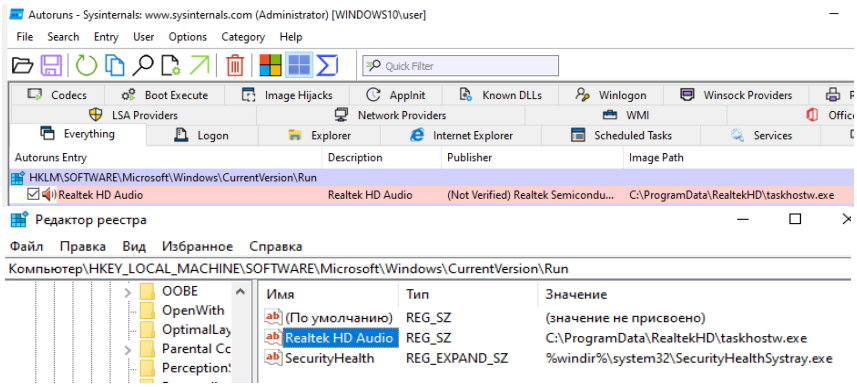
2. Список процесів, які не є легітимними (CMD — wmic process get ExecutionPath).



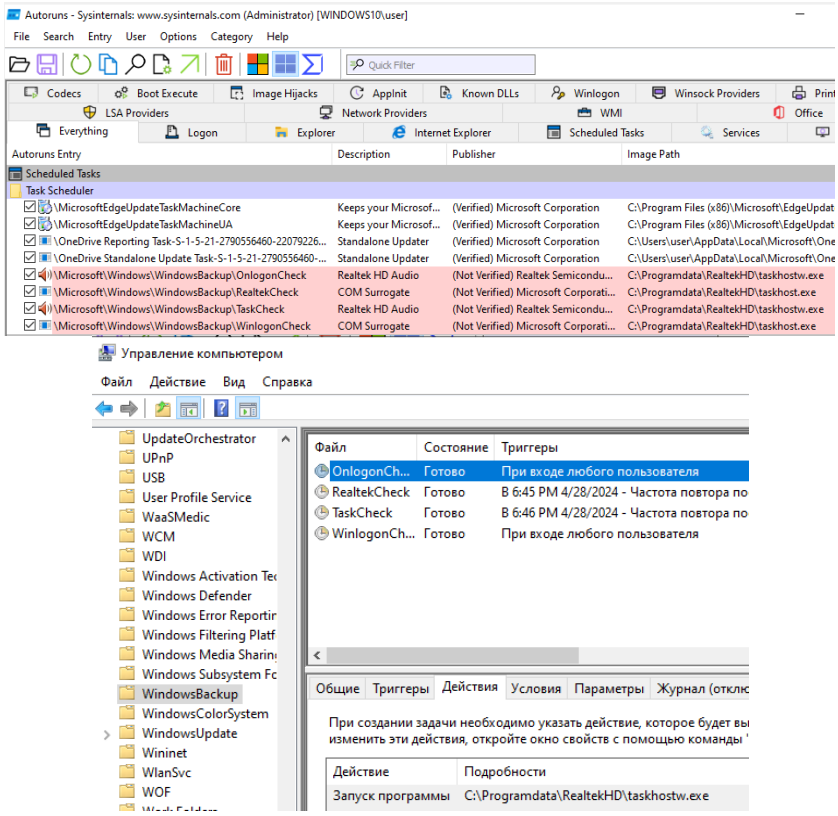
3. Сховані папки у каталозі програм, що мають назву таку ж як і у антивірусних рішень, при цьому, доступ до них заборонено користувачу який відкривав найперший вірусний файл, реалізовано це через Windows ACL [9].



4. Записи в ключі автозапуску Run, за допомогою утиліти Autoruns [10].

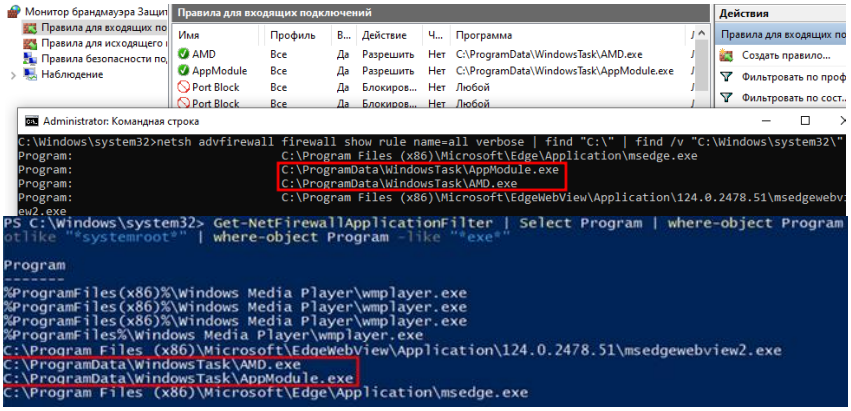


5. Записи в Windows TaskSheduller [11].

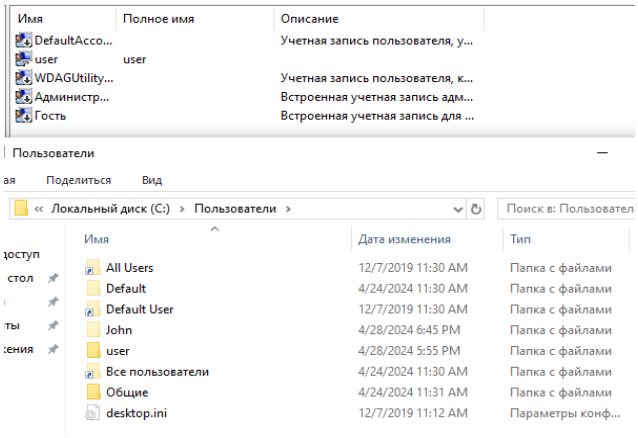


ISSN 2663 - 4023

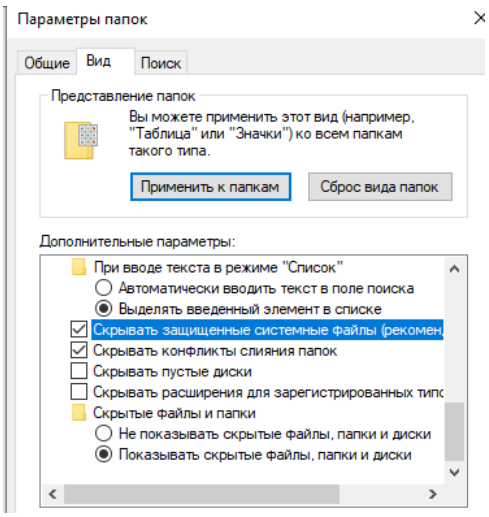
6. Записи в Windows Firewall (CMD – netsh advfirewall firewall show rule name=all verbose | find “C:\” | find /v “C:\Windows\system32\”
Powershell – Get-NetFirewallApplicationFilter | Select Program | Where-Object Program -notlike “*systemroot*” | Where-Object Program -like “*exe*”).



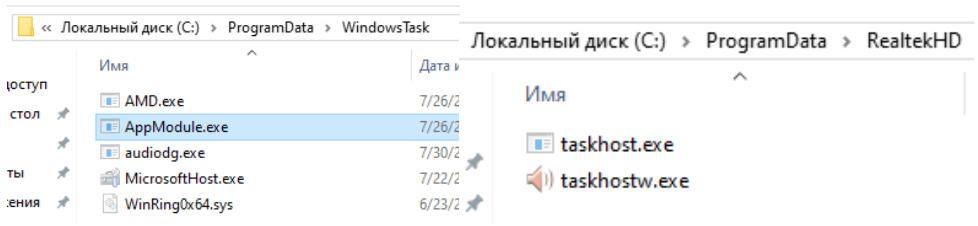
7. Створення нового схованого користувача “John”, при цьому самого користувача у списку користувачів – немає.



8. Додався прапорець «приховувати системні файли».



9. Вірусні файли мають атрибути «скритий та системний», мають іконку Realtek, мають таку ж назву як і у легітимних системних файлів (C:\Windows\System32\taskhostw.exe — системний процес для запуску запланованих завдань).



10. Вірус має функціонал anti-debugging, що проявляється у завершені процесу Диспетчера задач(taskmgr.exe) та при переході до вірусної папки будь-яким способом – завершені Провідника (explorer.exe).
11. Додатково можна зазначити, що частина вірусних файлів які ми бачимо у виключеннях антивірусу — не завантажилися.

Наприклад, файл winserv.exe це компонент Remote Utilities Server\Remote Manipulator System — легальний інструмент віддаленого адміністрування [12], [13]. Через наявний функціонал «налаштувати свій RMS-сервер» зазвичай використовується у різних ШПЗ в якості RAT(Remote Access Trojan\Remote Administration Tools) [13].

Наявні сліди, залишені після впливу ШПЗ на ПК, систематизовано в табл. 1.

Таблиця 1

Артефакти які залишились після впливу ШПЗ на ПК

	Які сліди залишаються	**Що може спричинити?**
Вірусні файли\каталоги у списку виключень Windows Defender	C:\Program Files\RDP Wrapper C:\ProgramData C:\ProgramData\RealtekHD\taskhost.exe C:\ProgramData\Windows Tasks Service\winserv.exe C:\ProgramData\WindowsTasks\AMD.exe C:\ProgramData\WindowsTasks\AppModule.exe C:\ProgramData\WindowsTasks\audiodg.exe C:\ProgramData\WindowsTasks\MicrosoftHost.exe C:\Windows\KMS C:\Windows\KMSAutoS C:\Windows\System32 C:\Windows\System32\SppExtComObjHook.dll C:\Windows\System32\SppExtComObjPatcher.exe	Неможливість для АВ самостійно видалити віруси
Список вірусних процесів у пам’яті	C:\ProgramData\RealtekHD\taskhost.exe C:\ProgramData\RealtekHD\taskhostw.exe C:\ProgramData\WindowsTasks\audiodg.exe C:\ProgramData\WindowsTasks\MicrosoftHost.exe	Доки вірус запущено(знаходиться у пам’яті) — він виконує потрібні зловмиснику дії.
Сховані папки у каталозі програм, що мають назву таку ж, як і у антивірусних рішень	Папки та файли з атрибутами «приховані» і «системні» в каталогах C:\Program Files, доступ до яких заборонено користувачу, що запустив вірус: AWAST Software AVG ByteFence COMODO Enigma Software Group Malwarebytes SpyHunter	Неможливість встановити альтернативні антивірусні рішення

Додаткові користувачі на ПК	User: John User Profile: C:\Users\John	Додаткові користувачі, яких створює вірус, будуть мати права Administrators\Remote Desktop Users, що дозволить отримати віддалений доступ до ПК з правами адміністратора
Зміна налаштувань Windows ACL	Папки та файли з атрибутами «приховані» і «системні» в каталогах C:\Program Files Icacls C:\Program Files\	Недоступність легітимних користувачів до папок\файлів, неможливість їх видалити\перейменувати, повний доступ до папок і файлів для нелегітимних користувачів навіть при відсутності додавання в адміністративні групи
Додавання в автозапуск реестра	HKLM\Software\Microsoft\Windows\CurrentVersion\Run «Realtek HD Audio» C:\ProgramData\RealtekHD\taskhostw.exe	Завантаження вірусних файлів при перезавантаженні ПК, їх персистентність
Додавання в автозапуск TaskSheduller	TaskSheduller - \Microsoft\Windows\WindowsBackup\OnlogonCheck C:\ProgramData\RealtekHD\taskhostw.exe \Microsoft\Windows\WindowsBackup\RealtekCheckC:\ProgramData\RealtekHD\taskhost.exe \Microsoft\Windows\WindowsBackup\TaskCheck C:\ProgramData\RealtekHD\taskhostw.exe \Microsoft\Windows\WindowsBackup\WinlogonCheck C:\ProgramData\RealtekHD\taskhost.exe	Завантаження вірусних файлів при окремих подіях
Вірусні файли\каталоги у списку виключень Windows Firewall	C:\ProgramData\WindowsTasks\AMD.exe C:\ProgramData\WindowsTasks\AppModule.exe	Безперешкодний доступ до інтернету для вірусних файлів, без додаткового повідомлення користувача
Приховано від користувача приховані файли	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL CheckedValue 1 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced «Hidden 1», «HideFileExt 1»	Навіть якщо у користувача до цього було увімкнено показ прихованих файлів — вірус сховає вірусні файли від користувача
Приховано від користувача вірусні файли та папки	Папки та файли з атрибутами «приховані» і «системні» в каталогах C:\Program Files, C:\ProgramData\RealtekHD, C:\ProgramData\WindowsTasks (файл з вразливим драйвером WinRing0x64.sys окремо до виключень не додавався)	Користувач не може побачити нові невідомі файли та насторожитися

В якості ідентифікаційних ознак стану ІКМ вибрано артефакти, подані в табл. 2.

Таблиця 2

Артефакти для ідентифікації стану ІКМ

Артефакт	Що може спричинити?	Де сліди залишаються\як їх вивантажити	Яку інформацію можна отримати зі слідів?
Вірусні файли\каталоги у списку виключень Windows Defender	Неможливість для АВ самостійно знайти та видалити віруси	Regedit HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes Powershell — (Get-MpPreference).ExclusionPath)	Усі можливі варіанти шляхів і файлів в якому знаходяться віруси (100% вірусна активність за наявності якихось записів)
Список вірусних процесів у пам'яті	Доки вірус запущено (знаходиться у пам'яті) — він виконує потрібні зловмиснику дії. Являється основним індикатором компрометації	wmic process get ExecutionPath	Повний шлях до вірусного файлу (100% вірусна активність за наявності аномалії у назві процесу і стандартному шляху де він повинен зберігатися)
Додаткові користувачі на ПК	Додаткові користувачі які створює вірус, будуть мати права Administrators\Remote Desktop Users, що дозволить отримати віддалений доступ до ПК з правами адміністратора	wmic useraccount where localaccount=true get name,sid,disabled Registry HKEY_LOCAL_MACHINE\SAM HKEY_LOCAL_MACHINE\SECURITY	Усі користувачі чий SID закінчується на -1000 (і вище) — додатковий користувач. Може свідчити про наявність вірусної активності
Сховані папки у каталозі програм, що мають назву таку ж як і у антивірусних рішень	Неможливість встановити альтернативні антивірусні рішення для видалення вірусів	C:\Program Files\	На комп'ютері 100% вірусна активність, яка має модуль захисту від антивірусів
Зміна налаштувань Windows ACL	Недоступність легітимних користувачів до папок\файлів, неможливість повного доступу до папок і файлів для нелегітимних користувачів навіть за відсутності додавання в адміністративні групи	Icacls C:\ Icacls "C:\Program Files\"	Які користувачі є нелегітимними. 100% вірусна активність
Додавання в автозапуск реєстру	Завантаження вірусних файлів при перезавантаженні ПК	HKLM\Software\Microsoft\Windows\CurrentVersion\Run HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	Перелік файлів, які критичні для функціонування і персистентності вірусу, за наявності невідомих файлів — 100% вірусна активність

		HKLM\SYSTEM\CurrentControlSet\Services HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree	
Додавання в автозапуск TaskSheduller	Завантаження вірусних файлів при окремих подіях	TaskSheduller HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule	Перелік файлів, які критичні для функціонування і персистентності вірусу, за наявності невідомих завдань — 100% вірусна активність
Вірусні файли\каталоги у списку виключень Windows Firewall	Безперешкодний доступ віруса до інтернету без додаткового запиту користувача	CMD — netsh advfirewall firewall show rule name=all verbose | find “C:\” | find /v “C:\Windows\system32\” HKLM\Software\Policies\Microsoft\WindowsFirewall\FirewallRules	Перелік вірусних файлів, яким необхідне інтернет-з’єднання, якщо є якісь файли з тимчасової папки користувача це 100% вірусна активність
Приховано від користувача приховані файли	Навіть якщо у користувача до цього було увімкнено показ прихованих файлів, вірус сховає вірусні файли від користувача, що робиться для того щоб користувач не побачив вірусні файли у каталогах	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\Hidden\SHOWALL CheckedValue 1 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced «Hidden 1», «HideFileExt 1» dir C:\ /A:HS	Частина вірусних файлів містить атрибути «прихований» та «системний», майже всі файли з такими атрибутами, що не знаходяться в системних папках — будуть свідчити про наявність вірусу
Prefetch	-	C:\Windows\Prefetch	Назву будь-коли запущеного .exe файлу та час коли він запускався
AppCompat Cache	-	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache\	Інформацію про запущені файли на ПК та повний шлях до них
Amcache	-	%SystemRoot%\AppCompat\Programs\Amcache.hve	Інформацію про запущені файли та час їх запуску
SRUM	-	C:\Windows\System32\sru\SRUDB.dat	Інформацію про запущені програми (з повним шляхом) конкретним користувачем (містить назву та SID) та у конкретний час
ShellBags	-	%UserProfile%\NTUSER.DAT HKCU\Software\Microsoft\Windows\Shell %UserProfile%\USRCLASS.DAT HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell	Інформацію про запущені команди конкретним користувачем через Win+R та час виконання, може містити шкідливі команди
Інформація про .zip .rar .exe .dll в каталогах користувача	-	Dir %userprofile% /r /s	Назву і шлях до виконуваних файлів, які є у користувача, що іноді може показати, який користувач завантажив і відкрив ШПЗ

Завдання оператора ідентифікації стану ІКМ, вирішення яких необхідне для прийняття рішень в циклах управління системи захисту інформації, подано на рис. 4.

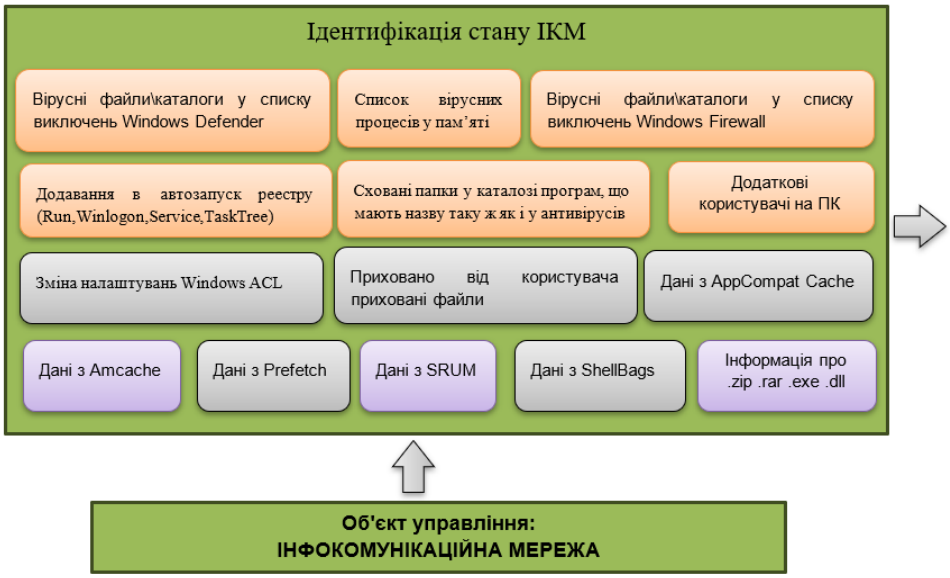


Рис. 4. Завдання оператора ідентифікації стану ІКМ

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Побудова системи захисту інформації у вигляді автоматизованої системи управління, спрямованої на забезпечення підтримки цільового стану ІКМ, дозволяє забезпечити необхідний рівень захищеності інформації.

Зазначений словник ознак для ідентифікації стану ІКМ є достатнім для прийняття рішень в циклах управління системи захисту інформації.

Практичне значення отриманих результатів полягає у можливості їх застосування в різних галузях для вдосконалення методів захисту інформації від впливу комп'ютерних вірусів і більш ефективного використання часу аналітика при проведенні Forensic-аналізу ІКМ.

Перспективні напрямки досліджень:

– вдосконалення методів вивантаження цифрових артефактів з урахуванням типових завдань для аналітика інформаційної безпеки в корпоративному середовищі;
– синтез методу прийняття рішень, що забезпечує вибір керуючих дій в контурі управління, спрямованих на оперативні локалізацію і нейтралізацію загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Vasylenko, M. D., Rachuk, V. O., & Slatvinska, V. M. (2021). Malware in the Context of Understanding Computer Virology and Technical and Legal Competition: An Interdisciplinary Study [Malware in the context of understanding computer virology and techno-legal adversarialism: an interdisciplinary study]. *Naukovi pratsi Natsionalnoho universytetu "Odeska yurydychna akademiia" – Scientific works of the National University "Odesa Law Academy", 28*, 28–36.

2. Rychka, D.O. (2018). Computer viruses - malicious software, the driving force of modification [Computer viruses are malicious software, the driving force of modification]. *Scientific Bulletin of Kherson State University. Series "Legal Sciences", 1(2),* 89–93.
3. Bashir, M., & Khan, M. (2013). Triage in Live Digital Forensic Analysis. *The International Journal of Forensic Computer Science, 8(1),* 35–44. https://doi.org/10.5769/j201301005
4. Kao, D.-Y. & Wu, G.-J. (2015). A Digital Triage Forensics framework of Window malware forensic toolkit: Based on ISO/IEC 27037:2012. *2015 International Carnahan Conference on Security Technology (ICCST),* 217–222. https://doi.org/10.1109/CCST.2015.7389685
5. Kriuchkova, L. P. (2016). *Problems of functioning of infocommunication networks in the conditions of destructive influences. Monograph.* K.: DUT.
6. Vasyliev, V. M., & Zhuk, S. Ya.. (2023). *Probability theory in radio engineering: a textbook.* Kyiv: Publishing House "Polytechnic".
7. Bohdanov, O., & Chernihivskyi, I. (2024). Types of digital forensic artifacts in windows computers. *Cybersecurity: Education, Science, Technique. 2024, 4(24),* 221–228. https://doi.org/10.28925/2663-4023.2024.24.221228
8. *Get-MpPreference (Defender).* (n. d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/powershell/module/defender/get-mppreference?view=windowsserver2022-ps
9. *Access Control: Understanding Windows File And Registry Permissions.* (n. d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/archive/msdn-magazine/2008/november/access-control-understanding-windows-file-and-registry-permissions
10. *Autoruns - Sysinternals.* (n. d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
11. *Scheduled Task Tampering.* (n. d.). WithSecure™ Labs Home | WithSecure™ Labs. https://labs.withsecure.com/publications/scheduled-task-tampering
12. *Automated Malware Analysis Report for winserv.exe - Generated by Joe Sandbox.* (n. d.). Automated Malware Analysis - Joe Sandbox Cloud Basic. https://www.joesandbox.com/analysis/844004/0/html
13. *RemoteUtilities.* (n. d.). Software S0592 | MITRE ATT&CK®. MITRE ATT&CK®. https://attack.mitre.org/software/S0592/

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Ivan Chernihivskyi
Graduate Student
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0009-0003-4568-3212
i.chernihivskiy@gmail.com

Larysa Kriuchkova
Doctor of Technical Sciences, Professor
Professor of the Volodymyr Buriachok Department of Information and Cyber Security
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-8509-6659
l.kriuchkova@kubg.edu.ua

SYSTEMATIC APPROACH TO SOLVING THE TASK OF PROTECTING INFORMATION IN THE INFOCOMMUNICATION NETWORK FROM THE INFLUENCE OF COMPUTER VIRUSES

Abstract. A modern infocommunication network is a distributed system, the basic elements of which are combined into a single information space. The task of ensuring the high-quality functioning of infocommunication networks under the influence of computer viruses necessitates the need to monitor the network status for timely detection of alarming events, which are understood as the detection of signs of infection of network hardware. It is obvious that to achieve the required level of information security in the network, correct and timely management decisions must be provided to prevent undesirable consequences. This necessitates the creation of more advanced methods of protecting information from the influence of computer viruses on network hardware. The purpose of the publication is to form a systematic approach to solving the tasks of protecting information in the infocommunication network from the influence of computer viruses with the justification of the dictionary of signs necessary for detecting alarming events, and ensuring the maintenance of the target state of the infocommunication network. The main scientific and technical tasks for creating an information protection system against the influence of computer viruses, built on the principle of a control system, are substantiated. It is proposed to use digital artifacts that leave malicious software as a result of the impact as identification signs of the state of the infocommunication network to detect alarming events. The possibility of using forensic analysis with an incomplete set of digital artifacts is considered. Universal artifacts are identified, the detection of which indicates one hundred percent infection. Building an information protection system in the form of an automated control system aimed at ensuring the support of the target state of the infocommunication network allows ensuring the required level of information security. The specified dictionary of signs for identifying the state of the infocommunication network is sufficient for making decisions in the control cycles of the information protection system. The practical significance of the results obtained lies in the possibility of their application in various industries to improve methods of protecting information against the influence of computer viruses and more efficient use of the analyst's time when conducting forensic analysis of the infocommunication network.

Keywords: information; cybersecurity; viruses; protection; identification features; detection of alarming events; information protection; infocommunication networks.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Vasylenko, M. D., Rachuk, V. O., & Slatvinska, V. M. (2021). Malware in the Context of Understanding Computer Virology and Technical and Legal Competition: An Interdisciplinary Study [Malware in the context of understanding computer virology and techno-legal adversarialism: an interdisciplinary study]. *Naukovi pratsi Natsionalnoho universytetu "Odeska yurydychna akademiia" – Scientific works of the National University "Odesa Law Academy", 28,* 28–36.

2. Rychka, D.O. (2018). Computer viruses - malicious software, the driving force of modification [Computer viruses are malicious software, the driving force of modification]. *Scientific Bulletin of Kherson State University. Series "Legal Sciences", 1(2),* 89–93.
3. Bashir, M., & Khan, M. (2013). Triage in Live Digital Forensic Analysis. *The International Journal of Forensic Computer Science, 8(1),* 35–44. https://doi.org/10.5769/j201301005
4. Kao, D.-Y. & Wu, G.-J. (2015). A Digital Triage Forensics framework of Window malware forensic toolkit: Based on ISO/IEC 27037:2012. *2015 International Carnahan Conference on Security Technology (ICCST)*, 217–222. https://doi.org/10.1109/CCST.2015.7389685
5. Kriuchkova, L. P. (2016). *Problems of functioning of infocommunication networks in the conditions of destructive influences. Monograph.* K.: DUT.
6. Vasyliev, V. M., & Zhuk, S. Ya.. (2023). *Probability theory in radio engineering: a textbook.* Kyiv: Publishing House "Polytechnic".
7. Bohdanov, O., & Chernihivskyi, I. (2024). Types of digital forensic artifacts in windows computers. *Cybersecurity: Education, Science, Technique. 2024, 4(24),* 221–228. https://doi.org/10.28925/2663-4023.2024.24.221228
8. *Get-MpPreference (Defender).* (n. d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/powershell/module/defender/get-mppreference?view=windowsserver2022-ps
9. *Access Control: Understanding Windows File And Registry Permissions.* (n. d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/archive/msdn-magazine/2008/november/access-control-understanding-windows-file-and-registry-permissions
10. *Autoruns - Sysinternals.* (n. d.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns
11. *Scheduled Task Tampering.* (n. d.). WithSecure™ Labs Home | WithSecure™ Labs. https://labs.withsecure.com/publications/scheduled-task-tampering
12. *Automated Malware Analysis Report for winserv.exe - Generated by Joe Sandbox.* (n. d.). Automated Malware Analysis - Joe Sandbox Cloud Basic. https://www.joesandbox.com/analysis/844004/0/html
13. *RemoteUtilities.* (n. d.). Software S0592 | MITRE ATT&CK®. MITRE ATT&CK®. https://attack.mitre.org/software/S0592/