УДК 004.056

Куцаєв В.В. (ВІТІ) ORCID – 0000-0001-8213-4739
Штонда Р.М. (ВІТІ) ORCID – 0000-0001-5986-0847
Терещенко Т.П. (ВІТІ) ORCID – 0000-0002-9659-7897
Артемчук М.В. (ВІТІ) ORCID – 0000-0003-4640-9429
Нещерет І.Г. (в/ч А0105) ORCID – 0000-0002-3500-5683

АЛГРИТМ БЛОКУВАННЯ ВІРУСУ ШИФРУВАЛЬНИКА В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

В статті запропоновано алгоритм дій адміністратора системи для протидії спробам несанкціонованого шифрування інформації в інформаційно-телекомунікаційній системі.

На актуальність розробки таких заходів вказує те, що кількість атак шифрувальників досягає 30 відсотків від загальної кількості кібернетичних інцидентів у світі. Масовані атаки відбуваються кожного півроку, а техніки проникнення до системи та алгоритми шифрування постійно покращуються. Згідно моделі Cyber-Kill Chain зловмисники вдало досягають встановленої мети на цільовій машині.

Метою заходів для нейтралізації несанкціонованого шифрування інформації в системі є блокування його дії на початку роботи.

Автори пропонують завчасно розгортати в інформаційно-телекомунікаційній системі зразки програмного забезпечення, які дозволять своєчасно виявити ознаки початку несанкціонованого шифрування інформації в системи.

Заходи передбачають завчасне розміщення в системі зразків спеціального програмного забезпечення, які здатні реалізувати «постійний програмний моніторинг» за процесами в системі, здійснити при зупинку процесора при виявленні ознак шифрування, а саме: при перевантаженні процесора, при виявленні підозрілих процесів, при виявленні ознак дії алгоритму шифрування, при синхронному зникненні важливих файлів, при спробі несанкціонованого перезавантаження системи та інших ознаках. Автори порівнюють кіберзахищеність системи без застосування запропонованих заходів та з ними. Автори вважають, що кіберзахищеність системи зросте до 0,99 в залежності від ефективності заходів задіяних.

Висновком статті є те, що завчасне розміщення спеціалізованих програмних засобів в системі дозволить своєчасно заблокувати дію вірусу шифрувальника та підвищити захищеність системи.

Подальші напрямки досліджень дозволять поширювати запропоновані заходи для нейтралізації дій різних класів кібернетичних атак, які досягли згідно моделі Cyber-Kill Chain цільової машини.

Ключові слова: *вірус-шифрувальник, кібератака, кіберзахищеність, Cyber Kill Chain, інформаційно-телекомунікаційна система.*

Куцаев В.В., Штонда Р.М., Терещенко Т.П., Артемчук М.В., Нещерет И.Г. Перечень действий для блокировки вируса шифровальщика в информационно-телекоммуникационных системах.

В статье предложен алгоритм действий администратора системы направленный на противодействиее попыткам несанкционированного шифрования информации в информационно-телекоммуникационной системе в условиях кибератаки зловредным программным обеспечением типа вирус шифровальщик.

На актуальность разработки таких действий указывают выводы мировых кибер - специалистов. Они указывают, что количество атак вируса шифровальщика достигает до 30 процентов от общего количества кибернетических инцидентов в мире. Массированные атаки происходят каждые пол год, а техники проникновения в информационно-телекоммуникационные системы и алгоритмы шифрования постоянно совершенствуются. Согласно модели Cyber-Kill Chain злоумышленники успешно достигают поставленной задачи на целевой машине в выбранной сети.

Целью действий направленных на нейтрализацию несанкционированного шифрования информации в системе это блокирование начала работы вируса шифровальщика или нейтрализация его действий в самом начале роботы.

Авторы предлагают заранее установить в системе образцы специального программного обеспечения, которые позволят своевременно обнаруживать признаки начала несанкционированного шифрования информации.

Авторы сравнивают киберзащищенность системы без использования предложенных мер защиты системы от шифрования и с ними. Авторы считают, что киберзащищенность системы увеличится до 0,99 в зависимости от эффективности мер задействованных для блокирования работы вируса шифровальщика.

Выводы статьи заключаются в том, что заблаговременная разработка и размещение специальных программных средств в системе позволит своевременно заблокировать действие вируса шифровальщика и усилить защищенность системы от действий вируса шифровальщика до удовлетворительного уровня.

Дальнейшим направлением исследований станет использование предложенных мер на нейтрализацию

работы других классов кибернетических атак, которые достигли целевой машины согласно модели Cyber-Kill Chain.

Ключевые слова: *вирус-шифровальщик, кибератака, киберзащищенность, Cyber Kill Chain, информационно-телекоммуникационной система.*

V. Kytsayev, R. Shtonda, T. Terestchenko, M.Artemtchuk, I. Neshcheret List of actions to block the cryptographer virus in information and telecommunications systems.

The article proposes an algorithm of actions of the system administrator to counteract attempts of unauthorized encryption of information in the information and telecommunication system.

The urgency of developing such measures is indicated by the fact that the number of encryption attacks reaches 30 percent of the total number of cyber incidents in the world. Massive attacks occur every six months, and intrusion techniques and encryption algorithms are constantly being improved. According to the Cyber-Kill Chain model, attackers successfully achieve the set goal on the target machine.

The purpose of measures to neutralize unauthorized encryption of information in the system is to block its action at the beginning of work.

The authors propose to deploy software samples in advance in the information and telecommunication system, which will allow to detect in time the signs of the beginning of unauthorized encryption of information in the system.

Measures include early placement in the system of samples of special software that are able to implement "continuous software monitoring" of processes in the system, to perform when the processor stops when detecting signs of encryption, namely: when overloading the processor, detecting suspicious processes, detecting signs of algorithm encryption, in case of simultaneous disappearance of important files, in case of attempt of unauthorized reboot of the system and other signs. The authors compare the cybersecurity of the system without applying the proposed measures and with them. The authors believe that the cybersecurity of the system will increase to 0.99 depending on the effectiveness of the measures involved.

The conclusion of the article is that the early placement of specialized software in the system will timely block the action of the encryptor virus and increase the security of the system.

Further research will allow to disseminate the proposed measures to neutralize the actions of different classes of cyber attacks that have reached the target machine according to the Cyber-Kill Chain model.

Key words: encrypting virus, technique, cyberattack, cybersecurity, Cyber Kill Chain, information and telecommunication system.

Постановка завдань в загальному вигляді. Основні світові аналітики визнають, що 30 відсотків сучасних кіберзагроз становлять спроби шифрування інформації в системі з подальшою вимогою надати викуп за можливість її відновлення.

Відома розширена модель проведення атаки Cyber-Kill Chain [1] визначає кроки, які реалізує зловмисник для досягнення можливості виконати несанкціоновані дії на кінцевих точках у визначених ним мережах. При цьому зловмисник реалізує наступні кроки:

1. Кроки зовнішньої Cyber-Kill Chain:
зовнішня розвідка мережі;
озброєння – вибір інструментів;
доставка шкідливого програмного забезпечення (далі – ШПЗ);
зовнішнє зараження;
встановлення ШПЗ;
досягнення можливості управління;
дії в мережі.
2. Кроки внутрішньої Cyber-Kill Chain:
внутрішня розвідка в мережі;
озброєння – вибір інструментів;
доставка ШПЗ;
внутрішнє зараження;
підвищення прав;
горизонтальне переміщення;
маніпуляції з цільовою машиною.
3. Cyber-Kill Chain маніпуляції з цільовою машиною:
розвідка цілі;
зараження цілі;
озброєння інструментами;
встановлення ШПЗ;
досягнення цілі зловмисника.

На рис. 1 вказано ланцюжок дій зловмисників згідно моделі Cyber-Kill Chain необхідних для досягнення зловмисником можливості виконання мети на кінцевій машині.

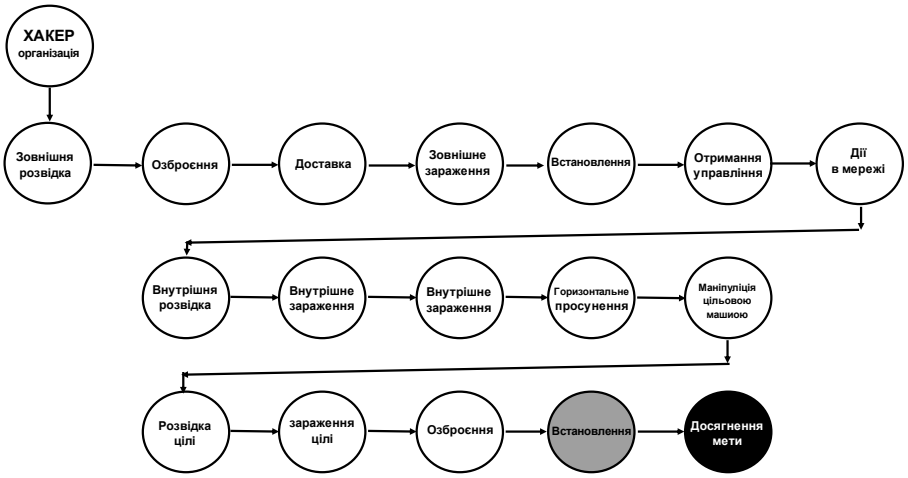

Рис. 1 Ланцюжок дій, які реалізує зловмисник згідно моделі Cyber-Kill Chain

Експерти вважають що зловмисники досконало відпрацьовують всі кроки ланцюжка моделі Cyber-Kill Chain необхідні для вдалого вторгнення до цільової машини та потім успішно виконують заплановані шкідливі дії на цільовий машині. На кожному етапі моделі Cyber-Kill Chain застосовуються необхідні заходи кіберзахисту, але зловмисники постійно та впевнено долають цій захист. Тому автори пропонують зосередити зусилля захисту від кібервпливу на останніх етапах встановлення та початку дії вірусу шифрувальника. На рис. 2 вказано місце дії заходів кіберзахисту в ланцюжку моделі Cyber-Kill Chain, які будуть запропоновані для протидії роботі вірусу шифрувальнику.

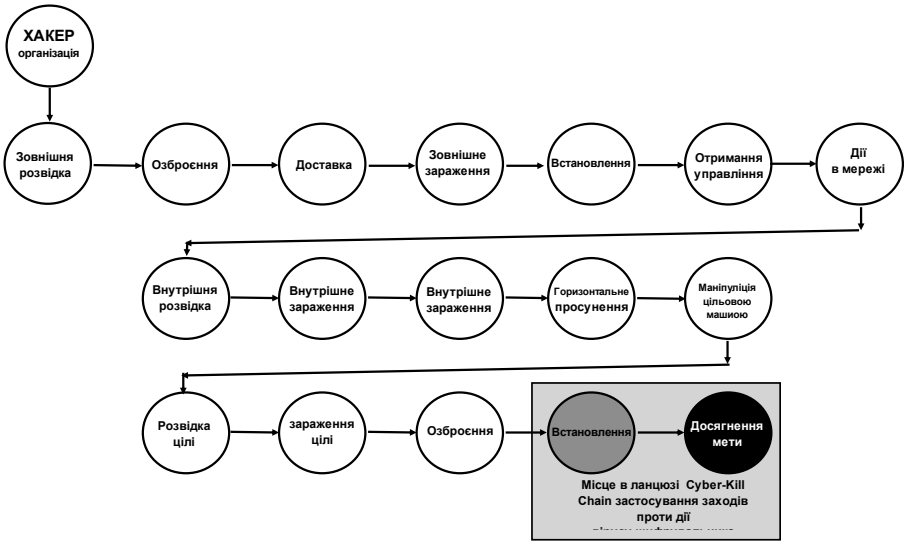

Рис. 2 Місце впливу запропонованих заходів протидії вірусу шифрувальнику в ланцюжку моделі Cyber-Kill Chain

Вірус шифрувальник (далі – ВШ), це програмне забезпечення, яке здатне непомітно проникати в інформаційно-телекомунікаційну систему (далі – ІТС) та шифрувати важливу інформацію, блокуючи роботу ІТС. Після цього зловмисники, які оперують ВШ вимагають власників системи заплатити викуп.

Наприклад на екранах в ІТС з'являється напис „Ваші файли зашифровані. Щоб отримати ключ для розшифрування, терміново переведіть деяку визначену суму коштів ”[2].

Вірус може потрапити у комп'ютер з прикріпленого до електронного листа документу Word або з оновлення додатку, наприклад бухгалтерського M.E.doc.

При відкритті такого документу завантажуєтеся прихований шкідливий файл, який, в свою чергу, використовується в якості завантажувача основного функціоналу ВШ. Найвідомішим в Україні прикладом ВШ стали віруси WannaCry та Petya.A [3].

Надалі в планувальнику задач встановлюється команда на перезавантаження системи, а після перезавантаження на інфікованому комп'ютері починає виконуватися шкідливий код ВШ. Потім вірус шифрує значну частину призначених для користувача файлів: фотографії, музичні файли, відео файли, текстові документи, архіви, електронну пошту, бази даних та файли з розширенням, які виконуються.

Кілька років тому атакам вірусів цього класу піддавалися тільки комп'ютери на базі операційної системи Windows. Сьогодні їх ареал розширився до таких операційних систем, як Linux, Mac і Android. Після WannaCry з'явилися не менш витончені Petya.A, Alkatraz Locker, CrySIS, Globe, NoobCrypt, Bad Rabbit та багато інших [4].

Актуальність. У 2013-2017 роках кібератаки проти України здійснювалися з використанням APT-атак (Snake, Uroboros, Sofacy/APT28, Epic Turla, Black Energy 2 і 3, Arma-geddon та інші), характерних саме для України. Перші системні атаки були зафіксовані у травні 2014 року на об'єкти критичної інформаційної інфраструктури України (Укрзалізницю та сервери Центральної виборчої комісії під час проведення президентських виборів).

Також відбулися кібератаки на енергетичний сектор: у грудні 2015 року – на ПАТ „Прикарпаття обленерго" і ПАТ "Київ обленерго"; у грудні 2016 року – на компанію „Укренерго" (споживачі частини правого берега Києва та прилеглих районів області залишилися без струму).

У червні 2017 року об'єкти критичної інфраструктури України зазнали масштабної атаки комп'ютерного вірусу Petya.A.

Тому існує необхідність створення заходів для протидії ВШ.

Важливість створення таких заходів полягає в тому, що спостерігається постійне просування нових зразків вірусу шифрувальника типу Petya.A по всьому світу та нажаль до низки мереж українських державних і приватних установ, зокрема, сайту Кабінету Міністрів України і ряду інших міністерств, а саме пенсійного фонду, Київської міської державної адміністрації, низки банків, крупних державних і приватних підприємств тощо.

Аналіз останніх досліджень і публікацій.

Складність захисту від дій ВШ потребує створення динамічних систем захисту здатних заздалегідь перехоплювати вірус або блокувати його роботу на початку, коли інформацію системи ще можливо зберегти.

Питання кіберзахисту ІТС та їх складових знайшли своє відображення у розробці наукових підходів та математичного апарату в роботах багатьох дослідників, для прикладу взяті джерела [6 – 9], а нижче коротко наведені їх особливості.

В запропонованій авторами [5] методиці оцінки ризиків в ІТС оцінка захищеності від вірусів досягається шляхом виконання трьох етапів.

На першому етапі розраховуються методики для об'єктів, графіків атак (критичність, значимість, складність доступу, реалізація загрози).

На другому етапі на основі розрахунків, виконаних на першому етапі, розраховується кількісний рівень для загроз, які аналізуються.

На останньому етапі на основі рівнів загроз визначається підсумковий рівень безпеки ІТС.

В наведеній методиці не запропоновано порівняння ризиків для ІТС без застосування упереджуючих заходів та при застосуванні заходів, які здатні блокувати початок шифрування.

У тезах статті [6] приведено алгоритм протидії автоматизованим засобам соціальної інженерії, завдяки яким можливо унеможливити впровадженню ВШ та його блокування на етапі його втручання в систему.

Алгоритм в поєднанні з методиками менеджменту ризиків та вразливостей ІТС декларується, як корисний інструмент для підвищення рівня інформаційної безпеки ІТС у цілому.

На думку авторів, алгоритм не є вирішенням всіх можливих проблем інформаційної безпеки ІТС, особливо від дії ВШ тому що він не дає можливості заздалегідь заблокувати всі напрямки зараження, виявити техніку приховування тіла вірусу шифрувальника та заблокувати процес шифрування.

У дослідженні [7] запропоновано кортежну модель базових параметрів оцінювання негативних наслідків блокування ІТС від кібератак на дану ІТС.

В контексті дослідження шляхів чи напрямків кібернетичного захисту модель має сенс, але не відповідає потребі покращення захисту від ВШ на окрему ІТС.

Метод реєстрацій аномалій в ІТС на основі контрольних карт Шухарта, як і будь-який статистичний метод виявлення аномалій [8] в ІТС та запобігання вторгненням при кіберзахисті об’єкту, має недолік пов’язаний з необхідністю набору статистики даних про значення параметру відносно якого проводиться аналіз стану кіберзахищеності ІТС. Використання контрольних карт Шухарта вимагає попереднього визначення середніх значень та контрольних границь параметру, що досліджуються.

Недоліком роботи [8] є те, що для адекватного виявлення аномалій, які викликані кібератаками типу ВШ, середні значення контрольних границь під час функціонування повинні щоразу переглядатись, що вимагає додаткових ресурсів часу та авторами вважається важко досяжними.

В такому випадку значно ускладняється процес оперативного впливу на кіберзахищеність ІТС від дій ВШ.

Сучасні практичні рекомендації та інструкції для протидії спробам шифрування інформації в системі та заходів для її відновлення.

На даний час деякі інструкції та алгоритми дій адміністраторів при перших ознаках роботи ВШ, таких як перезавантаження ІТС, подальше блокування ІТС, банер з умовами зловмисників та інші рекомендують негайно вимкнути живлення комп’ютера натисканням і утриманням кнопки Power протягом 3-4 секунд.

Це дозволяє врятувати хоча б частину файлів або не врятувати нічого, тому що можливо процес шифрування вже закінчено, а ключова інформація надійно знищена. Надалі рекомендовано створити на іншому комп’ютері завантажувальний диск або USB-флеш з антивірусною програмою.

Наприклад LiveDisk, ESET NOD32, LiveCD і т.ін.. Завантажити комп’ютер, який піддався дії вірусу шифрувальника з цього диска та просканувати систему. Видалити знайдене шкідливе програмне забезпечення зі збереженням в карантин (на випадок, якщо вони знадобляться для розшифрування) [9].

Спробувати відновити зашифровані файли з тіньових копій засобами системи або за допомогою сторонніх додатків призначених для відновлення даних.

Більшість сучасних інструкцій не рекомендують платити викуп, тому що оплата не гарантує отримання ключів для розшифрування даних, що підлягли впливу ВШ.

Якщо ви користуєтеся платним антивірусним програмним забезпеченням, необхідно звернутись в службу його підтримки.

Більшість розробників антивірусних програм допомагають не тільки своїм користувачам, а й всім постраждалим.

Надалі можливо використати викладені на сайтах розробників антивірусних продуктів безкоштовні утиліти-дешифратори для різних типів вірусу шифрувальника. Визначивши тип ВШ, необхідно скачати відповідну утиліту, обов’язково зробити копії пошкоджених файлів і спробувати їх розшифровувати.

Якщо файли не розшифровуються та жодна утиліта не допомогла, цілком ймовірно, що відновлення інформації неможливо або потрібно довго чекати появи ключової інформації.

Недоліком такої стратегії є запізнення з заходами щодо протидії процесу шифрування та майже унеможливлення можливості розшифрування інформації системи.

На рис. 3 відображено запізнювання заходів, що вживаються для вирішення проблем, коли інформація в системі вже зашифрована.

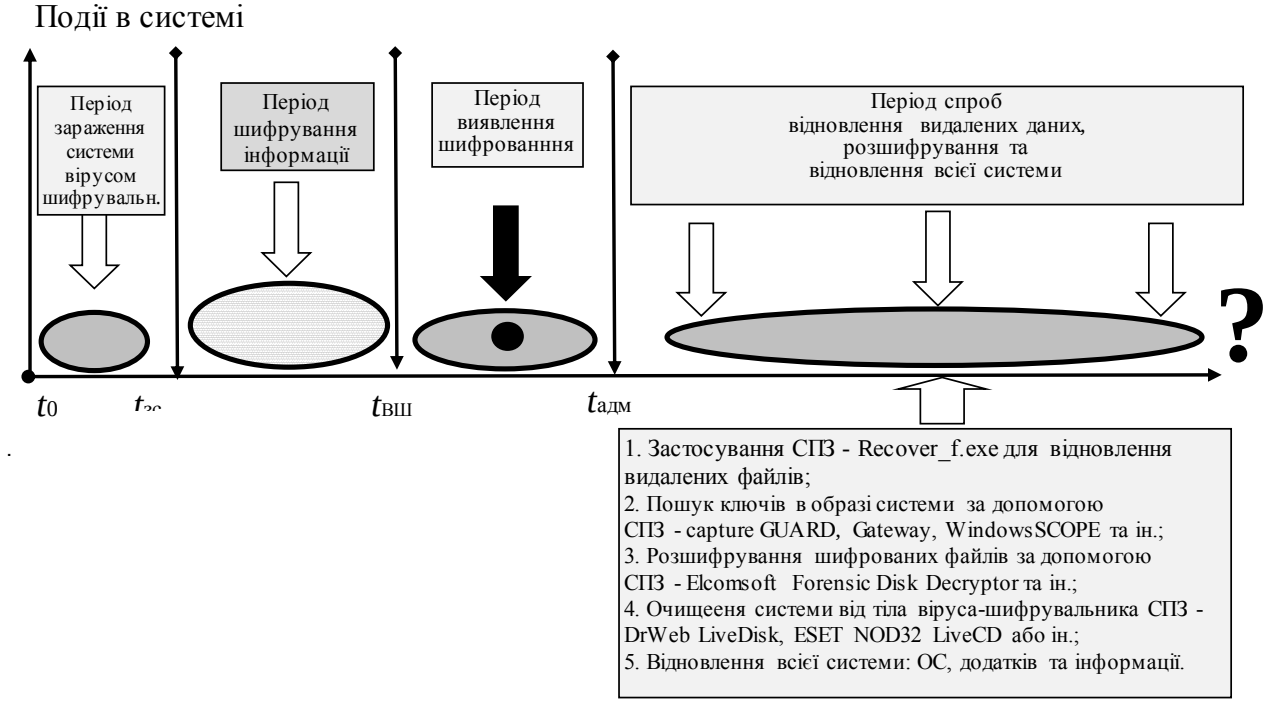

Рис. 3 Послідовність подій в ІТС, коли захист системи не встигає вчасно зупинити процес шифрування інформації

В організації CERT-UA рекомендують наступну послідовність кроків для протидії процесу шифруванню та відновлення інформації [10] рис. 3:

1. Забезпечити неприпустимість відкриття вкладень у підозрілих повідомленнях.

2. Системним адміністраторам і адміністраторам безпеки звернути увагу на фільтрування вхідних/вихідних інформаційних потоків, зокрема поштового й веб-трафіку.

3. Встановити офіційний патч MS17-010.

4. На мережному обладнанні заблокувати на серверах порти 135, 445, 1024-1035 TCP/UDP.

5. В разі інфікування персонального комп'ютера застосувати наступну тактику: не перезавантажувати ІТС (а швидко скопіювати важливі дані на змінний носій).

6. Обмежити можливість запуску виконуваних файлів (*.exe) на комп'ютерах користувачів з тимчасових директорій та папок.

7. Звернутися до рекомендацій CERT-UA стосовно безпеки поштових сервісів.

8. Для можливості відновлення зашифрованих файлів скористатися програмами ShadowExplorer або PhotoRec.

Недоліком рекомендацій CERT-UA є те, що після завершення процесу шифрування у 99 відсотках випадків практично розшифрувати інформацію неможливо або за час дешифрування інформація стає неактуальною.

На рис. 4 відображено алгоритм дій необхідних для відновлення інформації ІТС при умові пропускання всього процесу шифрування.

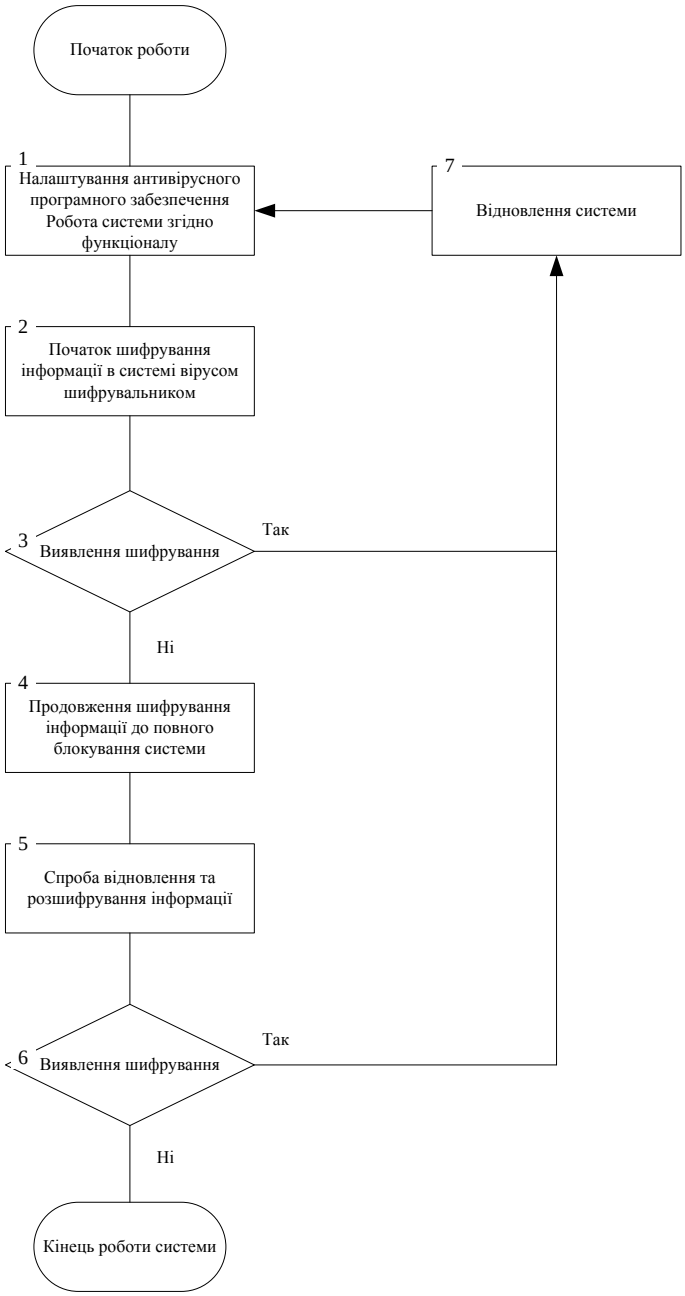

Рис. 4 Схема – алгоритм дій для відновлення інформації системи при умові пропускання всього процесу шифрування

Висновок щодо **аналізу** ***існуючих публікацій.*** Таким чином зазначимо, що публікації в даній предметній області не дають остаточні відповіді на питання пов'язані з пошуком ефективних шляхів захисту ІТС від кібератак типу несанкціоноване шифрування. Відсутні обґрунтовані рекомендації щодо заходів для блокування процесу шифрування інформації в ІТС. Відсутні відповіді на наступні питання:

що робити, як що ВШ вдало пройшов усі ланцюжки Cyber-Kill Chain, а антивіруси та системи безпеки типу IDS, IPS, NGFW не перехопити ВШ на етапі його впровадження до цільової машини;

яким чином встигнути заблокувати ВШ на початку його роботи;

які демаскуючі ознаки діяльності ВШ на цільовій машині дозволять своєчасно його виявити та заблокувати;

яким чином можливо ефективно відновити або розшифрувати інформацію ІТС;

яким чином покращити ефективність відновлення роботи ІТС загалом.

***Мета статті*:** запропонувати алгоритм покращеного захисту ІТС від діяльності ВШ, який дозволить заблокувати ВШ ще до початку його роботи в системі.

Виклад основного матеріалу. Більшість існуючих рекомендації та інструкцій регламентують дії адміністраторів після того, як інформація в системі вже зашифрована. Тільки тоді зусилля концентруються на спробах розшифрування. Практика вказує, що це майже неможливо [2 – 5]. Розглянемо кіберзахищеність ІТС P_C з точки зору «теорії масового обслуговування». Кіберзахищеність ІТС – здатність системи виконувати завдання за призначенням в умовах кібератак противника [10]; На вхід системи кібернетичної безпеки (далі – СКБ) поступають кібератаки, які мають наступні характеристики:

λ – інтенсивність загального потоку кібератак на вході ІТС;

$\lambda_{ВШ}$ – інтенсивність потоку кібератак на вході ІТС націлених на шифрування інформації;

$\lambda z_{ВШ}$ – інтенсивність загального потоку кібератак націлених на шифрування інформації після впливу на потік $\lambda_{ВШ}$ СКБ;

$P_З$ – показник захищеності ІТС від кібератак;

$K_В$ – коефіцієнт вразливості ІТС від кібератак.

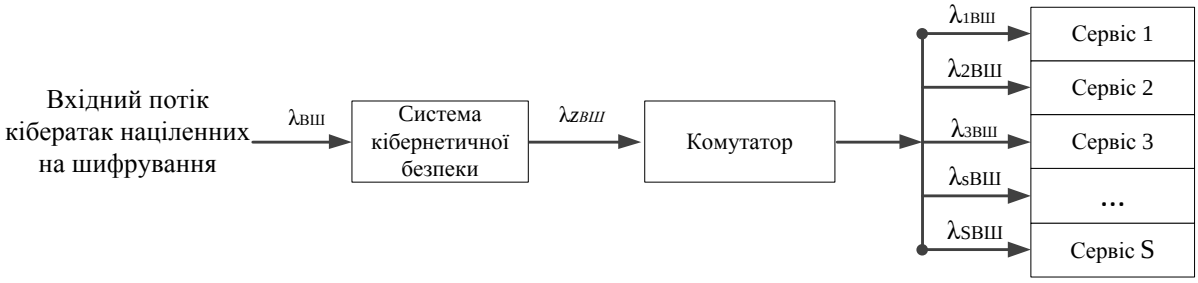

Рис. 5 Модель ІТС з СКБ для захисту від кібератак, в тому числі від атак ВШ

$$K_В = \lambda z / \lambda,\ P_З = 1 - \lambda z / \lambda,$$

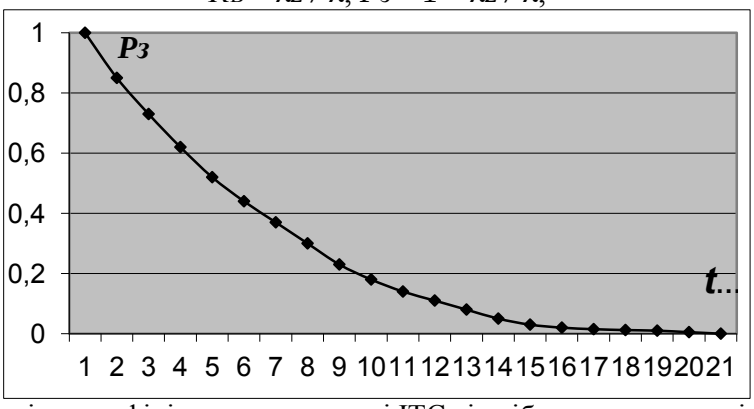

Рис. 6 Залежність коефіцієнта захищеності ІТС від кібератак при умові незмінності налаштувань системи кібернетичної безпеки

Для визначення кіберзахищеності ІТС використаємо формулу розрахунку кіберзахищеності ІТС (1) від дій шкідливого програмного забезпечення (далі – ШПЗ) з роботи [10].

$$P_C = \Sigma_j(P_{tsj} \times K_{ВГ\ ZJ}) / \Sigma_j(K_{ВГ\ ZJ}), \quad (1)$$

де P_C – показник кіберзахищеності системи від впливу ШПЗ;

P_{tsj} – показник ефективності заходу застосування засобів *(j)* призначених для захисту ІТС від дій ШПЗ;

$K_{ВГ\ ZJ}$ – ваговий коефіцієнт заходу застосування засобів *(j)* призначених для захисту ІТС від дій ШПЗ;

J – кількість заходів застосування засобів захисту ІТС, $j = 1...J$.

Використаємо формулу (1) для розрахунку захищеності ІТС від дій ВШ. Розрахуємо $P_{ЗВШ}$ – захищеність ІТС від дій ВШ з урахуванням вагових коефіцієнтів кожного заходу застосування засобів – $K_{ВГj}$ за формулою (2).

$$P_{ЗВШ} = \Sigma_j(P_{ВШ_j} \times K_{ВГВШ\,j}) / \Sigma_j(K_{ВГВШ\,j}), \quad (2)$$

де $P_{ЗВШ}$ – показник кіберзахищеності ІТС від впливу ВШ;

$P_{ВШ_j}$ – показник ефективності заходу застосування засобів *(j)* для захисту ІТС від дії ВШ;

$K_{ВГВШ\,j}$ – ваговий коефіцієнт заходу застосування засобів *(j)* для захисту ІТС від дії ВШ;

J – кількість заходів застосування засобів для захисту ІТС від дії ВШ, $j = 1...\ J$.

Тоді локальну захищеність ІТС від дії ВШ $P_{ЗВШ}$ при умові застосуванні засобів для вчасного блокування та подальшого розшифрування інформації пропонуємо розрахувати за формулою (3).

$$P_{ЗВШ} = ((P_{ББВШ} \times K_{ВГББВШ}) + (P_{ДШФ} \times K_{ДШФ})) / (K_{ВГВШ} + K_{ДШФ}), \quad (3)$$

де $P_{ББВШ}$ – показник ефективності застосування засобів блокування початку роботи ВШ;

$P_{ДШФ}$ – показник ефективності застосування засобів для розшифрування інформації;

$K_{ВГББВШ}$ – ваговий коефіцієнт застосування засобів блокування початку роботи ВШ;

$K_{ДШФ}$ – ваговий коефіцієнт застосування засобів для розшифрування інформації;

$J = 2$ – кількість заходів застосування засобів, які задіяні проти ВШ.

Для порівняння проведемо розрахунок захищеності ІТС від дій ВШ у випадку, коли заходи захисту зовсім не реалізовані. Тоді зрозуміло, що $P_{ББВШ} = 0$; $P_{ДШФ} = 0$, а згідно методики Сааті та експертним оцінкам кіберфахівців [11, 12] в даному випадку $K_{ВГББВШ} = 0{,}9$; $K_{ДШФ} = 0{,}9$.

$$P_{ЗВШ} = ((0{,}0 \times 0{,}9) + (0{,}0 \times 0{,}9)) / (0{,}9 \times 0{,}9) = 0{,}00.$$

Проведемо розрахунок захищеності ІТС від дій ВШ у випадку, у випадку коли реалізовано тільки заходи для малоймовірного розшифрування та відновлення ІТС, після вдалої дії ВШ. Зазначимо, що згідно методики Сааті та експертним оцінкам кіберфахівців [11, 12] $P_{ББВШ} = 0$; $P_{ДШФ} = 0{,}1$.

$$P_{ЗВШ} = ((0{,}0 \times 0{,}9) + (0{,}1 \times 0{,}9)) / (0{,}9 \times 0{,}9) = 0{,}05.$$

Бачимо що у цьому випадку оцінка захищеності ІТС від дії ВШ – $P_{ЗВШ}$ дорівнює 0,05 що є незадовільною оцінкою ефективності системи кібернетичної безпеки.

Автори пропонують зосередити зусилля захисту на блокуванні процесу шифрування ще на його початку, щоб потім не було потреби в надскладному розшифрування інформації.

Пропозиція полягає в тому, щоб заздалегідь розгорнути в ІТС програмно-апаратні засоби, які здатні до своєчасного виявлення ознак шифрування, блокування процесу шифрування, аварійного копіювання, пошуку ключової інформації, відновлення видалених або зашифрованих файлів та відновлення працездатності системи в цілому.

Пропонується комплексно застосувати наступні зразки спеціального програмного забезпечення (далі – СПЗ):

СПЗ для недопущення проникнення ВШ в ІТС;

СПЗ для екстреного резервного копіювання образу ІТС;

СПЗ для контролю за існуючими “процесами” в ІТС;

СПЗ для контролю за навантаженням CPU;

СПЗ для контролю за файлами;

СПЗ для виявлення ознак шифрування інформації в ІТС;

СПЗ для екстреної при зупинки CPU або уповільнення його роботи;

СПЗ – для оповіщення підрозділів ІТС про загрозу дії ВШ;

СПЗ – для блокування спроб несанкціонованого пере завантаження системи;

СПЗ – для пошуку парольної інформації;

СПЗ – для відновлення ІТС (ОС, додатків та даних).

Головна пропозиція авторів наведена на рис. 7 та полягає у концентрації зусиль на недопущенні початку шифрування інформації. Розміщення такого СПЗ дозволить адміністраторам ІТС вчасно виявити та призупинити процес шифрування інформації, провести аналіз інциденту та зберегти працездатність системи.

На рис. 7 надано пояснення щодо попереднього розміщення СПЗ необхідного для своєчасного блокування процесу шифрування.

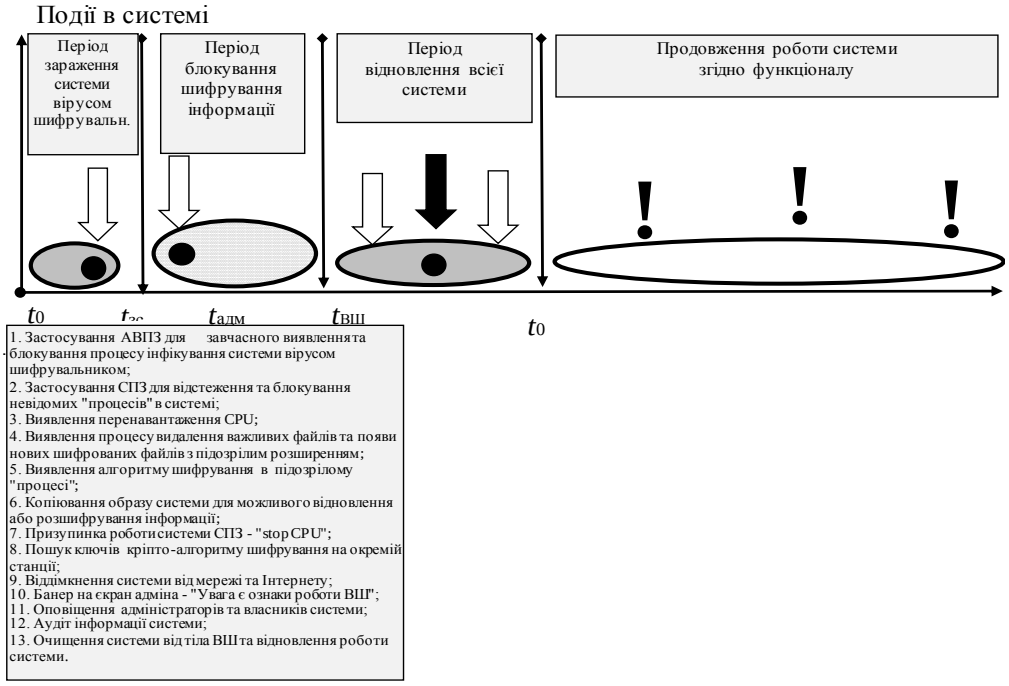

Рис. 7 Період упереджуючих заходів необхідних для блокування початку шифрування інформації в системі

Автори пропонують в подальшому розробити та застосувати в складі СКБ зразки вищевказаного СПЗ, таким чином щоб мати можливість своєчасного блокування початку роботи ВШ під час його проникнення в ІТС або на перших етапах здійснення роботи ВШ. Таким чином, можливо недопущення шифрування, а в наслідок цього і відсутність проблем щодо надскладного та малоймовірного розшифрування інформації.

Адміністраторам ІТС слід зосередити увагу на прямі та опосередковані ознаки дії ВШ.

На рис. 8 вказана рекомендована послідовність дій для завчасного блокування дії ВШ, яка ймовірно покращить захищеність ІТС від дій ВШ – $P_{ЗВШ}$.

Автори пропонують наступну послідовність дій адміністраторів:

1. Заздалегідь завантажити в ІТС актуальні зразки СПЗ з функціями антивірусного захисту.

2. Завантажити в систему СПЗ здатне виявляти ознаки несанкціонованого шифрування, призупинення процесів та CPU, копіювання інформації з ОЗУ та HDD, пошуку ключів, відновлення і розшифрування інформації та відновлення ІТС.

3. Забезпечити роботу ІТС згідно її функціоналу.

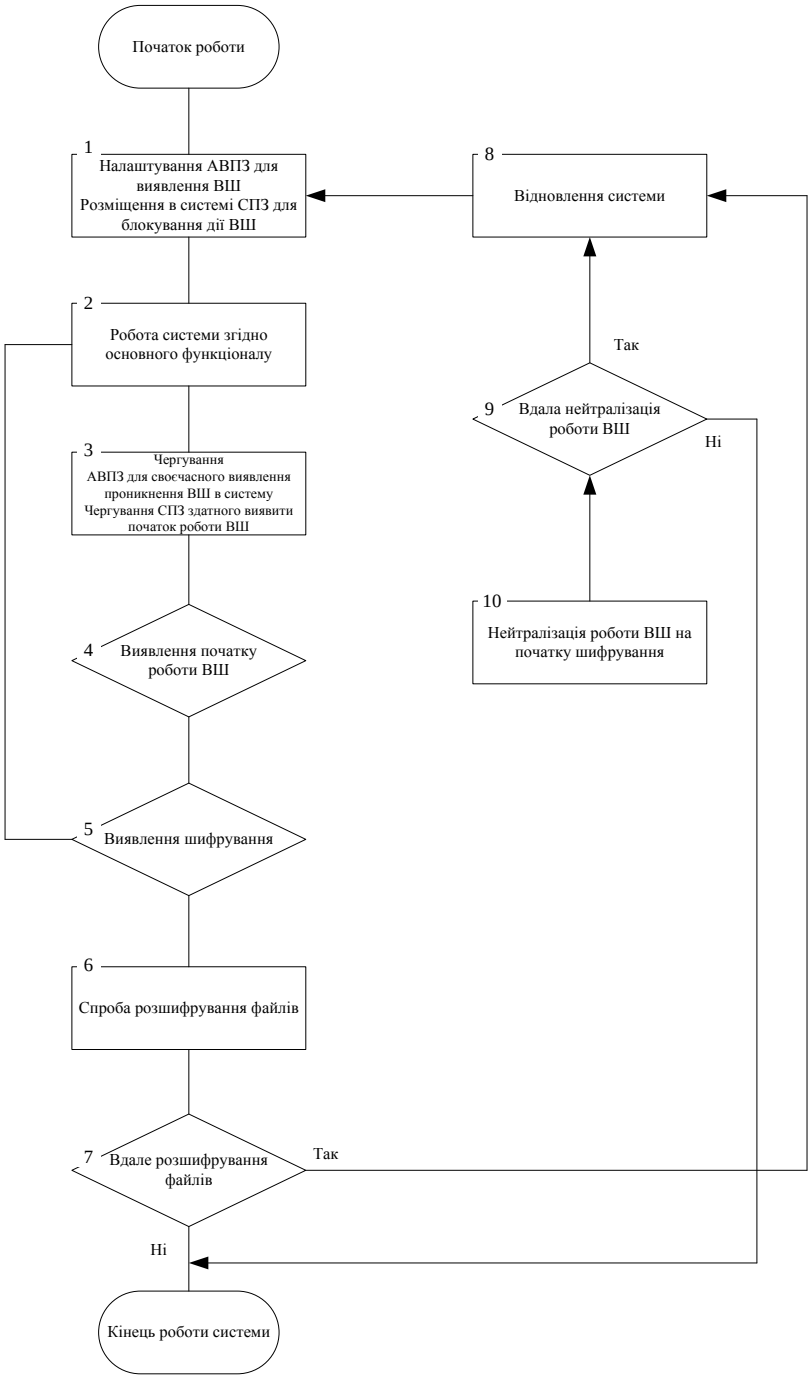

Рис. 8 Схема-алгоритм запропонованих дій для завчасного блокування діяльності ВШ

4. Налаштувати роботу СПЗ необхідного для виявлення ознак дії ВШ в ІТС.
5. Забезпечити чергування вищевказаного СПЗ в системі.
6. У випадку своєчасного виявлення ознак ВШ здійснити блокування роботи ВШ.
7. Відновити працездатність ІТС згідно її функціоналу.
8. При необхідності здійснити пошук ключів та розшифрування інформації.
9. У випадку коли ознаки шифрування виявлені, адміністратор здійснює наступні дії:

знищує шкідливі процеси в ІТС; здійснює копіювання образу інформації ІТС; завантажує образи ІТС на станцію кібернетичної експертизи типу Ntb HP “G7/8”; здійснює спробу крипто аналізу алгоритму шифрування; здійснює пошук сигнатур ВШ; здійснює пошук ключів шифрування в образах інформації;здійснює розшифрування та відновлення файлів; здійснює відновлення ОС, додатків та даних ІТС; розробляє звіт про інцидент в ІТС; приймає участь в аналізі шляхів зараження ІТС (наприклад з оновлень додатків, вкладень E.mail повідомлень або веб-сайтів); якщо адміністратор не виявляє ознак ВШ, то робота ІТС

– продовжується. Для відпрацювання запропонованої послідовності дій автори рекомендують сформувати безпечний сектор обладнання та засобів - “cyber training ground” для тренування адміністраторів – “кіберполігон”. Регулярно проводити тренування фахівців для відпрацювання захисту від спроб несанкціонованого шифрування інформації.

У випадку, коли послідовність дій для нейтралізації дій ВШ реалізована вдало при розрахунку захищеності ІТС використаємо експертні оцінки [11–13], де $P_{\text{БВШ}} = 0{,}9$; $P_{\text{ДШФ}} = 0{,}9$. Тоді захищеність системи від дії ВШ дорівнює:

$$P_{\text{ЗВШ}} = ((0{,}9 \times 0{,}9) + (0{,}0 \times 0{,}9)) / (0{,}9 \times 0{,}9) = 0{,}45.$$

Захищеність $P_{\text{ЗВШ}} = 0{,}45$ також недостатня, але під час налаштування зразків СПЗ, а головне після підвищення професійності дій користувачів, адміністраторів та власників системи, захищеність ІТС від дій ВШ може досягти до $P_{\text{ЗВШ}} = 0{,}95$ при цьому згідно експертним оцінкам [11–13] $P_{\text{БВШ}} = 0{,}99$; $P_{\text{ДШФ}} = 0{,}9$. Тоді захищеність системи від дії ВШ дорівнює:

$$P_{\text{ЗВШ}} = ((0{,}99 \times 0{,}9) + (0{,}9 \times 0{,}9)) / (0{,}9 \times 0{,}9) = 0{,}95.$$

На рис. 9 вказані періоди часу використання заходів протидії ВШ, блокування шифрування та заходів направлених на відновлення даних ІТС.

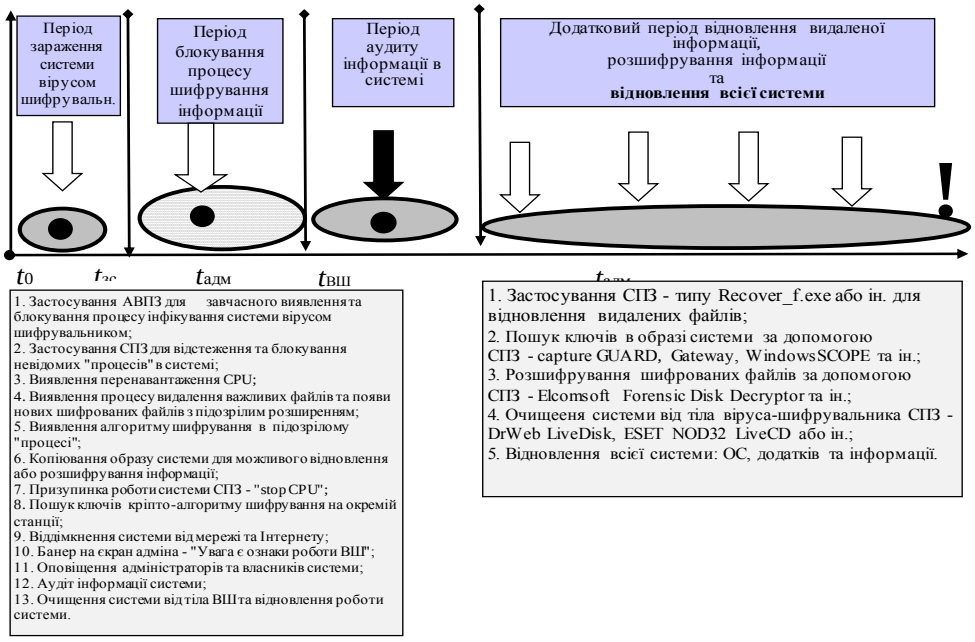

Рис. 9 Приклад одночасного використання двох заходів застосування засобів необхідних для ефективного блокування роботи ВШ

Тоді у випадку, коли реалізовано всі сучасні заходи для завчасного блокування початку роботи ВШ в ІТС та заходи для ефективного розшифрування файлів, розрахунок захищеності, де згідно експертним оцінкам [11–13] $P_{\text{БВШ}} = 0{,}99$; $P_{\text{ДШФ}} = 0{,}99$ дорівнює:

$$P_{\text{ЗВШ}} = ((0{,}99 \times 0{,}9) + (0{,}99 \times 0{,}9)) / (0{,}9 \times 0{,}9) = 0{,}99.$$

В такому разі захищеність ІТС $P_{\text{ЗВШ}} = 0{,}99$, що є достатньою, а під час постійного доопрацювання СПЗ та навчання фахівців, захищеність ІТС дій від ВШ може досягти $P_{\text{ЗВШ}} = 0{,}999$.

Висновки. Використання запропонованого порядку дій адміністраторів безпеки при виявлення ознак шифрування інформації дозволить адміністратору системи своєчасно заблокувати дії ВШ та підвищити захищеність ІТС від дій ВШ до $P_{\text{ЗВШ}} = 0{,}99$.

Для унеможливлення роботи ВШ в ІТС доцільно заздалегідь підготувати засоби захисту та забезпечити повну обізнаність фахівців адміністраторів а саме: досягати повної обізнаності адміністраторів та користувачів щодо загрози від ВШ та відпрацьовувати їх

практичні навички для протидії загрозам дій ВШ; постійно оновляти актуальне СПЗ для можливості ефективного блокування початку роботи ВШ; постійно резервувати інформацію системи, щоб у вас було декілька бекапів: один у хмарі, наприклад Dropbox, Google Drive та інших спеціалізованих сервісах, а також на змінному носії (знімний жорсткий диск, USB-флеш або запасний комп'ютер); проводити навчання для підвищення навичок адміністраторів системи практично нейтралізувати дії ВШ; для захисту ІТС слід застосовувати обидва комплекти засобів захисту від дії ВШ для недопущення початку шифрування та можливості ефективного розшифрування інформації.

Наслідком таких зусиль стане ріст захищеності системи від дій ВШ до $P_{\text{ЗВШ}} \rightarrow 0{,}999$.

Подальші напрямки досліджень дозволять поширити запропонований підхід на блокування різноманітних класів ШПЗ – руткитів, хробаків, бекдорів, різноманітних вірусів та систем вторгнень, враховуючи при цьому особливості їх дій.

ЛІТЕРАТУРА

1. Расширенная модель Cyber-Kill Chain и почему ее надо учитывать в стратегии защиты [Електронний ресурс]. – Режим доступу: https://habr.com/ru/company/panda/blog/327488/

2. Новое время "Захисти себе сам. Все що потрібно знати про вірус Petya.A" [Електронний ресурс]. – http://nv.ua/ukr/techno/gadgets/zahisti-sebe-sam-vse-shcho-potribno-znati-pro-virus-petya-a-1392163.html.

3. Vesti Ukraine "Все что известно о вирусе WannaCry и Petya.A" [Електронний ресурс]. – Режим доступу: http://vesti-ukr.com/mir/244843-vse-chto-izvestno-o-viruse-wannacry.html.

4. Tech today "Все что нужно знать о вирусе Petya и как с ним бороться" [Електронний ресурс]. – https://techtoday.in.ua/ru/reviews-ru/vse-chto-nuzhno-znat-o-viruse-petya-kak-s-nim-borotsya-75861.html.

5. Котенко И.В. Оценка рисков в компьютерных сетях критических інфраструктур / И.В. Котенко , И.Б. Саенко, Е.В. Дойникова // Инновации в науке: зб. наук. пр. / XVI міжнар. наук.-практ. конф. Частина І. – Новосибірськ: СибАК, 2013. Вип.№16-1. С. 84 – 88.

6. Давидюк А.В. Протидія автоматизованим засобам використання соціальної інженерії / А.В. Давидюк, В.М. Петрик // Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.) [Електронне видання]. – К.: Нац. акад. СБУ, 2018. С. 346 – 347.

7. Korchenko A., Dreis Yu., Roshchuk M., Romanenko O. Consequence evaluation model of leak the state secret from cyberattack directing on critical information infrastructure of the state // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 1, P. 29-35.

8. Шевченко А.С. Механізми виявлення кібернетичних атак на основі контрольних карт Шухарта/ А.С. Шевченко // Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.) [Електронне видання]. – К.: Нац. акад. СБУ, 2018. С. 186 – 189.

9. Новий небезпечний вірус-шифрувальник. Молодий буковинець https://molbuk.ua/news/201684-fakhivci-znayshly-novyy-nebezpechnyyvirus-shyfruvalnyk.html.

10. Рекомендації до знищення наслідків дії вірусу Petya.A – "Новинарня". Вірус шифрувальник., CERT– Режим доступу: https://novynarnia.com/2018/11/17/cert-ua.html.

11. Куцаєв В.В. Радченко М.М. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла. Збірник наукових праць ВІТІ. Київ, 2018. Вип. №2.

12. Куцаєв В.В., Козубцов І.М. Експертні оцінки захищеності систем методом Сааті. Збірник наукових праць ВІТІ. Київ, 2017. Вип. №3.

13. Чередніченко О.М., Куцаєв В.В., Гук О.М., Шугалій О.О. Аналіз кібернетичних інцидентів на території України та базові методи кібернетичного захисту від них. Збірник наукових праць ВІТІ. Київ, 2018. Вип. №3.