DOI:**10.33099/2311-7249/2021-40-1-27-36**

УДК 004.056.5

Роман Михайлович Штонда
Володимир Вікторович Куцаєв
Олена Михайлівна Сівоха
Михайло Васильович Артемчук

Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна

МЕТОДИ ПРОТИДІЇ ВІРУСУ ШИФРУВАЛЬНИК В ІНФОРМАЦІЙНИХ СИСТЕМАХ

У цій статті пропонується алгоритм, яким керуються системні адміністратори для протидії несанкціонованим спробам шифрування інформації в інформаційних системах.

Факти вказують, що терміновість вжитих заходів полягає в тому, що кількість атак програм шифрування досягла 30% від загальної кількості глобальних кібератак та кіберінцидентів. Масштабні кібератаки відбуваються приблизно кожних шість місяців, а методи проникнення та алгоритми шифрування постійно вдосконалюються. Відповідно до моделі Cyber-Kill Chain, зловмисники успішно досягають поставленої мети на цільовому комп'ютері.

Метою заходів щодо усунення несанкціонованого шифрування інформації в системі є запобігання її дії на початку роботи.

Автори рекомендують заздалегідь розміщувати зразки програмного забезпечення в інформаційній системі, це дозволить своєчасно виявляти ознаки несанкціонованого шифрування інформації в системі.

Заходи включають розміщення зразка спеціального програмного забезпечення в системі якомога раніше. Зразок може реалізувати "постійний програмний моніторинг" процесу в системі, щоб зупинити процесор, коли є ознаки шифрування, тобто: коли процесор перевантажений, коли виявляються підозрілі процеси, при виявленні ознак дії алгоритму шифрування, у разі синхронізації і коли важливі файли зникають, у разі спроби перезапустити систему та інших ознак. Автори порівнюють систему мережевої безпеки із ситуацією, коли рекомендовані заходи не застосовуються. Автори вважають, що, виходячи з ефективності відповідних заходів, система захисту мережі зросте до 0,99.

Висновок цієї статті полягає в тому, що розміщення спеціального програмного забезпечення в системі дозволить протидіяти якомога швидше вірусу шифрувальнику та покращить безпеку системи.

Подальші дослідження дозволять розповсюдити рекомендовані заходи щодо усунення поведінки різних типів кібератак, які досягли цільової машини, а також виникнення кіберінцидентів відповідно до моделі Cyber-Kill Chain.

Ключові слова: *вірус-шифрувальник; кібератака; кіберзахист; Cyber Kill Chain; інформаційна система.*

Вступ

Основні світові аналітики визнають, що 30% сучасних кіберзагроз становлять спроби шифрування інформації в системах 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.

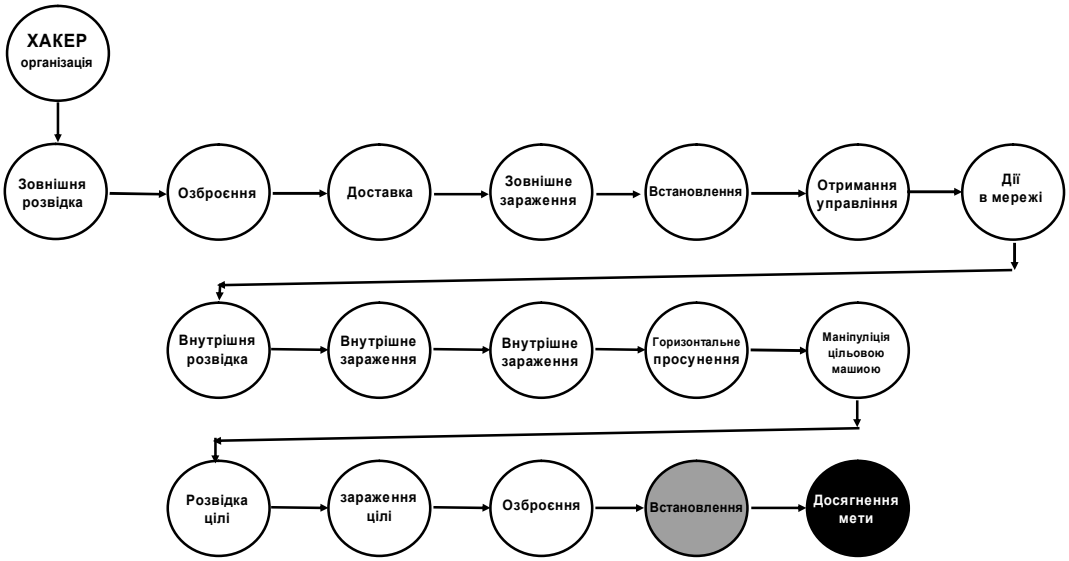


Рис. 1 Ланцюжок дій, які реалізує зловмисник згідно моделі Cyber-Kill Chain

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.

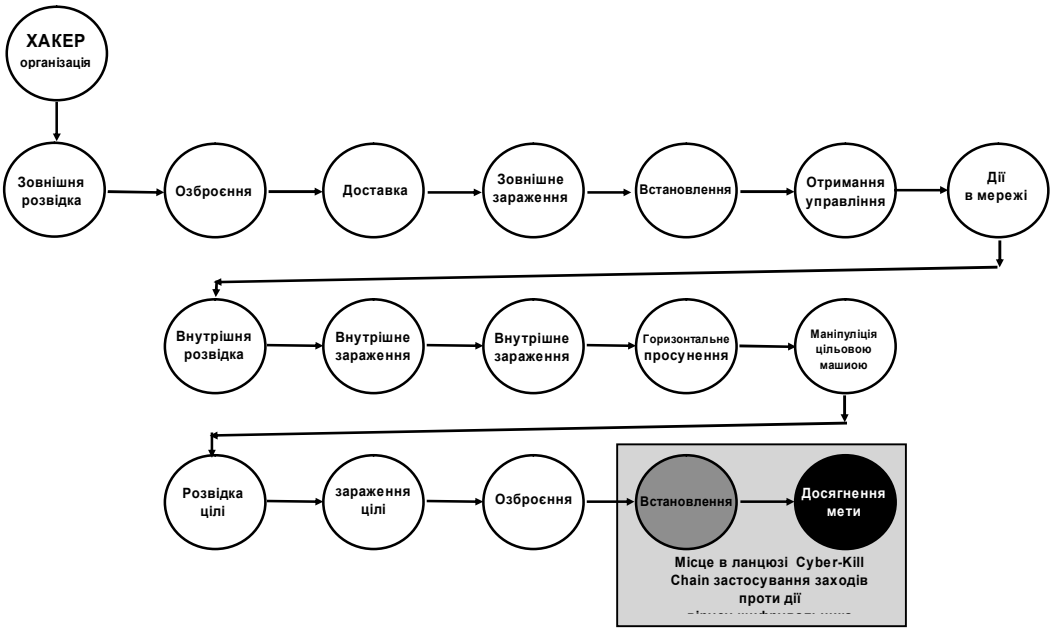


Рис. 2 Місце впливу запропонованих заходів протидії вірусу шифрувальнику в ланцюжку моделі Cyber-Kill Chain

Вірус шифрувальник (далі – ВШ), це програмне забезпечення, яке здатне непомітно проникати в інформаційні системи (далі – ІС) та шифрувати важливу інформацію, блокуючи роботу ІС. Після цього зловмисники, які оперують ВШ вимагають власників систем заплатити викуп. Наприклад на екранах в ІС 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 систем, 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].

Постановка проблеми. У 2013-2017 роках кібератаки проти України здійснювалися з використанням APT-атак (Snake, Uroboros, Sofacy/APT28, Epic Turla, Black Energy 2 і 3, Armageddon 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 ІС 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 ІС 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 ІС.

В наведеній методиці не запропоновано порівняння ризиків для ІС 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 системи. Алгоритм в поєднанні з методиками менеджменту ризиків та вразливостей ІС декларується, як корисний інструмент для підвищення рівня інформаційної безпеки ІС у цілому. На думку авторів, алгоритм не є вирішенням всіх можливих проблем інформаційної безпеки ІС, 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 ІС від кібератак на дану ІС. В контексті дослідження шляхів чи напрямків кібернетичного захисту модель має сенс, але не відповідає потребі покращення захисту від ВШ на окрему ІС.

Метод реєстрацій аномалій в ІС на основі контрольних карт Шухарта, як і будь-який статистичний метод виявлення аномалій [8] в ІС та запобігання вторгненням при кіберзахисті об'єкту, має недолік пов'язаний з необхідністю набору статистики даних про значення параметру відносно якого проводиться аналіз стану кіберзахисту ІС. 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 захищеність ІС від дій ВШ.

Метою статті є запропонувати алгоритм покращеного захисту ІС від діяльності ВШ, який дозволить заблокувати ВШ ще до початку його роботи в системах.

Виклад основного матеріалу дослідження

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

На даний час деякі інструкції та алгоритми дій адміністраторів при перших ознаках роботи ВШ, таких як перезавантаження ІС, подальше блокування ІС, 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 системи. 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 систем 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 систем.

Таким чином зазначимо, що публікації в даній предметній області не дають остаточні відповіді на питання пов'язані з пошуком ефективних шляхів захисту ІС від кібератак типу несанкціоноване шифрування. Відсутні обґрунтовані рекомендації щодо заходів для блокування процесу шифрування інформації в ІС. 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 ІС;

яким чином покращити ефективність відновлення роботи ІС загалом.

Більшість існуючих рекомендації та інструкцій регламентують дії адміністраторів після того, як інформація в системах вже зашифрована. Тільки тоді зусилля концентруються на спробах розшифрування. Практика вказує, що це майже неможливо [2-5].

Розглянемо кіберзахист ІС РС з точки зору "теорії масового обслуговування". Кіберзахист ІС – здатність систем виконувати завдання за призначенням в умовах кібератак противника [10].

На вхід системи кібернетичної безпеки (далі – СКБ) поступають кібератаки, які мають наступні характеристики (рис. 3):

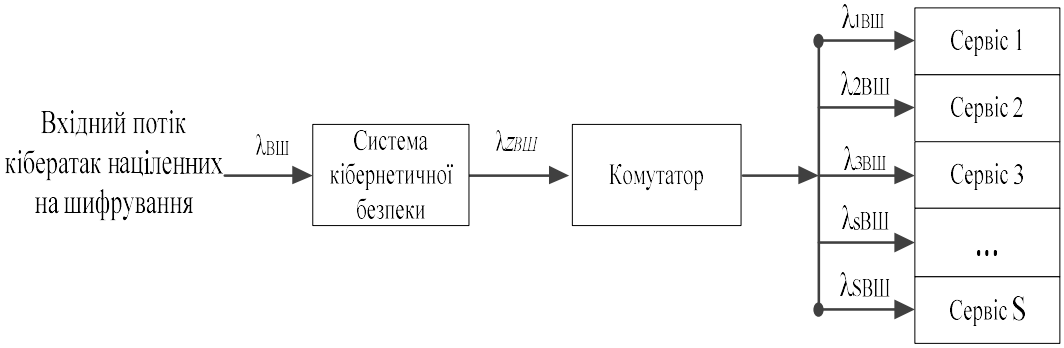
λ – інтенсивність загального потоку кібератак на вході ІС;

λВШ – інтенсивність потоку кібератак на вході ІС націлених на шифрування інформації;

λzВШ – інтенсивність загального потоку кібератак націлених на шифрування інформації після впливу на потік λВШ СКБ;

РЗ – показник захищеності ІС від кібератак;

КВ – коефіцієнт вразливості ІС від кібератак.



$КВ = \lambda z / \lambda, \quad РЗ = 1 - \lambda z / \lambda$

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

Для визначення кіберзахисту ІС використаємо формулу розрахунку кіберзахисту ІС (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 кіберзахисту систем від впливу ШПЗ;

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

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

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

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

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

де $P_{ЗВШ}$ – показник кіберзахисту ІС від впливу ВШ;

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

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

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

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

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

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

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

$K_{ВГБВШ}$ – 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 ІС від дій ВШ у випадку, коли заходи захисту зовсім не реалізовані. Тоді зрозуміло, що $P_{БВШ} = 0$; $P_{ДШФ} = 0$, а згідно методики Сааті та експертним оцінкам кіберфахівців [11, 12] в даному випадку $K_{ВГБВШ} = 0{,}9$; $K_{ДШФ} = 0{,}9$.

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

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

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

Бачимо що у цьому випадку оцінка захищеності ІС 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 ІС 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 систем в цілому.

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

СПЗ для недопущення проникнення ВШ в ІС;

СПЗ для екстреного резервного копіювання образу ІС;

СПЗ для контролю за існуючими “процесами” в ІС;

СПЗ для контролю за навантаженням CPU;

СПЗ для контролю за файлами;

СПЗ для виявлення ознак шифрування інформації в ІС;

СПЗ для екстреної при зупинки CPU або уповільнення його роботи;

СПЗ – для оповіщення підрозділів ІС про загрозу дії ВШ;

СПЗ – для блокування спроб несанкціонованого перезавантаження систем;

СПЗ – для пошуку парольної інформації;

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

Головна пропозиція авторів наведена на рис. 4 та полягає у концентрації зусиль на недопущенні початку шифрування інформації. Розміщення такого СПЗ дозволить адміністраторам ІС вчасно виявити та призупинити процес шифрування інформації, провести аналіз інциденту та зберегти працездатність систем.

На рис. 4 надано пояснення щодо попереднього розміщення СПЗ необхідного для своєчасного блокування процесу шифрування.

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 ІС 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 ІС слід зосередити увагу на прямі та опосередковані ознаки дії ВШ.

На рис. 5 вказана рекомендована послідовність дій для завчасного блокування дії ВШ, яка ймовірно покращить захищеність ІС від дій ВШ – РЗВШ.

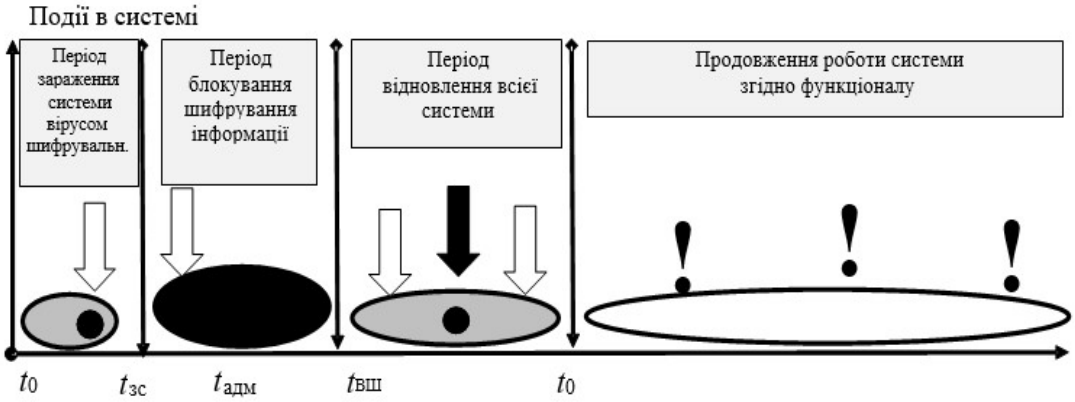


Рис. 4 Період упереджуючи заходів необхідних для блокування початку шифрування інформації в системах

На рис. 4 надано пояснення щодо попереднього розміщення СПЗ необхідного для своєчасного блокування процесу шифрування.

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 ІС 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 ІС слід зосередити увагу на прямі та опосередковані ознаки дії ВШ.

На рис. 5 вказана рекомендована послідовність дій для завчасного блокування дії ВШ, яка ймовірно покращить захищеність ІС від дій ВШ – РЗВШ.

Автори пропонують наступну послідовність дій адміністраторів:

1. Заздалегідь завантажити в ІС актуальні зразки СПЗ з функціями антивірусного захисту.
2. Завантажити в системи СПЗ здатне виявляти ознаки несанкціонованого шифрування, призупинення процесів та CPU, копіювання інформації з ОЗУ та HDD, пошуку ключів, відновлення і розшифрування інформації та відновлення ІС.
3. Забезпечити роботу ІС згідно її функціоналу.
4. Налаштувати роботу СПЗ необхідного для виявлення ознак дії ВШ в ІС.
5. Забезпечити чергування вищевказаного СПЗ в системах.
6. У випадку своєчасного виявлення ознак ВШ здійснити блокування роботи ВШ.
7. Відновити працездатність ІС 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 ІС;

здійснює копіювання образу інформації ІС;

завантажує образи ІС 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 ІС;

розробляє звіт про інцидент в ІС;

приймає участь в аналізі шляхів зараження ІС (наприклад з оновлень додатків, вкладень E.mail повідомлень або веб-сайтів);

якщо адміністратор не виявляє ознак ВШ, то робота ІС – 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 ІС використаємо експертні оцінки [11–13], де $P_{ББШ}$ =0,9; $P_{ДШФ}$ =0,9. Тоді захищеність систем від дії ВШ дорівнює:

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

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

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

На рис. 6 вказані періоди часу використання заходів протидії ВШ, блокування шифрування та заходів направлених на відновлення даних ІС.

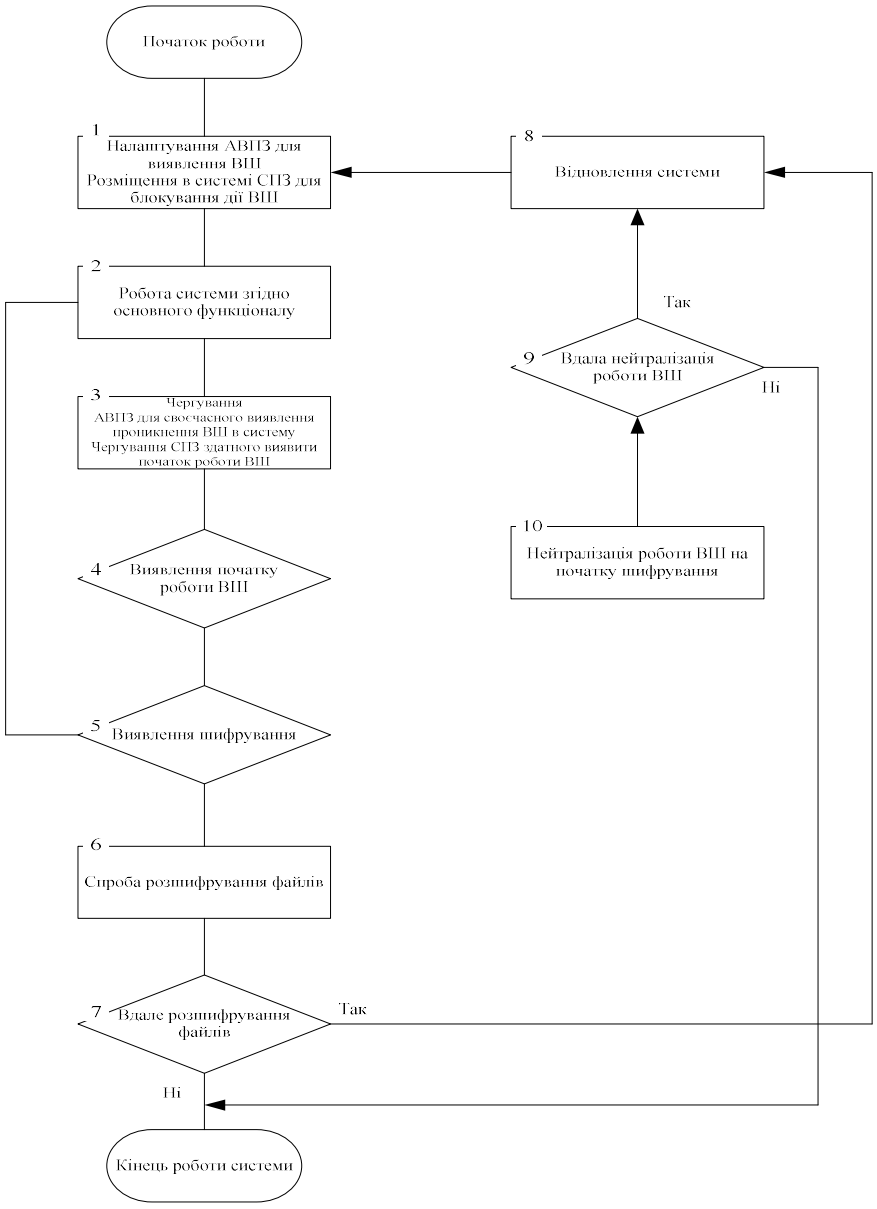


Рис. 5 Схема-алгоритм запропонованих дій для завчасного блокування діяльності ВШ

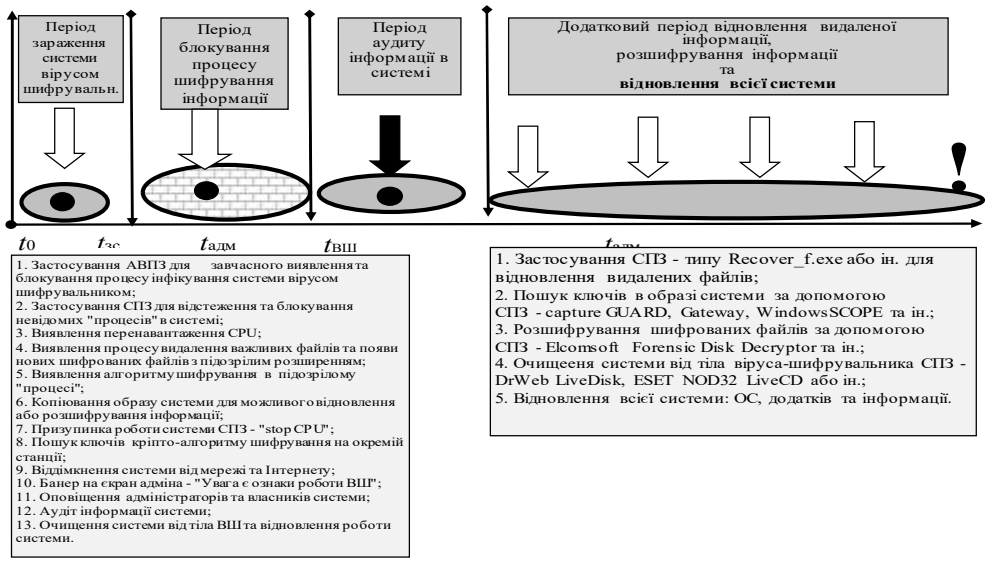


Рис. 6 Приклад одночасного використання двох заходів застосування засобів необхідних для ефективного блокування роботи ВШ

Тоді у випадку, коли реалізовано всі сучасні заходи для завчасного блокування початку роботи ВШ в ІС 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 ІС $P_{\text{ЗВШ}} = 0{,}99$, що є достатньою, а під час постійного доопрацювання СПЗ та навчання фахівців, захищеність ІС дій від ВШ може досягти $P_{\text{ЗВШ}} = 0{,}999$.

Висновки і перспективи подальших досліджень

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

Для унеможливлення роботи ВШ в ІС 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 систем, 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 систем практично нейтралізувати дії ВШ;

для захисту ІС слід застосовувати обидва комплекти засобів захисту від дії ВШ для недопущення початку шифрування та можливості ефективного розшифрування інформації.

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

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]. https://habr.com/ru/company/panda/blog/327488/

2. Новое время "Захисти себе сам. Все що потрібно знати про вірус Petya.A" [Електронний ресурс]. – https://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]. https://vesti.ua/mir/244843-vse-chto-izvestno-o-viruse-wannacry-i- **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 инфраструктур / 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-nebezpechnyy-virus-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.

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ВИРУСУ ШИФРОВАЛЬЩИК В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Роман Михайлович Штонда
Владимир Викторович Куцаев
Елена Михайловна Сивоха
Михаил Васильевич Артемчук

Военный институт телекоммуникаций и информатизации имени Героев Крут, Киев, Украина

В этой статье предлагается алгоритм, которым руководствуются системные администраторы для противодействия несанкционированным попыткам шифрования информации в информационных системах.

Факты указывают, что срочность принятых мер заключается в том, что количество атак программ шифрования достигла 30% от общего количества глобальных кибератак и киберинцидентив. Масштабные кибератаки происходят примерно каждые шесть месяцев, а методы проникновения и алгоритмы шифрования постоянно совершенствуются. Согласно модели Cyber-Kill Chain, злоумышленники успешно достигают поставленной цели на целевом компьютере.

Целью мероприятий по устранению несанкционированного шифрования информации в системе является предотвращение ее действия в начале работы.

Авторы рекомендуют заранее размещать образцы программного обеспечения в информационной системе, это позволит своевременно выявлять признаки несанкционированного шифрования информации в системе.

Мероприятия включают размещение образца специального программного обеспечения в системе как можно раньше. Образец может реализовать "постоянный программный мониторинг" процесса в системе, чтобы остановить процессор, когда есть признаки шифрования, то есть: когда процессор перегружен, когда появляются подозрительные процессы, при обнаружении признаков действия алгоритма шифрования, в случае синхронизации и когда важные файлы исчезают, в случае попытки перезапустить систему и других признаков. Авторы сравнивают систему сетевой безопасности с ситуацией, когда рекомендованные меры не применяются. Авторы считают, что, исходя из эффективности соответствующих мер, система защиты сети возрастет до 0,99.

Вывод этой статьи заключается в том, что размещение специального программного обеспечения в системе позволит противодействовать как можно скорее вируса шифровальщик и улучшит безопасность системы.

Дальнейшие исследования позволят распространить рекомендованные меры по устранению поведения различных типов кибератак, которые достигли целевой машины, а также возникновения киберинцидентов согласно модели Cyber-Kill Chain.

Ключевые слова: *вирус-шифровальщик; кибератака; киберзащита; Cyber Kill Chain; информационная система.*

METHODS FOR ANTI-ENTRY VIRUS IN INFORMATION SYSTEMS

Roman Mikhailovich Shtonda
Vladimir Viktorovich Kutsaev
Elena Mikhailovna Sivokha
Mikhail Vasilievich Artemchuk

Military Institute of Telecommunications and Informatization named after Heroes Krut, Kiev, Ukraine

The article proposes an algorithm for the actions of the system administrator to counteract attempts at unauthorized encryption of information in information systems.

The relevance of the development of such measures is that the number of ransomware attacks reaches 30 percent of the total number of cyber incidents in the world. Massive attacks occur every six months, and penetration techniques and encryption algorithms are constantly improving. According to the Cyber-Kill Chain model, attackers successfully achieve their 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 in advance in information systems software samples that will allow timely identification of signs of the beginning of unauthorized encryption of information in systems.

The measures provide for the advance placement in systems of samples of special software that are able to implement "constant program monitoring" of processes in the system, stop the processor when signs of

encryption are detected, namely: when the processor is overloaded, when suspicious processes are detected, when signs of the encryption algorithm are detected when important files disappear simultaneously, when an unauthorized system reboot is attempted, and other signs. The authors compare the cyber defense of systems without and with the proposed measures. The authors believe that the cyber defense of systems will increase to 0.99 depending on the effectiveness of the measures involved.

The conclusion of the article is that the advance placement of specialized software in systems will allow timely blocking of the ransomware virus and increase the security of systems.

Further directions of research will allow the dissemination of the proposed measures to neutralize the actions of various classes of cyber attacks, which were achieved according to the Cyber-Kill Chain model of the target machine.

Key words: *ransomware virus, cyberattack, cyber defense, Cyber Kill Chain, information system.*

References

1. Extended Cyber-Kill Chain model and why it should be taken into account in the defense strategy. https://habr.com/ru/company/panda/blog/327488/ **2.** New time Protect yourself. Everything you need to know about the Petya.A virus. https://nv.ua/ukr/techno/gadgets/zahisti-sebe-sam-vse-shcho-potribno-znati-pro-virus-petya-a-1392163.html **3.** Vesti Ukraine Everything we know about WannaCry and Petya.A. https://vesti.ua/mir/244843-vse-chto-izvestno-o-viruse-wannacry-i- **4.** Tech today Everything You Need to Know About Petya and How to Fight It. https://techtoday.in.ua/ru/reviews-ru/vse-chto-nuzhno-znat-o-viruse-petya-kak-s-nim-borotsya-75861.html **5. Kotenko I.V.,** Saenko I.B., Doinikova E.V. (2013), Risk assessment in computer networks of critical infrastructures. [*Otsenka riskov v komp'yuternykh setyakh kriticheskikh infrastruktur*], Novosibírs'k, Innovatsii v nauke: zb. nauk. pr. / XVI mízhnar. nauk.-prakt. konf., Chast. I, SibAK, №16-1. pp. 84 - 88. **6. Davidyuk A.V.** Petrik V.M., (2018), Countering automated means of using social engineering. [*Protidiya avtomatizovanim zasobam v ispol'zovanii sotsial'noy inzhenerii*], Kiïv, Aktual'ní problemi upravlínnya ínformatsíynoyu bezpekoyu derzhavi: zb. tez nauk. dop. nauk. prakt. konf., Nats. akad. SBU, pp. 346 - 347. **7. Korchenko A.,** Dreys YU., Roshchuk M., Romanenko O. (2018), Consequence evaluation model of leak the state secret from cyberattack directing on critical information infrastructure of the state. [*Model' otsenki posledstviy utechki gosudarstvennoy tayny ot kiberataki, napravlennoy na kriticheskuyu informatsionnuyu infrastrukturu gosudarstva*], Ukr. nauch. zhur. inf. bez., vyp. 24, pp. 29-35. **8. Shevchenko A.S.** (2018), Mechanisms for detecting cyber attacks based on Schuhart control charts. [*Mekhanízmi viyavlennya kíberneticheskikh atak na osnoví kontrol'nikh kart Shukharta*], Kiïv, Aktual'nyye problemy upravleniya ínformatsíynoyu bezpekoyu derzhavi: zb. tez nauk. dop. nauk.-prakt. konf., Nats. akad. SBU, pp. 186 - 189. **9.** New dangerous encryption virus. https://molbuk.ua/news/201684-fakhivci-znayshly-novyy-nebezpechnyy-virus-shyfruvalnyk.html **10.** Recommendations for the elimination of the effects of Petya.A virus. [*Rekomendatsii po snizheniyu nasledovaniya vírusu Petya.A*], available at:https://novynarnia.com/2018/11/17/cert-ua.html. **11. Kutsaêv V.V.** Radchenko M.M. (2018), Methods for assessing the cyber security of information and telecommunications nodes. [*Metodika otsínki kíbernetichnoí zashchishcheností informatsíyno-telekomunikatsíynogo vuzla*], Kiïv, zb. nauk. pr. VÍTÍ. №2. **12. Kutsaêv V.V.,** Kozubtsov Í.M. (2017), Expert assessments of system security by Saati method. [*Yekspertní otsínki zashchishcheností sistem metodom Saatí*], Kiïv, zb. nauk. pr.VÍTÍ, №3. **13. Cherednichenko O.M.,** Kutsaêv V.V., Guk O.M., Shugalíy O.O., (2018), Analysis of cyber incidents on the territory of Ukraine and basic methods of cyber protection against them. [*Analiz kiberneticheskikh infektsiy na teritorii Ukrainy i osnovnyye metody kibernetichnogo zarazheniya víd nikh*], Kiïv, zb. nauk. pr. VÍTÍ, №3.