NETWORK AND APPLICATION SECURITY

УДК 004.056.53

ІГОР СУБАЧ,
ВІТАЛІЙ ФЕСЬОХА,
НАДІЯ ФЕСЬОХА

АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ЗАПОБІГАННЯ ВТОРГНЕННЯМ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІ МЕРЕЖІ

У статті представлено огляд сучасного стану кібернетичного простору в контексті зростання випадків кіберзлочинності (масштабних кібернетичних атак, що набули широкого розголосу в Україні та світі). Наведено порівняльний аналіз основних існуючих програмних рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі, які відкриті на основі загальнодоступних ліцензій. Наведено характеристики основних методів виявлення атак (вторгнень) та виділено їхні основні недоліки: відсутність адаптивності, стійкості та верифікованості, високий рівень помилкових спрацьовувань та пропусків кібернетичних атак, слабкі можливості щодо виявлення нових атак, відсутність можливості визначення атаки на її початкових етапах, практична відсутність можливості ідентифікації атакуючого й визначення цілі атаки, складність виявлення вторгнень у режимі реального часу, значне завантаження системи та слабка інтерпретація поточної ситуації. Запропоновано перспективні шляхи їх усунення, які ґрунтуються на застосуванні гібридних інтелектуальних систем запобігання вторгненням, в основу яких покладено методи інженерії знань, математичний апарат теорії нечітких множин та нечіткого логічного виводу, а також методи та технології інтелектуального аналізу даних. Отримані результати завдяки цьому можна розглядаються як підґрунтя для реалізації нових механізмів ідентифікації кібернетичних атак та застосування їх під час реалізації систем виявлення вторгнень наступного покоління з метою реагування на раніше невідомі типи кібернетичних атак. Це дозволить підвищити оперативність та обґрунтованість рішень, які приймає адміністратор безпеки інформаційно-телекомунікаційних систем та мереж в режимі реального часу під час виявлення та запобігання кібернетичним атакам.

Ключові слова: кібернетичний простір, інформаційно-телекомунікаційна мережа, кібернетична безпека, кібернетична атака, система запобігання вторгненням, нечіткі множини, інтелектуальний аналіз даних.

Вступ. Постійна модифікація форм та способів реалізації основних загроз об’єктам критичної інфраструктури держави – кібернетичних атак (КА) в умовах неконтрольованого поширення та необмеженого використання інформаційного простору все більше спонукають до перенесення протиправної діяльності у віртуальний простір.

Виходячи з цього, в рамках концепції інформаційного протиборства зростають вимоги до систем захисту сучасних інформаційно-телекомунікаційних систем та мереж (ІТМ), які повинні забезпечувати не тільки виявлення КА та реагування на них з метою блокування їх деструктивного впливу, а й в активній фазі ідентифікування вторгнення на початкових його етапах, адаптування до невідомих атак та в ідеальному випадку усунення їх в автоматичному режимі.

Одним із ефективних засобів захисту є системи виявлення атак (запобігання вторгненням) (СВА/СЗВ) – програмні або апаратні засоби, які призначені для виявлення фактів неавторизованого доступу у комп’ютерну систему або мережу та несанкціонованого керування ними. Проте, незважаючи на той факт, що у теперішній час питанням побудови СЗВ присвячено велику кількість наукових праць, питання ефективного застосування їх для побудови системи кібернетичного захисту, залишається повністю не вирішеними.

Це обумовлює актуальність подальших наукових досліджень, які полягають у підвищенні ефективності застосування СЗВ на основі розробки та впровадження нових методів виявлення КА [1].

Метою статті є проведення порівняльного аналізу застосування існуючих СЗВ, відкритих на основі загальнодоступних ліцензій (*Open Source*), а також визначення основних недоліків методів виявлення атак, що реалізовані у них.

Актуальність роботи. В умовах тотальної інформатизації всіх сфер діяльності суспільства і відсутності фактичних кордонів у кібернетичному просторі спостерігається стрімке зростання актів кібертероризму та кіберзлочинів [2].

Не випадково питання кібернетичної безпеки (КБ) все більше актуалізується та розглядається як стратегічний напрямок держави, оскільки робота уряду, діяльність комерційних структур та забезпечення національної безпеки держави з кожним роком все більше залежать від інформаційних технологій (ІТ) та інфраструктур, що функціонують у кіберпросторі [3]. Так, однією з масштабних та таких, що набула широкого розголосу в Україні та світі, стала КА групи хакерів "*Sandworm*" на критичну інфраструктуру енергетичного комплексу України, зокрема енергосистему ПАТ "Прикарпаттяобленерго" 23 грудня 2015 року, внаслідок якої на значній території Івано-Франківської області було відключено майже тридцять підстанцій, а 230 тисяч осіб залишилось без світла (див. рис.1) [4], [5].

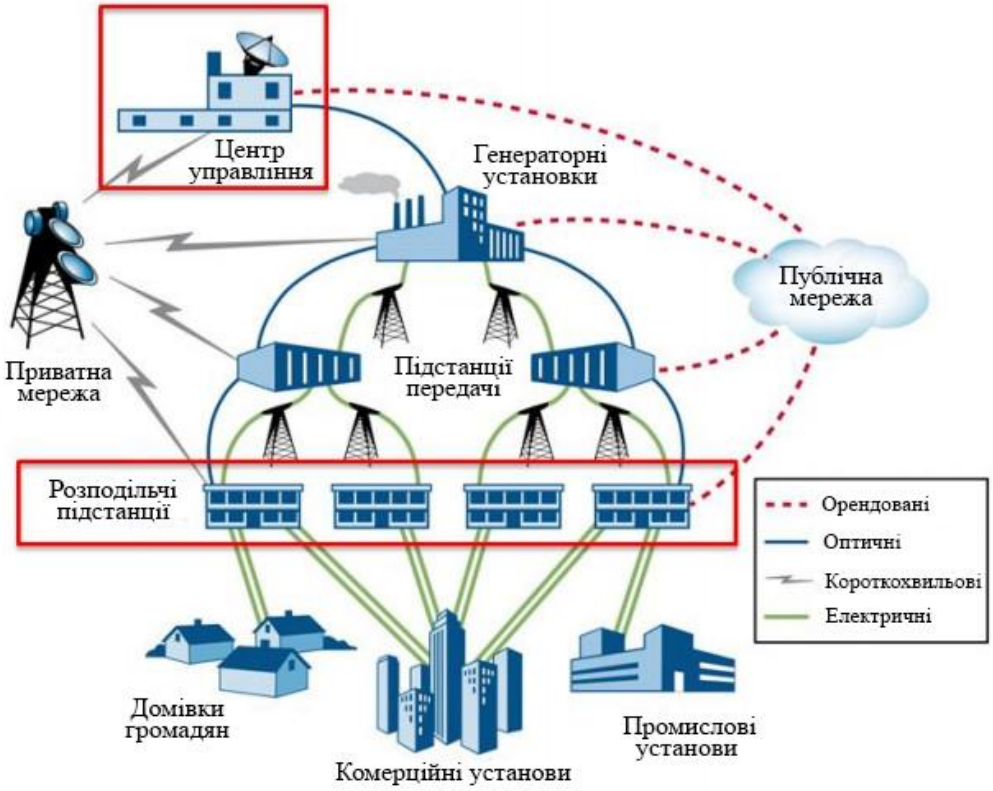

Рисунок1 – Об'єкти кібернетичної атаки на ПАТ "Прикарпаттяобленерго"

Унаслідок КА 6 грудня 2016 року було виведено з ладу мережу Державної казначейської служби та Міністерства фінансів, що призвело до порушення казначейського обслуговування розпорядників і одержувачів бюджетних коштів. Трапилася надзвичайна подія в системі, де зазвичай здійснюється близько 150 тисяч електронних транзакцій за добу.

Національна, кіберполіція, а також Служба безпеки України розслідують КА на сайт "Укрзалізниці", що відбулися в ніч з 14 на 15 грудня 2016 року, внаслідок якої було тимчасово призупинено роботу її ІТ-систем. "Укрзалізниця" перейшла на друковані документи для обслуговування клієнтів, а також традиційні способи комунікації, зокрема, телеграфний зв'язок, а також розповсюдила серед машиністів друковані попередження [6].

Аналіз стану кібернетичного простору України свідчить про велику інтенсивність КА на ресурси сектору критичної інфраструктури держави. Тільки впродовж останніх двох місяців

2016 року на об’єктах п’яти відомств і 31 державного інформаційного ресурсу було здійснено близько 6500 спланованих кібернетичних атак, а до початку 2017 року їх кількість зросла до 7000. Всі ці виклики та загрози кібернетичній безпеці держави призвели до появи Стратегії кібернетичної безпеки України, що була введена в дію указом Президента України від 15 березня 2016 року, метою створення якої є забезпечення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства та держави.

Не менш занепокоєними є країни Західної Європи та Північної Америки. Так, під час президентських виборів у США групою кібернетичних злочинців (КЗ) була спланована інформаційна кампанія на підтримку Дональда Трампа і дискредитацію його суперника від Демократичної партії Гілларі Клінтон.

Спроби групи КЗ викрасти дані в сфері оборони і закордонних справ Великобританії (близько 60-ти кібернетичних атак щомісяця) – група інцидентів отримала назву “онлайн-агресія”.

Організація КА на Національне Міністерство закордонних справ Італії. Згідно з повідомленням, КА тривали кілька місяців чим викликали регулярні порушення в роботі електронної пошти даного відомства [7].

Також кібернетична зброя стала доступним та ефективним інструментом досягнення злочинних цілей для організованих кримінальних та терористичних угрупувань. Прикладом діяльності останніх є постійні повідомлення про успішні, хоч і недостатньо масштабні та критичні КА, що проводить угрупування “Кіберхаліфат” в інтересах терористичної організації “ІДІЛ” та спрямовує свої сили проти організацій та урядів інших держав [3].

Порівняльний аналіз та дослідження існуючих програмних рішень запобігання вторгненням, відкритих на основі загальнодоступних ліцензій [1], [8], [9]. З метою дослідження характеристик СВА/СЗВ, які характеризують їх здібність до виявлення відповідних класів атак застосовують критерії, які представлені на рис. 2 [1], [8], [9].

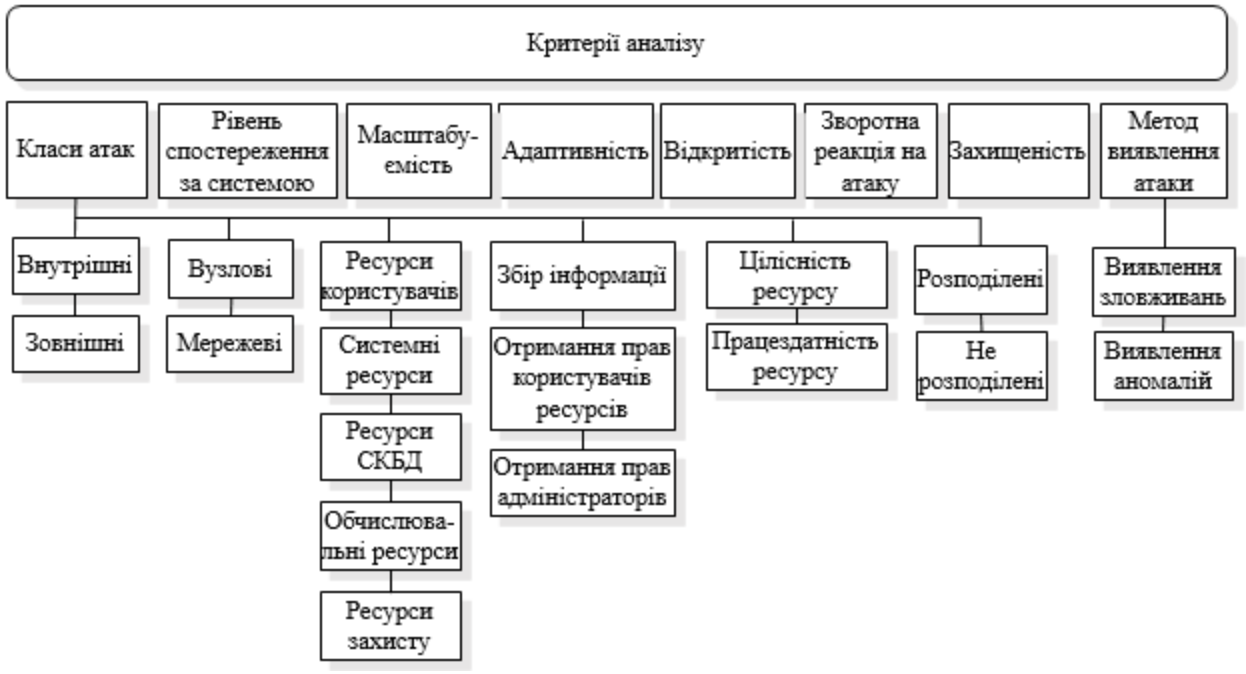

Рисунок 2 – Критерії порівняльного аналізу СВА/СЗВ

Аналіз наведених критеріїв показує, що найбільш ефективною можна вважати СЗВ, яка: є повною (покриває всі класи атак); дозволяє аналізувати поведінку ІТМ, яка захищається, на всіх рівнях (мережевому, вузловому, окремих додатків тощо); є адаптивною до раніше невідомих типів атак; масштабується для різних класів ІТМ (від локальних до корпоративних); є відкритою; має вбудовані механізми реагування на атаки; є захищеною від атак на свої компоненти. В табл. 1 приведено коротку інформативну довідку про найбільш розповсюджені СВА , аналіз функціонування яких та можливості розглядаються в роботі.

Таблиця 1 – Сучасні відкриті програмні рішення запобігання вторгненням

Найменування системи	Операційна система	Виробник	Офіційний веб-сайт
Bro	Linux	Vern Paxson	https://www.bro.org/
OSSEC	FreeBSD, Linux, UNIX, Mac OS X, Microsoft Windows	Daniel B. Sid , OSSEC.net	http://ossec.github.io/
Prelude	Linux, BSD, Windows	CS Group C-S	http://www.prelude-siem.com/
Suricata	FreeBSD, Linux, UNIX, Mac OS X, Microsoft Windows	Open Information Security Foundation	https://suricata-ids.org/

Bro [8], [10] є відкритою системою пасивного моніторингу мережевого трафіку і пошуку підозрілої активності. Виявлення атак виконується на декількох рівнях: вхідний мережевий трафік розбирається для виявлення семантики рівня додатків, після чого отримана траса подій прикладного рівня аналізується набором подійно-орієнтованих аналізаторів і порівнюється з шаблонами атак. Спеціалізована мова управління політиками, дозволяє налаштовувати поведінку системи у відповідності до поточних зовнішніх умов. При виявленні атаки система може виконати різні дії – записати повідомлення в журнал, оповістити оператора, виконати команди операційної системи. Призначенням системи є високошвидкісне виявлення атак на мережевих каналах з високою пропускною здатністю.

OSSEC [8], [11] є відкритою вузловою СВА. В її завдання входить: аналіз журналів, контроль цілісності, виявлення закладок, оповіщення про атаки і активна реакція на них. Система може бути встановленою як в одиночній конфігурації на одному вузлі, так і в розподіленій конфігурації на декількох вузлах – в такому випадку одна з інсталяцій стає сервером, а інші – агентами системи. При цьому управління агентами виконується централізовано з сервера. До її складу входять декілька різних аналізаторів. Аналізатор журналів використовує файли журналів типових додатків для UNIX-систем, системні журнали Windows і деяких додатків. Модуль виявлення закладок сканує файлову систему вузла і шукає відомі закладки по сигнатурам, а також невідомі на основі виявлення аномалій. Модуль контролю цілісності виконує перевірку найбільш критичних системних файлів (виконувані, конфігураційні, файли бібліотек). При першому запуску даний модуль створює базу даних (БД) критичних файлів, і зберігає в ній інформацію цілісності: параметри доступу, розмір, інформацію про власників, контрольні суми, періодично скануючи систему і порівнюючи системні файли з копіями в БД.

Prelude [8], [12] є гібридною системою з відкритими вихідними текстами та складається з наступних компонентів:

- мережеві сенсори, що аналізують дані на рівні мережі на основі сигнатурного аналізу. Сенсори генерують повідомлення про виявлення атак і відправляють їх до модулів управління. Система використовує в якості мережевого сенсора систему Snort;
- вузлові сенсори рівня системи, що аналізують журнали реєстрації ОС, додатків. Сенсори генерують повідомлення про виявлення аномалій і відправляють їх модулям управління. Існуючий набір сенсорів дозволяє аналізувати дані журналів реєстрації таких систем і додатків, як міжмережевий екран IPFW, NetFilter, маршрутизатори Cisco і Zyxel, GRSecurity, і типові сервіси операційної системи UNIX;
- модулі управління – процеси, які отримують і обробляють повідомлення сенсорів. Відповідають за реєстрацію повідомлень в журналах реєстрації або базах даних, аналізують повідомлення і генерують можливу реакцію системи на атаку. Можливі такі види реакції як блокування порушника засобами міжмережевого екрану, ізоляція порушника і звуження пропускної здатності каналу порушника;
- агенти реагування реалізують згенеровану менеджером реакцію на атаку.

Suricata [13] є системою виявлення і попередження мережевих вторгнень, альтернатива проекту Snort. По замовчуванню працює в багатопотоковому режимі, що дозволяє оптимально

використовувати кілька процесорів. Як і Snort, складається з декількох модулів (захоплення, збору, декодування, виявлення і виведення), до декодування захоплений трафік йде одним потоком, що оптимально з точки зору детектування але більше навантажує систему. Для перехоплення трафіку використовується кілька інтерфейсів, один з яких дозволяє автоматично аналізувати PCAP-файли, попередньо згенеровані іншою програмою, наприклад сніфером. Релізовано режим блокування шкідливого трафіку, що проводиться засобами штатного пакетного фільтра ОС. Система дозволяє використовувати два режими: через чергу NFQUEUE, яка обробляється на рівні користувача, і через режим AF_PACKET, що вимагає наявності двох мережевих інтерфейсів, оскільки система повинна працювати в якості шлюзу.

Проте, проведений аналіз за наведеними критеріями показує, що на сьогоднішній день жодна з СЗВ з відкритим кодом не відповідає у повній мірі сформульованим критеріям, зокрема завдяки відсутньої адаптації до невідомих типів атак та неможливості аналізувати поведінку ІТМ на всіх рівнях одночасно (див. табл. 2).

Таблиця 2 – Результати аналізу СЗВ

	Bro	OSSEC	Prelude	Suricata
Класи атак:				
Внутрішні	+	+	+	+
Зовнішні	+	-	+	+
Вузлові	-	+	+	+
Мережеві	+	-	+	+
Ресурси користувачів	+	+	+	+
Системні ресурси	+	-	+	+
Ресурси СКБД	-	-	-	-
Обчислювальні ресурси	-	-	-	-
Ресурси захисту	-	-	+	-
Отримання прав доступу	+	+	+	+
Цілісність ресурсу	-	-	-	-
Порушення працездатності	+	+	+	+
Розподілені	+	+	-	+
Нерозподілені	+	+	+	+
Рівень спостереження за системою	Системний	Системний	Системний, мережевий	Системний, мережевий
Метод виявлення	Сигнатурний	Сигнатурний	Сигнатурний	Сигнатурний
Адаптивність	-	+/-	-	-
Масштабованість	-	+	+	+
Відкритість (API)	+	+	+	+
Реакція	-	-	-	+

Аналіз існуючих методів запобігання вторгненням [8], [9], [14] - [20]. Проведені дослідження показують, що методи виявлення КА у сучасних СВА/СЗВ недостатньо повно опрацьовані з точки зору стійкості, адаптованості та верифікації, а також достатньо складно оцінити їхні властивості такі, як обчислювальна складність та коректність.

Класифікація відомих методів виявлення КА наведена на рис. 3. Серед них найбільш поширеними методами є:

сигнатурний аналіз: найбільш часто використовуване сімейство методів, суть яких полягає в складанні алфавіту на основі подій, що відстежуються в системі та описі сигнатур атак у вигляді регулярних виразів в побудованому алфавіті. Як правило, сигнатурні методи працюють на найнижчому рівні абстракції і аналізують безпосередньо мережеві дані, параметри системних викликів і записи файлів журналів. Метод не є адаптивним;

аналіз систем станів: у цій групі методів процес функціонування системи представляється у вигляді орієнтованого графа. Суть методу ідентифікації атак полягає в тому, що частина шляхів в графі позначаються як неприпустимі; кінцевий стан кожного такого шляху вважається небезпечним для системи. Виявлення послідовності переходів, що приводить в небезпечний стан означає успішне виявлення атаки;

Рисунок 3 – Існуючі методи виявлення атак/вторгнень

графи сценаріїв атак: на вхід системі верифікації поступає кінцева модель системи, яка захищається та деяке формальне правило коректності, яке виконується тільки для дозволеної поведінки системи та яке розділяє усю множину її поведінок на два класи: допустимої поведінки, для якого правило виконується та недопустимої, у протилежному випадку;

методи, засновані на специфікаціях: в основу цього методу покладено опис обмежень на заборонене поводження об'єктів в системі у вигляді специфікацій атак. До специфікації може входити: обмеження на завантаження ресурсів, на список заборонених операцій і їх послідовностей, на час доби, протягом якого застосовуються ті чи інші обмеження. Відповідність поведінки специфікації вважається атакою;

методи на сплайнах: метод оперує у багатовимірному просторі ознак, де поведінка мережевих об'єктів відображується у послідовності векторів даного простору, причому задача виявлення атаки полягає у побудові оптимальної апроксимації поведінки за заданою історією у вигляді навчальної множини векторів, при цьому у якості апроксимуючої функції застосовуються сплайни із змінним числом вершин;

експертні системи: виявлення атак засноване на описі функціонування системи у вигляді множини фактів і правил виведення, в тому числі для вторгнень. На вхід експертна система отримує дані про спостережувані події в системі у вигляді фактів. На підставі фактів і правил виведення система робить висновок про наявність чи відсутність атаки. Дана група методів має дуже велику обчислювальну складність, так як для неї може спостерігатися явище «комбінаторного вибуху» і повного перебору великого числа альтернатив;

мережі Петрі: функціонування системи передбачає запуск переходів та визначається як $<P, T, I, O, \mu>$, де P і T - кінцеві множини позицій і переходів; I та O - множини вхідних і вихідних функцій, μ - маркування. Формально робота мережі Петрі описується множиною послідовностей запусків і реалізованих маркувань. Кожному виду атак відповідає конкретна мережа Петрі. Якщо ці умови існують, то можна стверджувати, що атака точно виявлена, у випадку їх відсутності – атака відсутня або присутня з деякою часткою ймовірності;

генетичні алгоритми: методи, в основу функціонування яких покладено механізм біологічного принципу природного відбору в популяції (множина хромосом, кожна з яких моделюється у вигляді бітового рядку). Застосування генетичних алгоритмів для виявлення атак в якості елементів популяції виступають вектора певної довжини, кожен елемент яких відповідає певній атаці. В результати розвитку такої популяції можна отримати оптимальний вектор, який буде вказувати на те, які атаки відбуваються в системі в поточний момент;

нейронні мережі: для виявлення аномалій навчаються протягом деякого часу. Після навчання мережа запускається в режимі розпізнавання. У ситуації, коли у вхідному потоці не вдається розпізнати нормальну поведінку, фіксується факт атаки. У разі використання репрезентативної навчальної вибірки нейронні мережі дають достатню стійкість в межах заданої системи; але складання подібної вибірки є серйозним і складним завданням;

імунні мережі: також як і нейронні мережі, імунні мережі є механізмом класифікації і будуються за аналогією з імунною системою живого організму. Основна перевага імунних мереж полягає у можливості отримання "антитіл" до невідомих атак. Проте, використання даного методу дає велику обчислювальну складність;

нечітка логіка: метод на основі теорії нечітких множин використовується для формалізації неточних знань та виконання наближених міркувань в тій чи іншій області, яка досліджується. Дозволяє визначити проміжні значення для загальноприйнятих оцінок (так | ні, істинно | хибно). Метод є ефективним для дослідження об'єктів, ідентифікація яких занадто трудомістка, розмита, а також у випадках, коли за умовами задачі необхідно використовувати знання експерта;

метод опорних векторів: дозволяє побудувати функцію, яка вирішує задачу класифікації, при цьому, для виявлення атак формується вектор ознак, а далі – здійснюється навчання та побудова класифікатора, в результаті чого отримана функція здійснює класифікацію векторів-ознак і, таким чином, розпізнає до якого класу відноситься дія програмного забезпечення чи користувача: правомірного чи забороненого;

дерева рішень: метод вирішення завдань класифікації, що структурно складається з елементів трьох категорій (вузли - атрибути, за якими розрізняють елементи; листя - мітки зі значеннями рішень для класифікації; ребра - значення атрибута, з якого виходить ребро). Процес класифікації здійснюється шляхом послідовного проходження по дереву зверху вниз. На кожному рівні дерева рішення приймається на основі значень атрибутів. Результат оцінки завжди відповідає тільки одному з ребер, що виходить з вузла прийнятих рішень;

мережі Баєса: модель, що надає механізм для обчислення умовних ймовірностей настання розглянутих подій. Дозволяє оцінити апостеріорну ймовірність приналежності екземпляра заданому класу на основі безумовної теореми Баєса. Для цього застосовуються оціночні функції для визначення апріорних і апостеріорних ймовірностей нових атак, а наївний баєсовский класифікатор використовується для класифікації мережевих зразків;

роєві алгоритми: сімейство методів, в основу яких покладено моделювання поведінки та взаємодії біологічних особин (мурах, бджіл) в роях (зграях). Окрім ефективного застосування для рішення задач пошуку оптимальних маршрутів на графах їх також застосовують для вирішення задач класифікації вторгнень в ІТМ;

алгоритми регресії: даний метод використовується для прогнозу, аналізу часових рядів, тестування гіпотез і виявлення прихованих взаємозв'язків в досліджуваних даних, що складаються з пар значень залежної і незалежної змінних. Регресійна модель є функцією незалежної змінної і параметрів з доданою випадковою змінною. Параметри моделі налаштовуються таким чином, щоб модель найкращим чином наближала дані. Критерієм якості наближення є середньоквадратична помилка: сума квадратів різниці значень моделі і залежної змінної для всіх значень незалежної змінної в якості аргументу;

статистичний аналіз: сімейство методів засноване на побудові статистичного профілю поведінки системи протягом деякого періоду «навчання», при якому її поведінка вважається нормальною. Для кожного параметра функціонування системи будується інтервал допустимих значень, з використанням відомого закону розподілу. Далі система оцінює відхилення спостережуваних значень від значень, отриманих під час навчання. Якщо відхилення перевищують деякі задані значення, то фіксується факт аномалії (атаки);

вейвлет-аналіз: суть методу полягає в побудові коефіцієнтів розкладання вихідного сигналу (інтенсивність мережевого трафіку, дані про кореляцію IP-адрес призначення) по базисних функціях. Виконання вейвлет-перетворення дозволяє виділити найбільш вагому інформацію як сигнал, відповідний коливанню з високою амплітудою, й ігнорувати менш корисну інформацію з низькою амплітудою як шумову складову. Наявність різких амплітуд в кожному з представлених сигналів відповідає аномаліям;

кластерний аналіз: суть даної групи методів полягає в розбитті множини спостережуваних векторів-властивостей системи на кластери, серед яких виділяють кластери нормальної поведінки. У кожному конкретному методі кластерного аналізу використовується своя метрика, яка дозволяє оцінювати приналежність спостережуваного вектора властивостей одному з кластерів або вихід за межі відомих кластерів;

спектральний аналіз: метод дозволяє виділяти найбільш інформативні складові досліджуваного процесу за допомогою зміни розмірності вихідного простору ознак. Аналізується матриця елементів досліджуваного процесу за допомогою методу головних компонент або сингулярного спектрального аналізу. Отримані компоненти аномального трафіку відрізняються від компонент звичайного;

фрактальний аналіз: даний метод заснований на припущенні, що мережевий трафік задовольняє властивості самоподібності, ключовими поняттями в якому є параметр Херста – H і фрактальна Хаусдорфова розмірність. Для самоподібних процесів виконується співвідношення $0,5 < H < 1$;

аналіз ентропії: суть методу полягає в побудові моделі, яка максимізувала б значення ентропії. Застосовується метод максимуму ентропії для створення нормальної моделі, в якій виділені класи мережевих пакетів з найкращим рівномірним розподілом. Далі застосовується умовна ентропія для виявлення відмінностей між розподілом класів пакетів в поточному трафіку в порівнянні з розподілом, знайденим в результаті методу максимуму**;**

біометрія поведінки: ґрунтується на результатах спостереження клавіатурного почерку та використання комп'ютерної миші, а також гіпотези про відмінність почерку роботи з інтерфейсами вводу-виводу для різних користувачів.

Результати порівняльного аналізу методів виявлення КА показують, що для більшості поведінкових методів характерним недоліком є слабка верифікованість та стійкість. З іншого боку, основною їх перевагою є адаптивність та здатність виявляти раніше невідомі атаки. Основним недоліком методів на основі знань є слабка їх адаптивність до виявлення ще не класифікованих атак, а більшість методів ІАД є слабко верифікованими. Проте, серед них можна виділити методи, які показали найбільш повну відповідність заданим критеріям аналізу, є одночасно верифікованими, адаптивними та стійкими: експертні системи та методи на основі нечіткої логіки.

Результати проведених досліджень наведено в табл. 3, де H – спостереження на рівні вузла, N – спостереження на рівні мережевої взаємодії, HG – спостереження на різних рівнях.

Таблиця 3 – Результати аналізу

	Рівень спостереження	Аномалії/ зловживання	Верифікованість	Адаптивність	Стійкість	Обчислювальна складність
Сигнатурний аналіз	*HG*	-/+	+	-	+	*ln(n)*
Аналіз систем станів	*HG*	-/+	+	-	+	*> O(n)*
Графи сценаріїв атак	*HG*	-/+	+	+	+	*NP*
Методи на специфікаціях	*N*	-/+	+	-	-	*ln(n)*
Методи на сплайнах	*N,H*	-/+	-	+	-	*> O(n)*
Експертні системи	*N,H*	+/+	+	+	+	*NP*
Мережі Петрі	*HG*	-/+	+	-	+	*NP*
Генетичні алгоритми	*HG*	+/+	-	+	+	*ln(n)*
Нейронні мережі	*N,H*	+/+	-	+	-	*> O(n)*
Імунні мережі	*N,H*	+/+	-	+	-	*> O(n)*
Нечітка логіка	*N,H*	+/+	+	+	+	*> O(n)*
Метод опорних векторів	*N,H*	+/+	-	+	-	*ln(n)*
Дерева рішень	*N,H*	+/+	+	-	-	*NP*
Мережі Баєса	*N*	+/+	-	+	+	*> O(n)*
Роєві алгоритми	*N,H*	+/+	+	+	-	*P*
Регресійний аналіз	*HG*	+/+	-	+	-	*P*
Статичний аналіз	*N,H*	+/-	-	+	-	*> O(n)*
Вейвлет-аналіз	*N*	+/-	-	+	-	*NP*
Кластерний аналіз	*HG*	+/+	-	+	-	*> O(n)*
Спектральний аналіз	*N*	+/-	-	+	-	*NP*
Фрактальний аналіз	*N*	+/-	-	+	-	*> O(n)*
Аналіз ентропії	*N,H*	+/-	+	+	-	*> O(n)*
Біометрія	*H*	+/-	-	+	-	*> O(n)*

Недоліки існуючих рішень. Проведений аналіз методів і СЗВ дозволяє зробити висновок про відсутність СВА/СЗВ, яка мала б адаптивність до невідомих КА. Дані програмні рішення використовують на базовому рівні ту чи іншу реалізацію сигнатурного методу виявлення (запобігання) вторгненням. Реалізації відрізняються рівнем розгляду системи, алфавітом сигнатур, структурою, архітектурою і способом побудови сигнатур – від простого пошуку до повноцінної реалізації регулярних виразів над заданим алфавітом. Незважаючи на те, що існує велика кількість методів виявлення аномалій, їхня слабка стійкість, відсутність верифікації, велика кількість хибних спрацьовувань, вузька спеціалізація та дослідницький характер, не дозволяють широко їх використовувати.

Таким чином, основними недоліками існуючих рішень запобігання вторгненням є: існуючі методи виявлення КА не є одночасно адаптивними, стійкими та верифікованими; досить високий рівень помилкових спрацьовувань та пропусків КА; слабкий механізм виявлення нових КА; більшість вторгнень неможливо визначити на початкових етапах; практична відсутність змоги ідентифікації атакуючого та визначення цілі атаки; слабкий механізм виявлення відомих атак, що використовують нові стратегії; складність виявлення вторгнень у реальному часі з необхідною повнотою у високошвидкісних мережах; значне завантаження систем при роботі в реальному часі; слабка можливість інтерпретації адміністратором безпеки результатів поточної ситуації; видача результату, точність ідентифікації якого не завжди відома та ін.

Шляхи вирішення. Для усунення вищевказаних недоліків є доцільним проведення низки наукових досліджень щодо розробки адаптивних СЗВ, в основу функціонування яких необхідно покласти методи, які б при низькій обчислювальній складності та високій стійкості та верифікації мали б низькій рівень хибних спрацьовувань.

Проведений порівняльний аналіз методів виявлення КА демонструє перевагу експертних систем серед методів на основі знань, а методи на основі нечіткої логіки - серед методів ІАД. Важливою особливістю експертних систем є практично повна відсутність помилкових тривог. Проте, повний перебір великого числа альтернатив залишає за ним досить велику обчислювальну складність. До того ж, щоб залишатися актуальними, експертні системи вимагають постійного оновлення бази правил, оскільки навіть невелика модифікація вже відомої атаки може стати серйозною перешкодою для коректного функціонування СЗВ.

У зв’язку з цим перспективним підходом до вирішення розглянутого питання є створення гібридних інтелектуальних СЗВ, в основу функціонування яких необхідно покласти методи інженерії знань, математичний апарат теорії нечітких множин та нечіткого логічного виводу, а також методи та технології інтелектуального аналізу даних. Застосування наведеного математичного апарату дозволить створити нечітку базу знань (НБЗ) про кібернетичні атаки та виявляти їх шляхом застосування процедури нечіткого логічного виводу на основі початкових даних, що поступають в систему, а також організувати процес до навчання НБЗ завдяки реалізації процедури генерації нечітких логічних правил на основі аналізу даних з журналів роботи системи.

Досвід дослідної експлуатації СЗВ, що реалізовані на основі застосування наведеного підходу дозволяє досягнути більше 90% спрацьовувань системи на КА, причому лише 10% тестового набору використовувалося для створення бази нечітких правил [12]. Крім того, застосування математичного апарату нечіткої логіки та нечіткого логічного виводу дозволить вирішити складноформалізуєму задачу автоматизованої побудови раніше не відомих або модифікацію існуючих сигнатур КА.

Висновки. Порівняльний аналіз існуючих СВА/СЗВ та методів виявлення КА дозволяють зробити висновок про те, що в даний момент не існує відкритої загальнодоступної системи виявлення КА, яка б задовольняла всім вимогам, зокрема, була б адаптивною до невідомих типів атак. Незважаючи на наявність великої кількості методів виявлення аномалій, значна кількість помилкових спрацьовувань, їх слабка стійкість не дозволяє їх ефективно використовувати в ІТМ. Крім того, до теперішнього часу використання методів виявлення аномалій є обмеженим дослідними і вузькоспеціалізованими системами.

У контексті викладеного, актуальним шляхом вирішення даної задачі є розробка гібридної системи запобігання вторгненням, яка об'єднає можливості методів інженерії знань, методів теорії нечітких множин та нечіткого логічного виводу та моделей і методів інтелектуального аналізу даних. Об'єднання цих методів дозволить зберегти невисоку обчислювальну складність алгоритмів при виявленні зловживань і доповнити СЗВ властивістю адаптивності до невідомих типів кібернетичних атак.

Таким чином, запропоновані шляхи вдосконалення СЗВ є підґрунтям для реалізації нових механізмів ідентифікації КА та застосування їх під час реалізації систем виявлення вторгнень наступного покоління з метою реагування на раніше невідомі типи КА. У свою чергу, це дозволить підвищити оперативність та обґрунтованість рішень, які приймає адміністратор безпеки ІТМ в режимі реального часу під час виявлення та запобігання КА.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] І. Ю. Субач, "Шляхи удосконалення систем виявлення кібернетичних атак", на *Всеукр. наук.-практ. конф. Актуальні проблеми забезпечення інформаційної безпеки держави*, Київ, 2014, с. 112.

[2] "Годовой отчет Cisco по информационной безопасности за 2016 год". [Электронный ресурс]. Доступно: http://www.cisco.com/c/dam/m/ru_ru/internet-of-everything-ioe/iac/assets/pdfs/security/cisco_2016_asr_011116_ru.pdf/. Дата обращения: Февр., 06, 2017.

[3] С. Радкевич, "Кібербезпека як ключовий елемент протидії гібридній агресії". [Електронний ресурс]. Доступно: http://cacds.org.ua/ru/safe/theme/870. Дата звернення: Січ., 23, 2017.

[4] "Analysis of the Cyber Attack on the Ukrainian Power Grid". [Online]. Available: https://ics.sans.org/media/E-SAC_SANS_Ukraine_DUC_5.pdf. Accessed on: March, 01, 2017.

[5] "Cyber-Attack Against Ukrainian Critical Infrastructure", [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01. Accessed on: Febr. 25, 2016.

[6] "Кибератака на "Укрзализныцю". [Электронный ресурс]. Доступно: https://www.depo.ua/rus/politics/kibeataka-na-ukrzaliznitsyu-postavila-na-vuha-natspolitsiyu-16122016143800. Дата обращения: Февр., 13, 2017.

[7] "Глава МИД Италии признал факт хакерских атак на министерство". [Электронный ресурс]. Доступно: http://tass.ru/mezhdunarodnaya-panorama/4015482. Дата обращения: Февр., 13, 2017.

[8] Д. Ю. Гамаюнов, "Обнаружение компьютерных атак на основе анализа поведения сетевых объектов", диссертация кандидата наук, Факультет вычислительной математики и кибернетики, Московский государственный университет имени М.В. Ломоносова, Москва, 2007.

[9] О. И. Шелухин, Д. Ж. Сакалема, и А. С. Филинова, *Обнаружение вторжений в компьютерные сети (сетевые аномалии)*. Москва, Россия: Горячая линия – Телеком, 2016.

[10] "The Bro Network Security Monitor". [Online]. Available: https://www.bro.org. Accessed on: Febr., 06, 2017.

[11] "OSSEC". [Online]. Available: http://ossec.github.io. Accessed on: Febr., 06, 2017.

[12] "Prelude". [Online]. Available: http://www.prelude-siem.com. Accessed on: Febr., 06, 2017.

[13] "Suricata". [Online]. Available: https://suricata-ids.org. Accessed on: Febr., 06, 2017.

[14] A. D. Falke, V. S. Fulsoundar, R. S. Pawase, S. B. Wale, and S. J. Ghule, "Network Intrusion Detection System using Fuzzy Logic", *International journal of scientific research and education*, vol. 2, iss. 4, pp. 626-635, April 2014.

[15] T. Lappas, and K. Pelechrinis, "Data Mining Techniques for (Network) Intrusion Detection Systems". [Online]. Available: https://www.slideshare.net/Tommy96/data-mining-techniques-for-network-intrusion-detection-systems. Accessed on: Febr., 16, 2017.

[16] Т. И. Булдакова, и А. Ш. Джалолов, "Выбор технологий Data Mining для систем обнаружения вторжений в корпоративную сеть". Инженерный журнал: наука и инновации, № 11 (23), с. 1-14, 2013.

[17] A. Youssef, and A. Emam, “Network intrusion detection using data mining and network behaviour analysis”, *International journal of computer science & information technology*, vol. 3, no. 6, pp. 87-98, December 2011.
doi: 10.5121/ijcsit.2011.3607.
[18] А. А. Браницкий, и И. В. Котенко, “Анализ и классификация методов обнаружения сетевых атак”, *Тр. СПИИРАН*, вып. 45, с. 207-244, 2016.
doi: 10.15622/sp.45.13.
[19] Е. В. Зубков, и В. М. Белов, “Методы интеллектуального анализа данных и обнаружение вторжений”, *Вестник СибГУТИ*, № 1, с. 118-133, 2016.
[20] С. А. Петренко, “Методы обнаружения вторжений и аномалий функционирования киберсистем”, *Труды ИСА РАН*, том 41, с. 194-202, 2009.

Стаття надійшла до редакції 03 березня 2017 року.

REFERENCES

[1] I. Y. Subach, “Ways of improving the detection of cyber attacks”, at *National Scientific Conference. Actual problems of ensuring information security of the state*, Kyiv, 2014, pp. 112.
[2] “Cisco Annual Information Security Report for 2016”. [Online]. Available: http://www.cisco.com/c/dam/m/en_en/internet-of-everything-oe/iac/assets/pdfs/security/cisco_2016_asr_011116_en.pdf. Accessed on: Febr. 06,2017.
[3] S. Radkevych, ”Cyber security as a key element of combating hybrid aggression”. [Online]. Available: http://cacds.org.ua/ru/safe/theme/870. Accessed on: Jan. 23, 2017.
[4] “Analysis of the Cyber Attack on the Ukrainian Power Grid”. [Online]. Available: https://ics.sans.org/media/E-SAC_SANS_Ukraine_DUC_5.pdf. Accessed on: March, 01, 2017.
[5] “Cyber-Attack Against Ukrainian Critical Infrastructure”, [Online]. Available: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01. Accessed on: Febr. 25, 2016.
[6] “Cyberattack on “Ukrzaliznytsia”. [Online]. Available: https://www.depo.ua/rus/politics/kibeataka-na-ukrzaliznitsyu-postavila-na-vuha-natspolitsiyu-16122016143800. Accessed on: Febr., 13, 2017.
[7] “Italian Foreign Minister acknowledged the fact of hacker attacks on the ministry”. [Online]. Available: http://tass.ru/mezhdunarodnaya-panorama/4015482. Accessed on: Febr., 13, 2017.
[8] D. I. Gamaiunov, “Detection of computer attacks based on the analysis of the behavior of network objects”, Faculty of computational mathematics and cybernetics, Lomonosov Moscow state university, Moscow, 2007.
[9] O. I. Shelukhin, D. Z. Sakalema, and A.S. Filinova, *Detection of intrusions into computer networks (network anomalies)*. Moscow, Russia: Goriachaia liniia – Telekom, 2016.
[10] “The Bro Network Security Monitor”. [Online]. Available: https://www.bro.org. Accessed on: Febr., 06, 2017.
[11] “OSSEC”. [Online]. Available: http://ossec.github.io. Accessed on: Febr., 06, 2017.
[12] “Prelude”. [Online]. Available: http://www.prelude-siem.com. Accessed on: Febr., 06, 2017.
[13] “Suricata”. [Online]. Available: https://suricata-ids.org. Accessed on: Febr., 06, 2017.
[14] A. D. Falke, V. S. Fulsoundar, R. S. Pawase, S. B. Wale, and S. J. Ghule, “Network Intrusion Detection System using Fuzzy Logic”, *International journal of scientific research and education*, vol. 2, iss. 4, pp. 626-635, April 2014.
[15] T. Lappas, and K. Pelechrinis, “Data Mining Techniques for (Network) Intrusion Detection Systems”. [Online]. Available: https://www.slideshare.net/Tommy96/data-mining-techniques-for-network-intrusion-detection-systems. Accessed on: Febr., 16, 2017.
[16] T. I. Buldakova, and A. S. Dzhalolov, “Choosing Data Mining Technologies for Intrusion Detection Systems in the Corporate Network”, *Engineering journal: science and innovation*, no. 11 (23), pp. 1-14, 2013.

[17] A. Youssef, and A. Emam, “Network intrusion detection using data mining and network behaviour analysis”, *International journal of computer science & information technology*, vol. 3, no. 6, pp. 87-98, December 2011.
doi: 10.5121/ijcsit.2011.3607.
[18] A.A. Branitskii, and I. V. Kotenko, ”Analysis and classification of methods for detecting network attacks”, *SPIIRAS Proceedings*, iss., 45, pp. 207-244, 2016.
doi: 10.15622/sp.45.13.
[19] E. Zubkov, and V. Belov, “Methods of Data Mining and Intrusion Detection”, *Bulletin of SibGUTI*, no. 1, pp. 118-133, 2016.
[20] S. A. Petrenko, “Methods for detecting intrusions and anomalies of the functioning of cybersystem”, *Proceedings of ISA RAS*, no. 41, pp. 194-202, 2009.

ІГОРЬ СУБАЧ,
ВИТАЛИЙ ФЕСЁХА,
НАДЕЖДА ФЕСЁХА

АНАЛИЗ СУЩЕСТВУЮЩИХ РЕШЕНИЙ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ

В статье представлен обзор современного состояния кибернетического пространства в контексте роста случаев киберпреступности (масштабных кибернетических атак, которые получили широкую огласку в Украине и мире). Представлен сравнительный анализ основных существующих программных решений предотвращения вторжений в информационно-телекоммуникационные сети, открытых на основе общедоступных лицензий. Приведены характеристики основных методов обнаружения атак (вторжений). Выделены их основные недостатки: отсутствие адаптивности, стойкости и верифікованності, высокий уровень ошибочных срабатываний та пропусков кибернетических атак, слабые возможности по выявлению новых атак, отсутствие возможности определения атаки на ее начальных этапах, практическое отсутствие возможности идентификации атакующего и определения цели атаки, сложность определения вторжений в режиме реального времени, существенная загрузка системы и слабая интерпретация текущей ситуации. Предложены перспективные пути их устранения, в основы которых положено использование гибридных интеллектуальных систем предотвращения вторжений, которые строятся на основе методов инженерии знаний, математического аппарата теории нечетких множеств и нечеткого логического вывода, а также методов и технологий интеллектуального анализа данных. Полученные результаты благодаря этому можна рассматривать як основу для реализации новых механизмов идентификации кибернетических атак и применения их во время реализации систем обнаружения вторжений следующего поколения с целью реагирования на неизвесные типы кибернетических атак. Это позволит повысить оперативность и обоснованость решений, которые принимает администратор безопасности информационно-телекомунникационных систем и сетей в режиме реального времени во время виявления и предотвращения кибернетических атак.

Ключевые слова: кибернетическое пространство, информационно-телекоммуникационная сеть, кибернетическая безопасность, кибернетическая атака, система предотвращения вторжений, нечеткие множества, интеллектуальный анализ данных.

IHOR SUBACH,
VITALII FESOKHA,
NADIIA FESOKHA

ANALYSIS OF EXISTING SOLUTIONS FOR PREVENTING INVASION IN INFORMATION AND TELECOMMUNICATION NETWORKS

The article presents an overview of the current state of cybernetic space in the context of the growth of cybercrime (large-scale cyber attacks, which have received wide publicity in Ukraine and

the world). A comparative analysis of the main existing software solutions for the prevention of intrusions into information and telecommunications networks, based on public licenses. The characteristics of the main methods for detecting attacks (intrusions) are given. There is identified its main shortcomings: lack of adaptability, persistence and verification, high level of erroneous attacks, those misses of cyber attacks, weak opportunities to identify new attacks, lack of ability to determine the attack in its initial stages, practical lack of identification of the attacker and the purpose of the attack, in real time, a significant load of the system and a weak interpretation of the current situation. Prospective ways of their elimination based on the use of hybrid intelligent intrusion prevention systems based on the methods of knowledge engineering, the mathematical apparatus of fuzzy sets theory and fuzzy inference, as well as methods and technologies for data mining are proposed. Obtained results can be considered as a basis for the implementation of new mechanisms for identifying cybernetic attacks and their application during the implementation of intrusion detection systems of the next generation in order to respond to previously unknown types of cybernetic attacks. This will increase the efficiency and validity of the decisions taken by the security administrator of information and telecommunication systems and networks in real time during the detection and prevention of cybernetic attacks..

Keywords: cybernetic space, information and telecommunication network, cybernetic security, cybernetic attack, intrusion prevention system, fuzzy sets, data mining.

Ігор Юрійович Субач, доктор технічних наук, доцент, завідувач кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

E-mail: igor_subach@ukr.net.

Віталій Вікторович Фесьоха, ад'юнкт, Військовий інститут телекомунікацій та інформатизації, Київ, Україна.

E-mail: vitaha.fes@gmail.com.

Надія Олександрівна Фесьоха, викладач кафедри комп'ютерних інформаційних технологій, Військовий інститут телекомунікацій та інформатизації, Київ, Україна.

E-mail: nadya_viti@i.ua.

Игорь Юрьевич Субач, доктор технических наук, доцент, заведующий кафедрой кибербезопасности и применения автоматизированных информационных систем и технологий, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина.

Виталий Викторович Фесёха, адъюнкт, Военный институт телекоммуникаций и информатизации, Киев, Украина.

Надежда Александровна Фесёха, преподаватель кафедры компьютерных информационных технологий, Военный институт телекоммуникаций и информатизации, Киев, Украина.

Igor Subach, doctor of technical science, associate professor, head at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Vitalii Fesokha, postgraduate student, Military institute of telecommunications and informatization, Kiev, Ukraine.

Nadiia Fesokha, lecturer at the computer information technologies academic department, Military institute of telecommunications and informatization, Kiev, Ukraine.