УДК 621.396.933 (043.2) DOI: 10.31673/2412-4338.2019.041224

Галахов Є.М., Собчук В.В. *Державний університет телекомунікацій*

РОЗВИТОК МОДЕЛЕЙ КІБЕРАТАК У ПЛОЩИНІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Проблеми інформаційної безпеки обумовлюють дослідження уразливостей, моделей кібератак, які складаються з чотирьох груп: моделі кібератак на стандартне програмне забезпечення і пропрієтарні додатки; моделей кібератак на конфігурацію сервера, рівень виправлень сервера та моделей кібератак на мережеву інфраструктуру. Представлено відповідні уразливості і проблеми усіх груп кібератак на підприємство. Уразливості і проблеми на стандартне програмне забезпечення і пропрієтарні додатки включають аутентифікацію, авторизацію, бізнес-логіку, розкриття інформації, браузерні атаки, підстановки інтерпретатора управління станом, небезпечне управління довіреними даними, небезпечну функціональність, небезпечні алгоритми та відмову в обслуговуванні. Показано, що найбільш поширені вразливості програмного забезпечення трапляються внаслідок використання програмних помилок у пам'яті, перевірки введення користувачем, умов перегонів та привілеїв доступу користувачів. Уразливості і проблеми на мережеву інфраструктуру стосуються протоколу каналу передачі даних, шарів мережевого і транспортного протоколу, конфігурації файєрволу. Проаналізовано статистичні дані кібератак у полі діяльності ІТ-підприємства, що залучає фріланс-ресурс, для використання часових кореляцій між кількістю кібератак за часовий період для передбачення майбутніх інтенсивності кібер-інцидентів, що повинно створити ефективну систему прогнозування. Передбачення кількості кібератак за встановлений раціональний часовий період необхідне для визначення ефективної частоти аудиту. Виявлено і класифіковано віруси кібератак на веб-ураження та ураження електронної пошти та знайдена їх частка у загальній кількості кібератак. Досліджено часові ряди веб-загроз та уражень електронної пошти за певний період та їх згладжування за допомогою фільтрації за трьома точками часового ряду. Була проведена апроксимація згладжуваних відповідних часових рядів аналітичними функціями. Показано, що використання логістичної регресії дає можливість передбачити ризик виникнення хостів від зловмисного програмного забезпечення.

***Ключові слова**: кібератака, веб-загрози, електронна пошта, сервер, програмне забезпечення, віруси, часовий ряд, фільтрація, апроксимація.*

Галахов Е.М., Собчук В.В. *Государственный университет телекоммуникаций*

РАЗВИТИЕ МОДЕЛЕЙ КИБЕРАТАК В ПЛОСКОСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Проблемы информационной безопасности обусловливают исследования уязвимостей, моделей кибератак, которые состоят из четырех групп: модели кибератак на стандартное программное обеспечение и проприетарные приложения; моделей кибератак на конфигурацию сервера, уровень исправлений сервера и моделей кибератак на сетевую инфраструктуру. Представлены соответствующие уязвимости и проблемы всех групп кибератак на предприятие. Уязвимости и проблемы на стандартное программное обеспечение и проприетарные приложения включают аутентификацию, авторизацию, бизнес-логику, раскрытие информации, браузерные атаки, подстановки интерпретатора управления состоянием, опасное управления доверенными данным, опасную функциональность, опасные методы и отказ в обслуживании. Показано, что наиболее распространенные уязвимости программного обеспечения случаются вследствие использования программных ошибок в памяти, проверки ввода пользователем, условий гонки и привилегий доступа пользователей. Уязвимости и проблемы на сетевую инфраструктуру касаются протокола канала передачи данных, слоев сетевого и транспортного протокола, конфигурации файервола. Проанализированы статистические данные кибератак в поле деятельности ИТ-предприятия, которое привлекает фриланс-ресурс для использования временных корреляций между количеством кибератак за временной период для предсказания будущих интенсивности кибер-инцидентов, что должно создать эффективную систему прогнозирования. Прогнозирование количества кибератак в пределах установленного рациональный временной период необходимо для определения эффективной частоты аудита. Обнаружены и классифицированы вирусы кибератак на веб-поражения и

поражения электронной почты, а также найдена их доля в общем количестве кибератак. Исследованы временные ряды веб-угроз и поражений электронной почты за определенный период и их сглаживания с помощью фильтрации по трем точкам временного ряда. Была проведена аппроксимация сглаживаний соответствующих временных рядов аналитическими функциями. Показано, что использование логистической регрессии дает возможность предсказать риск возникновения хостов от вредоносных программ.

Ключевые слова: *кибератака, веб-угрозы, электронная почта, сервер, программное обеспечение, вирусы, временной ряд, фильтрация, аппроксимация.*

Halakhov Y.M., Sobchuk V.V. *State University of Telecommunications*

DEVELOPMENT OF MODELS OF CYBER ATTACKS IN THE PLANE ENTERPRISE INFORMATION SECURITY

Information security problems are caused by studies of vulnerabilities, models of cyberattacks, which consist of four groups: models of cyberattacks against standard software and proprietary applications; models of cyberattacks on the server configuration, the level of server patches, and cyberattack models on the network infrastructure. The corresponding vulnerabilities and problems of all cyber-attack groups at the enterprise are presented. Vulnerabilities and problems for standard software and proprietary applications include authentication, authorization, business logic, information disclosure, browser attacks, state management interpreter substitutions, dangerous trusted data management, dangerous functionality, dangerous methods, and denial of service. It is shown that the most common software vulnerabilities occur due to the use of software errors in memory, user input verification, race conditions and user access privileges. Generic server configuration vulnerabilities include configuration errors that could be exploited by cybercriminals in relation to all types of server software. Statistical data of cyberattacks in the field of activity of an IT enterprise is analyzed, which attracts a freelance resource to use temporal correlations between the number of cyberattacks over a time period to predict future intensity of cyber incidents, which should create an effective forecasting system. Predicting the number of cyberattacks within the established rational time period is necessary to determine the effective audit frequency. Cyber-attacks were detected and classified as cyber-attacks on web and email attacks, and their share in the total number of cyber-attacks was found. The time series of web threats and email attacks over a certain period and their smoothing by filtering by three points of the time series are investigated. An approximation of smoothing of the corresponding time series by analytical functions was carried out. It is shown that the use of logistic regression makes it possible to predict the risk of hosts against malware.

Keywords: *cyber-attack, web threats, email, server, software, viruses, time series, filtering, approximation.*

Вступ. Інформаційна безпека підприємства на даний час вимагає не тільки методичного забезпечення її ефективної реалізації, а і надання нових ідей для створення безпечного обчислювального, комунікаційного, соціального середовища. Уразливості, проблеми безпеки та моделі атак на конфігурацію сервера, рівень виправлень сервера, на мережеву інфраструктуру, на стандартне програмне забезпечення і пропрієтарні додатки потребують дослідження із зазначенням їх класифікації. Дослідження окресленої проблеми вимагає побудови емпірико-статистичних рядів розподілу вірусних атак на веб-сторінки та електронну пошту за встановлені часові періоди.

Аналіз останніх досліджень і публікацій.

На сьогодні є дослідження [10, 11] щодо моделей інформаційної безпеки підприємства, що стосуються її конкретних зон безпеки, як наприклад, безпека веб-розробки OWASP [12,14], що зосереджена на розробці захищеності коду і запобіганню кібератак. В той же час не розглядаються аспекти конфіденційності і управління кіберзагрозами.

Як зазначається у [13] не існує структурованої та об'єднаної інформації про найкращі практики інформаційної безпеки на підприємстві. Не вистачає інформації про інформаційну безпеки, яку, наприклад, розробник SaaS може використовувати як орієнтир, створюючи додаток Cloud SaaS [13].

Останні дослідження включають використання моделей часових рядів для

прогнозування кількості кібератак [14], що мотивує потребу у таких моделей для прогнозування кібератак. Автори в [14] використовують дані часових рядів для передбачення кібератаки у будь-який момент часу за допомогою контрольованої моделі навчання, у якій часовий ряд утворюється шляхом усереднення, що можна трактувати як бінарну проблему. У роботі [8] автори вивчаючи вплив поздовжньої розрідженості у даних часових рядів, пропонують підхід до надання вагомості однаковим характеристикам у різні моменти часу, що охоплює тимчасову надмірність.

У роботі [15] використовуються функції часових рядів для моделі навчання на основі логістичної регресії зі щоденною кібератакою за умови вивчення інформації про вразливість через центральні мережі та статистику розміщення на форумах.

Автори у роботі [7] наголошують про відбір даних про тип атаки, який називається типом події, дати події: дата нападу та конкретного типу події. Розглядаються типи подій, які використовуються в цьому дослідженні: зловмисні повідомлення електронної пошти стосується зловмисного програмного забезпечення. Автори доводять, що розподіл кібератак у часі відрізняється від подій.

У [16] методами перехресної перевірки розглянуто використання послідовної інформації при обчисленні функції інтенсивності кібератак, починаючи з інформації про період кібератаки, що надається, змінюється за часом для кожної з подій, при цьому використовуються різні часові рамки для тренінгу моделі та тестові набори даних.

Багатогранні рішення машинного навчання та розробка інтегрованої системи для перетворення великих обсягів публічних даних, які є релевантними та прогнозують кібератаки представлено в роботі [17]. Автори відзначають, що основна проблема в прогнозуванні кібератак з нетрадиційними сигналами полягає в тому, що не всі сигнали дають вірні значення через неправильні показання датчика, недоступність спостереження протягом певного періоду часу, або із-за проблем обробки даних.

Деякі сигнали призначені для виявлення попередніх кроків у циклі кібератак, що не передбачає залучення фактичної мережевої інфраструктури [19]. Автори показали, що здатність прогнозування сигналів змінюється з часом залежно від типу атаки. Крім того, визначення суттєвих відставань автоматизується для відповідних сигналів, щоб включити систему прогнозування, яка має бути адаптивною до різноманітних та змінних характеристик нетрадиційних сигналів [19].

В останні роки дослідники почали використовувати прогностичну аналітику, яка допомагає прогнозувати майбутні кібератаки. У цьому контексті використання логістичної регресії дає можливість передбачити ризик виникнення хостів від зловмисного програмного забезпечення [18].

Постановка завдання. Проаналізувати уразливості, проблеми безпеки та моделі атак у розрізі інформаційної безпеки підприємства та представити їх класифікацію. Виявити і класифікувати віруси кібератак для їх статистичного аналізу. Класифіковано віруси кібератак на веб-ураження та ураження електронної пошти. Дослідити часові ряди веб-загроз та уражень електронної пошти за певний період. Провести апроксимацію згладжуваних відповідних часових рядів аналітичними функціями.

Основна частина.

Проаналізуємо уразливості, проблеми кібербезпеки безпеки та моделі атак, які притаманні на підприємстві. Як різновид кібератак, існують таргетовані кібератаки APT (Advanced Persistent Threat – "Розвинена стійка загроза"), які відрізняються цілеспрямованістю від масових хакерських атак – коли одночасно атакується велике число цілей. Взагалі усі види кібератак можна класифікувати за чотирма групами відповідно до мережевої інфраструктури, рівня виправлень, конфігурації сервера і стандартного програмного забезпечення.

Розглянемо класифікацію моделей кібератак, яка приведена на рис.1, що складена автором на основі [1, 3].

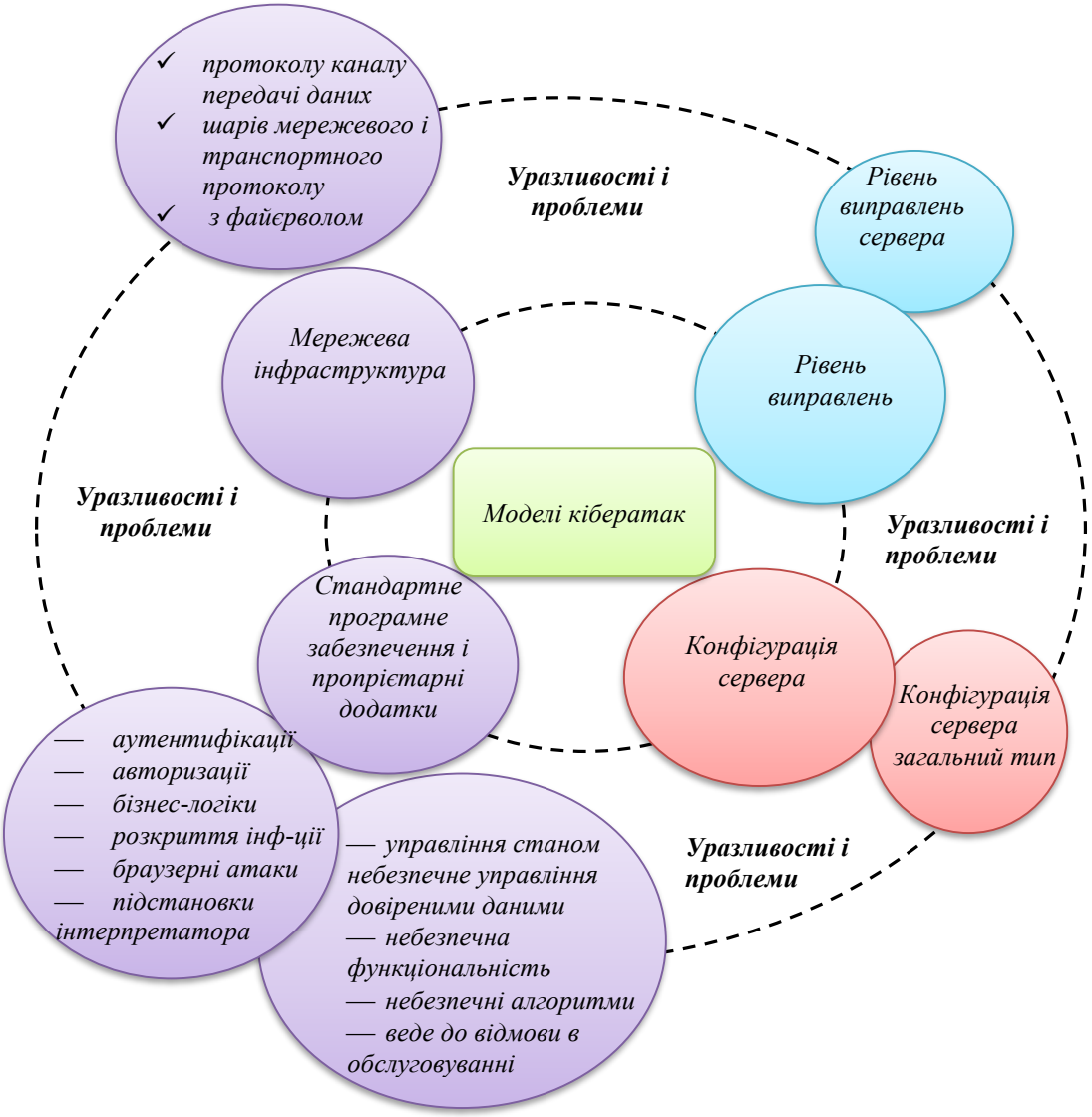

Рис.1. Схема класифікації моделей кібератак

Зауважимо, що акустичні атаки впливають на жорсткі диски і призводять до програмних і апаратних несправностей у багатьох пристроях, що оснащені HDD-накопичувачами – від комп'ютерів і систем відеоспостереження до спеціалізованих обчислювачів медичних пристроїв. Звук великої амплітуди підсилює вібрацію в блоці магнітних головок (Head Stack Assembly, HSA) жорсткого диска, що призводить до зміщення головок та порушує процес зчитування/запису. При цьому ультразвук може провокувати помилкове спрацьовування ударного датчика, що призначено для захисту HDD від пошкоджень при ударі. В результаті жорсткий диск отримує непотрібну команду на парковку головки. В ході експериментів атака тривалістю 12 секунд з використанням спеціально згенерованих акустичних перешкод привела до втрати відеоданих в системі відеоспостереження виробництва компанії Ezviz [2]. Ще одна атака, яка тривала понад 105 секунд, викликала серйозний збій в жорсткому диску Western Digital: запис даних в ньому повністю припинився, і для нормалізації роботи HDD потрібно було перезавантаження системи відеоспостереження. Такий спосіб також спрацьовував на ноутбуках і настільних ПК під управлінням ОС Windows і Linux [2].

Існують додатки такі, як наприклад, NordVPN , що надають фрілансерам можливість отримувати бази даних компанії, онлайн-інструменти та робочі рахунки та забезпечувати їх безперешкодним доступом до мереж та ресурсів компанії. Також цей додаток забезпечує безпеку онлайн-даних від кіберзагроз та підключення до незахищених відкритих точок доступу. Додаток Peregrine International формує невід'ємну частину стратегії стійкості

підприємства, спеціалізується на проактивній ідентифікації та вирішенні ризику безпеки для бізнесу в будь-якій точці світу. Peregrine International робить особливий акцент на захисті існуючих інвестицій, активів та ресурсів та нові можливості розвитку нових підприємств. Peregrine International дає інформаційну без пекову підтримку у складних ситуаціях підприємства стосовно кібербезпеки.

Уразливості, проблеми безпеки та моделі атак мережевої інфраструктури, рівня виправлень і конфігурації сервера представлено в табл. 1.

Таблиця 1

Уразливості, проблеми безпеки та моделі атак мережевої інфраструктури, рівня виправлень і конфігурації сервера

Уразливості (Проблеми безпеки)	***Моделі атак***
Мережева інфраструктура	
Уразливості протоколу каналу передачі даних (Проблеми безпеки в шарі 2 моделі OSI)	— Розмітка 802.1Q і ISL (розстановка тегів) — ARP-фальсифікація — Злом шифрування бездротового з'єднання — Виснаження адрес DHCP — Атака з подвійним інкапсулювання 802.1Q / VLAN — Переповнення MAC — Маніпуляції STP
Уразливості шарів мережевого і транспортного протоколу (Проблеми безпеки в шарі 3, 4 and 5 моделі OSI)	— Маніпуляції BGP — Маніпуляції EIGRP — Маніпуляції IGRP — Маніпуляції OSPF — Перехоплення і аналіз мережевих пакетів — маніпуляції RIP — Передбачення порядкового номера TCP/IP — Переповнення SYN
Уразливості файєрвола (Проблеми безпеки конфігурації файєрвола)	— Обхід правил брандмауера — Недостатня фільтрація пакетів
Рівень виправлень	
Уразливості рівня виправлень сервера(Затосування багів ПЗ при патчі)	Використання відомих вразливостей додатків
Конфігурація сервера	
Уразливості конфігурації сервера / загальний тип (Цей клас включає в себе помилки конфігурації, які можуть бути використані зловмисниками, по відношенню до всіх типів серверного програмного забезпечення)	— Використання врахованих записів за замовчуванням — Перерахування облікових записів користувачів — Використання небезпечних методів протоколювання — Використання невідповідних дозволів для доступу — Використання незахищених функціональних можливостей — Збір внутрішньої інформації — вгадування паролів — Зчитування незашифрованих конфіденційних даних

Джерело: складено автором на основі [2,4,6,7]

Слабкі сторони мережевих протоколів є складними, коли і системні адміністратори, і користувачі мають обмежені знання про мережеву інфраструктуру [2], [4]. Наприклад, системні адміністратори не використовують ефективну схему шифрування , не застосовують рекомендовані виправлення вчасно або не забувають застосовувати фільтри безпеки або політики. Одна з найпоширеніших мережевих атак відбувається шляхом використання обмежень: часто використовуваних мережевих протоколів Internet Protocol (IP), протоколу управління передачею (TCP) або системи доменних імен (DNS).

IP – це основний протокол мережевого рівня. Він надає інформацію, необхідну для маршрутизації пакетів між маршрутизаторами та комп'ютерами мережі. Оригінальний

протокол IP не має жодного механізму для перевірки достовірності та конфіденційності даних, що передаються. Це дозволяє перехоплювати або змінювати дані під час передачі по невідомій мережі між двома пристроями. Для запобігання проблеми IPSec був розроблений для забезпечення шифрування IP-трафіку. Протягом багатьох років IPSec використовувалась як одна з основних технологій створення віртуальної приватної мережі (VPN), яка створює захищений канал через Інтернет між віддаленим комп'ютером та надійною мережею (тобто фірмовою Інтранет). TCP знаходиться на вершині IP для передачі у надійних пакетів (тобто повторна передача втрачених пакетів).

Зауважимо, що SSL спочатку був розроблений для забезпечення цілісного захисту, на відміну від протоколу, що базується лише на шарі, між двома комп'ютерами, що знаходиться над протоколом управління передачею (TCP). SSL / TLS зазвичай використовується з http для формування https для захищених веб-сторінок. Сервер доменних імен (DNS) – це протокол, який переводить читані людиною імена хостів у 32-розрядні адреси Інтернет-протоколів (IP). Він по суті працює як книга директорій для маршрутизаторів, що повідомляють Інтернет, на яку IP-адресу направляти пакети, коли користувач надає URL-адресу. Оскільки відповіді DNS не є аутентифікованими, то існує небезпечна можливість надсилати шкідливі повідомлення DNS для представлення на Інтернет-сервері. Інша головна проблема DNS – це його доступність. Оскільки успішна атака на службу DNS призвела б до значних порушень зв'язку в Інтернеті, DNS стала об'єктом кількох атак на відмову від обслуговування (DoS). Великий об'єм потоку даних в мережах з високою ємністю вимагає нових методів аналізу для обчислення, а також візуалізації невизначеності, пов'язаної з наборами даних. Цей виклик створив нову область досліджень, де для об'єднання мережевого трафіку з кращими методами візуалізації необхідні комбіновані набори навичок від практикуючих мережу та спільноти візуалізації [3]. Потім візуальне представлення даних аналізується мережевими експертами з поглибленими знаннями домену в системі мереж.

Наприклад, програмне забезпечення RobbinHood призначене для атаки на мережеву інфраструктуру підприємства та здатне вимикати служби Windows, які запобігають шифруванню даних та відключати їх від спільних накопичувачів. Також Sodinokibi ще одна типова загроза для підприємств. Це викликає занепокоєння через вектор атаки, який використовує новішу вразливість, яка дозволяє виконувати довільне виконання коду і не потребує жодної взаємодії з користувачем, як і інші програми, що надсилаються фітинг електронною поштою. Крім того, вразливості протоколу віддаленого робочого столу (RDP), такі як BlueKeep, є попередженням про те, що послуги віддаленого доступу можуть бути можливостями для кіберзлочинців, і що вони також можуть бути використані як вектор атаки для поширення програмного забезпечення. На рис. 2 представлено часові ряди Індексу поширення загрози Fortinet: ботнети, експлуатації, зловмисне програмне забезпечення за період з липня 2018 року по липень 2019 року та їх апроксимації поліномами.

Наголосимо, що підзвітність – це ще один аспект контролю доступу, який включає дослідження, яке забезпечує будь-кого або все, що має доступ до системного компонента, такого як обчислювальний пристрій, додаток, мережа, можуть нести відповідальність за результати такого доступу.

Відмітимо, що кібератаки використовують програмні помилки, щоб змусити системи вести себе ненавмисними способами, відмінними від їх первісних намірів. Більшість кібератак сьогодні все ще трапляються внаслідок використання вразливості програмного забезпечення, спричиненої помилками програмного забезпечення та недоліками дизайну [4]. Експлуатація на основі програмного забезпечення відбувається при використанні певних функцій стека програмного забезпечення та інтерфейсу.

Найбільш поширені вразливості програмного забезпечення трапляються внаслідок використання програмних помилок у пам'яті, перевірки введення користувачем, умов перегонів та привілеїв доступу користувачів.

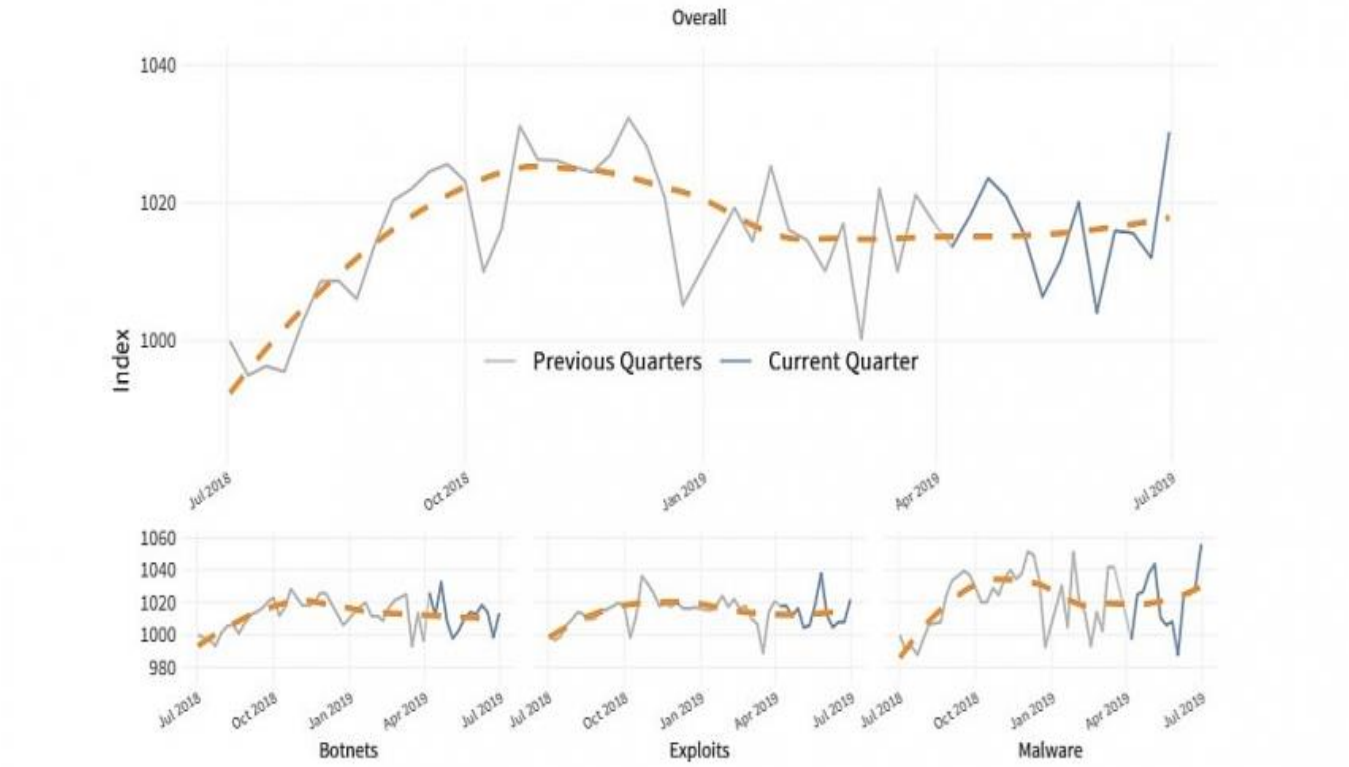

Рис.2. Індекс поширення загрози Fortinet: ботнети, експлуатації, зловмисне програмне забезпечення

Джерело: Fortinet threat landscape index hits historic record. URL:

https://www.vir.com.vn/fortinet-threat-landscape-index-hits-historic-record-70363.html

Найбільш зразковою технікою є переповнення буфера. Переповнення буфера виникає, коли програма намагається зберігати більше даних у буфері, ніж було призначено для утримання. Оскільки буфери створені, щоб містити кінцевий обсяг даних, додаткова інформація може переливатися в сусідні буфери, пошкоджуючи або перезаписуючи дійсні дані, що містяться в них. Це дозволяє втручатися в існуючий код процесу. Перевірка вводу – це процес забезпечення того, щоб вхідні дані відповідали певним правилам. Неправильна перевірка даних може призвести до пошкодження даних, таких як інжекція SQL. Інжекція SQL – одна з найвідоміших методик, яка використовує програмну помилку в програмному забезпеченні веб-сайту.

Уразливості, проблеми безпеки та моделі атак на стандартне програмне забезпечення і пропрієтарні додатки представлено в табл.2.

Зауважимо, що необхідне надання нових ідей для створення безпечного обчислювального середовища. У практиці безпечного кодування на основі огляду коду інженери програмного забезпечення виявляють поширені помилки програмування, що призводять до вразливості програмного забезпечення, встановлюють стандартні стандарти безпечного кодування, навчають розробників програмного забезпечення та покращують стан практики безпечного кодування. У мовній практиці безпечного кодування розроблені методи, що дозволяють покладатися на програми, щоб не порушувати важливі політики безпеки. Найбільш широко використовувані методи включають аналіз та трансформацію.

Таблиця 2

Моделі атак стандартного програмного забезпечення і пропрієтарних додатків

Уразливості (Проблеми безпеки)	***Моделі атак***
Аутентифікації (Веб-додаток не має достатніх коштів аутентифікації для захисту своїх ресурсів)	Обхід аутентифікації
Авторизації (Неавторизований користувач може отримати доступ до ресурсів, які захищені)	Доступ до захищених функцій Доступ до захищених ресурсів
Бізнес-логіки (Зловмисник може порушити бізнес-правила додатки)	В залежності від програми
Розкриття інформації (Зловмисник може збирати інформацію про внутрішні даних додатка або серверному оточенні)	Збір інформації з коментарів до коду Збір інформації з системних повідомлень,помилок Читання старих файлів, файлів архівних копій і файлів без зовнішніх посилань
Сприяння атакам з боку клієнта -браузерні атаки (Цей клас вразливостей відноситься до Інтернету. Входять атаки, націлені на веб-браузер)	Фальсифікація крос-сайтовий запитів (XSRF) Підстановка HTML / крос-сайтовий сценарій (XSS) Розщеплення відповіді HTTP / (підстановка заголовків, імітація фреймів, фіксація сесії)
Підстановки інтерпретатора / перевірки введених даних (Додаток передає введені параметри в базу даних, в API операційної системи або в інші інтерпретатори без належної перевірки даних)	Доступ до файлової системи (підстановка коду, підстановка команд) Підстановка рядки форматування Підстановка IMAP / SMTP (LDAP, ORM) Переповнення буфера символів(обхід шляху) Підстановка операторів SQL,SSI,XML,Xpath
Управління станом / сесією (Змінні стану ініціалізуються і застосовуються невірно)	Перерахування ідентифікаторів сесії Використання проблем стану сесії
Небезпечне управління довіреними даними (Зловмисник може маніпулювати довіреними даними і внутрішніми даними додатка)	Маніпулювання внутрішніми даними додатка про клієнта - конфіденційних даних про клієнта Читання внутрішніх даних програми Додаток має небезпечну функціональність Використання додатків-зразків Завантаження довільних файлів
Небезпечні алгоритми(Використання небезпечних алгоритмів дозволяє скомпрометувати вразливі дані)	Злом шифрування Використання слабкого генератора випадкових чисел та слабких алгоритмів шифрування
Уразливість, яка веде до відмови в обслуговуванні (Служба може бути виведена зловмисником з ладу)	Використання необмеженого розподілу ресурсів Блокування облікових записів замовників

Джерело: складено автором на основі [1,5,6]

Традиційні системи контролю доступу надають основні послуги, такі як аутентифікація, авторизація та підзвітність. Аутентифікація та авторизація – це процес підтвердження того, що суб'єкт пов'язаний з об'єктом. Традиційні механізми аутентифікації та авторизації використовують три різні чинники для ідентифікації суб'єкта для перевірки наявності суб'єктом права доступу до об'єкта. Перший фактор – це те, що ви знаєте, наприклад, пароль або особистий ідентифікаційний номер (PIN-код). Це передбачає, що лише власник облікового запису, який знає пароль або PIN, необхідний для доступу до облікового запису. Другий фактор – це те, що включає смарт-карту або маркер безпеки. Це передбачає, що лише власник облікового запису має необхідну смарт-карту або маркер, необхідний для розблокування облікового запису. Третій фактор – це те, що ти є, наприклад, відбитки пальців, голос чи райдужка. Сучасна тенденція аутентифікації – це багатошаровий підхід, який часто називають сильною аутентифікацією , відповідаючи на презентацію двох або більше факторів аутентифікації [4].

Проаналізуємо статистичні дані кібератак у полі діяльності ІТ-підприємства, що залучає

фріланс-ресурс, для того, щоб використувувати часові кореляції між кількістю кібератак за часовий період для передбачення майбутніх інтенсивності кібер-інцидентів для створення системи прогнозування. Передбачення кількості кібератак за встановлений раціональний часовий період необхідне для визначення ефективної частоти аудиту. Запропонований підхід може використовувати лише підмножину даних, що стосуються конкретного методу атаки. Такі моделі прогнозування повинні динамічно оновлюватися з часом, коли відслідковуються нові дані для підвищення точності прогнозу і, відповідно, ефективності аудиту.

Окремо дослідимо веб-загрози та ураження електронної пошти. Стосовно веб-загроз можна констатувати той факт, що чим більше веб-сторінок відвідує користувач, тим більше шансів йому зіткнутися з атакою. Наприклад, користувач може відвідувати шкідливу веб-сторінку, яка запускає веб-атаку. Як варіант, користувач може подивіться рекламу підробленої програми та завантажити підроблену програму. Нарешті, користувач може завантажити шкідливе відео чи PDF-файл. Варто зазначити, що не всі атаки вимагають від користувачів відвідування веб-сторінок. Наприклад, багато уражень можуть охопити будь-який прилад, підключений до Інтернету. Користувач, що не підозрює, вводить приватну інформацію на шкідливий веб-сайт, який згодом використовується зловмисниками. Зауважимо, що більшість методів фішингу використовують певну форму технічного обману, створену для створення посилань на електронній пошті (та підробленому веб-сайті), неправильно написані URL-адреси або використання під доменів.

На рис. 3 представлено часовий ряд веб-загроз (кібератак) за період 1.01-30.11.2019 року. Пунктирна лінія – фільтрація за трьома точками часового ряду, після чого була проведена апроксимація з коефіцієнтом детермінації $R^2 = 0,8552$, аналітична функція якої має вигляд:

$$y = 10^{-7} x^5 - 2 \cdot 10^{-5} x^4 + 0,0012x^3 - 0,017x^2 - 0,5441x + 19,738. \quad (1)$$

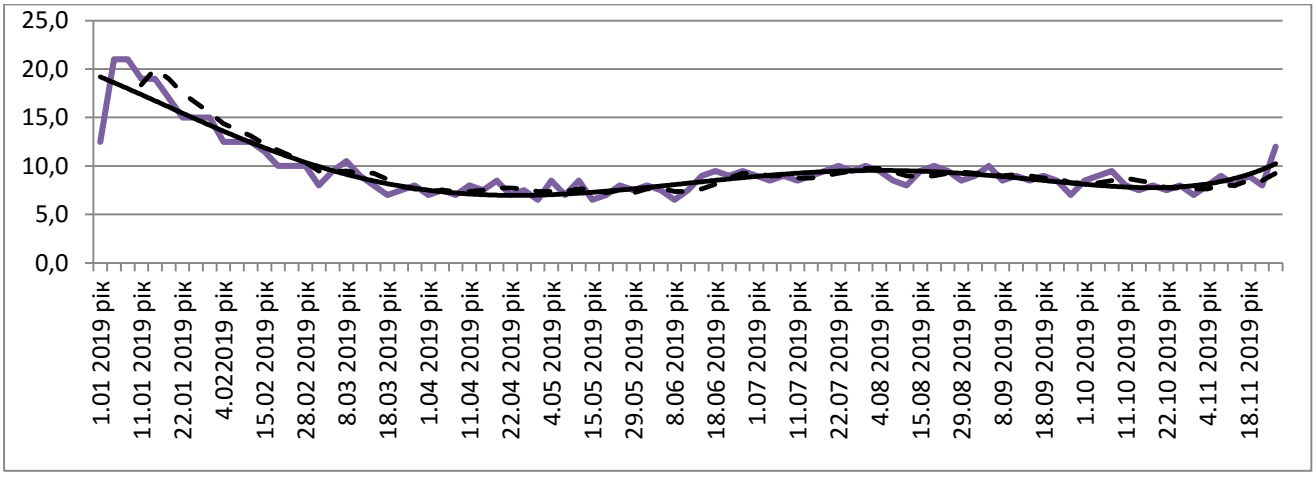

Рис.3. Часовий ряд веб-загроз (кібератак) за період 1.01-30.11.2019 року

У табл. 4 представлено кібератаки на веб-ураження та їх частка у загальній кількості кібератак за період з січня по листопад 2019 року для підприємства, що працює із залученням фріланс-ресурсу. За матеріалами доповіді FireEye Q1 2019 “Email Threat” зазначимо, що за третій квартал 2019 року на 26% зросло кількість кібератак, використовуючи протокол HTTPS, коли уражені URL-адреси можуть здаватися працездатними, причому спостерігається збільшення фішингових атак на 17%. Мають місце вкладені листи зі шкідливим змістом. Такий висновок було зроблено після аналізу 1,3 млрд. листів. Також у вищезазначеній доповіді підкреслюється про збільшення використання файлообмінних сервісів Google Drive і Dropbox в кібератаках, що дає можливість створення уражених платформ за умови фітингу [9].

Таблиця 4

Розподіл кібератак (веб-загрози) та їх частки у загальній кількості кібератак за 3 часових періодів 2019 року

Позначення	***Ураження***	***значення (%)***
V1	Trojan.Script.Generic	18,034
V2	Trojan.Multi.Preqw.gen	17,432
V3	Backdoor.HTTP.TeviRat.gen	15,934
V4	Trojan.Script.Miner.gen	11,466
V5	Trojan-Clicker.HTML.Iframe.dg	9,452
V6	Trojan.BAT.Miner.gen	7,834
V7	Trojan-Downloader.JS.Inor.a	6,764
V8	Trojan.Script.Redirector.gen	5,889
V9	Trojan-PSW.Win32.Predator.nt	4,623
V10	DangerousObject.Multi.Generic	2,572
Усього		100

Джерело: складено автором на основі даних підприємства

На рис. 4 представлено часовий ряд уражень електронної пошти (кібератак) за період 1.01-30.11.2019 року.

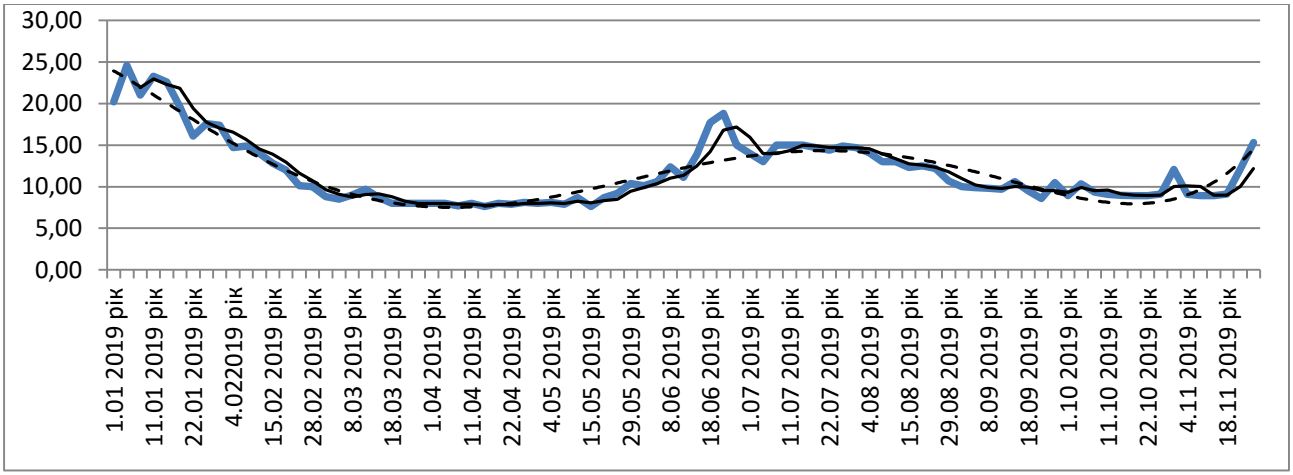

Рис.4. Часовий ряд кібератак на електронну пошту за період 1.01-30.11.2019 року

Пунктирна лінія – фільтрація за трьома точками часового ряду, після чого була проведена апроксимація з коефіцієнтом детермінації $R^2 = 0,8715$, аналітична функція якої має вигляд

$$y = 2 \cdot 10^{-7} x^5 - 4 \cdot 10^{-5} x^4 + 0,0023x^3 - 0,0287x^2 - 0,8622x + 24,819. \quad (2)$$

У табл. 5 представлено кібератаки на ураження електронної пошти та їх частка у загальній кількості кібератак на підприємстві за період з січня по листопад 2019 року.

Зауважимо, що для запозичення доступу до корпоративної мережі існує небезпека у підроблених листах, які начеб-то написані директорами фірм. Такі загрози можуть нанести ураження фінансовому та бухгалтерському відділам, причому може змінитися інформація про банківські реквізити та інш. [8, 9].

Таблиця 5

Кібератаки (ураження електронної пошти) та їх частки у загальній кількості кібератак за 3 часових періоди 2019 року

Позначення	***Ураження***	***Значення (%)***
W1	DangerousObject.Multi.Generic	16,836

W2	Trojan.PDF.Badur.gen	15,958
W3	Exploit.MSOffice.CVE-2017-11882.gen	14,01
W4	Trojan.PDF.Phish.gen	13,841
W5	Trojan.Script.Generic	12,689
W6	Trojan-Downloader.PDF.Agent.fx	11,432
W7	Worm.Win32.WBVB.vam	7,493
W8	Trojan.PDF.Fraud.gen	6,389
W9	Trojan.MSOffice.SAgent.gen	1,232
W10	VHO:Trojan.MSOffice.SAgent.gen	0,12
Усього		100

Джерело: складено автором на основі даних підприємства

На рис. 5 представлено часовий ряд сумісних кібератак: веб-загроз та уражень електронної пошти за період 1.01-30.11.2019 року та його апроксимація поліномом 4-го порядку з прийнятним коефіцієнтом детермінації) 0,8244:

$$y = 8 \cdot 10^{-6} x^4 - 0,0018x^3 + 0,1281x^2 - 3,6425x + 51,641. \quad (3)$$

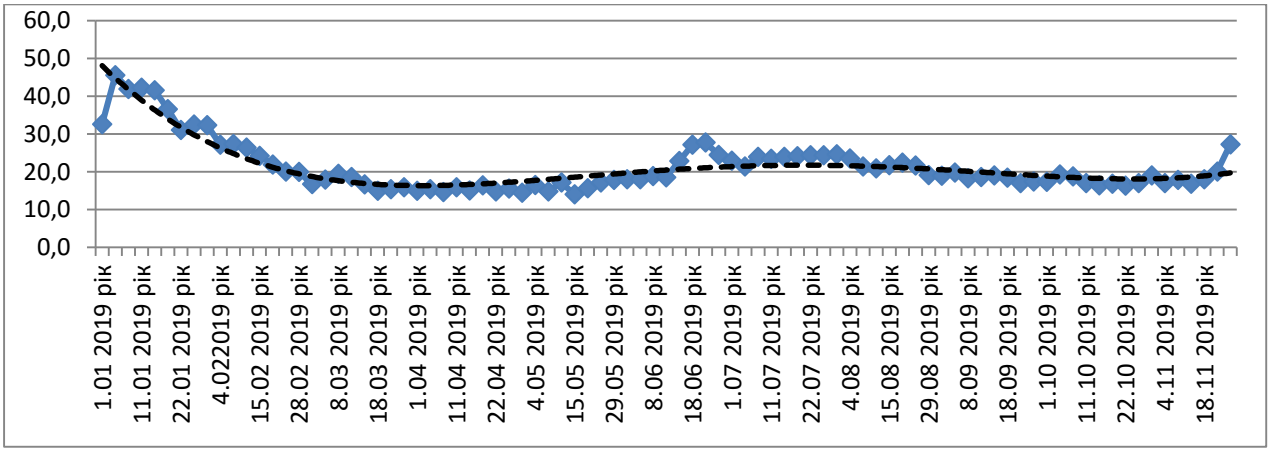

Рис.5. Часовий ряд сумісних кібератак: веб-загроз та уражень електронної пошти за період 1.01-30.11.2019 року

Отже, досліджено часові ряди веб-загроз (кібератак) та уражень електронної пошти за певний період та їх згладжування за допомогою фільтрації за трьома точками часового ряду. Була проведена апроксимація відповідних часових рядів аналітичними функціями.

Висновки.

Проаналізовано уразливості, проблеми безпеки та моделі атак мережевої інфраструктури, рівня виправлень, конфігурації сервера, стандартного програмного забезпечення і пропрієтарних додатків відповідно до класифікації TAdviser та Sec-Consult. Виявлено і класифіковано віруси кібератак на веб-ураження та ураження електронної пошти та знайдена їх частка у загальній кількості кібератак. Дослідження дає можливість агрегування моделей атак для збору статистичної інформації для подальшої її обробки ймовірнісно-статистичними методами.

Список використаної літератури

1. Барабаш О.В. Построение функционально устойчивых распределенных информационных систем: монография. К.: НАОУ, 2004. 224 с.

2. A.P. Moore, R.J. Ellison, R.C. Linger. Attack Modeling for Information Security and Survivability. Technical Note CMU/SEI-2001-TN-001. Survivable Systems, 2001.

3. K. Ingols, M. Chu, R. Lippmann, S. Webster, S. Boyer. “Modeling modern network attacks and countermeasures using attack graphs.” In Proc of Annual Computer Security Applications Conference (ACSAC ’09), Washington, D.C., USA, IEEE Computer Society, 2009, pp. 117-126

4. L. Wang, T. Islam, T. Long, A. Singhal, S. Jajodia. “An attack graph-based probabilistic security metric.” In Proc. of the 22nd annual IFIP WG 11.3 working conference on Data and Applications Security. Springer-Verlag Berlin, pp. 283-296, 2008.

5. N. Kheir, N. Cuppens-Boulahia, F. Cuppens, H. Debar. “A service dependency model for cost-sensitive intrusion response.” In Proc. of ESORICS 2010, Athens, Greece, 2010, pp. 626-642.

6. Samtani, Sagar, Ryan Chinn, and Hsinchun Chen. "Exploring hacker assets in underground forums." IEEE (ISI), 2015.

7. Thonnard, Olivier, et al. "Are you at risk? Profiling organizations and individuals subject to targeted attacks." International Conference on Financial Cryptography and Data Security. Springer 2015.

8. Xu, Tingyang, Jiangwen Sun, and Jinbo Bi. "Longitudinal lasso: Jointly learning features and temporal contingency for outcome prediction." ACM, KDD 2015.

9. Соціальна інженерія та "безпечні" протоколи: нові тренди в кібератаках. URL: https://cybercalm.org/novyny/sotsialna-inzheneriya-ta-bezpechni-protokoly-novi-trendy-v-kiberatakah/

10. Langer, T.; Pohls, H.C.; Ghernaouti, S. Selected Cloud Security Patterns to Improve End User Security and Privacy in Public Clouds. Privacy Technologies and Policy. APF 2016. Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2016; Volume 9857.

11. Spasic, B.; Rath, A.; Thiran, P.; Boucart, N. Security Pattern for Cloud SaaS: from system and data security to privacy. In Proceedings of the 4th IEEE International Conference on Cloud Computing Technologies and Applications, Brussels, Belgium, 26–28 November 2018.

12. Subramaniam, T.K.; Deepa, B. Security attack issues and mitigation techniques in Cloud computing environments. Int. J. UbiComp (IJU) 2016, 7, doi:10.5121/iju.2016.7101.

13. Taherizadeh, S.; Stankovski, V.; Grobelnik, M. A Capillary Computing Architecture for Dynamic Internet of Things: Orchestration of Microservices from Edge Devices to Fog and Cloud Providers. Sensors 2018, 18, 2938.

14. Ondiege, B.; Clarke, M.; Mapp, G. Exploring a new security framework for remote patient monitoring devices. Computers 2017, 6, 11.

15. Achbarou, O.; Kiram, M.A.E.; Bouanani, S.E. Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems. Int. J. Interact. Multimed. Artif. Intell. 2017, 4, 61–64.

16. Sapienza, Anna, et al. "Early warnings of cyber threats in online discussions." Data Mining Workshops (ICDMW), 2017.

17. Okutan et al. Cybersecurity (2018) 1:15 https://doi.org/s42400-018-0016-5

18. Sapienza A, Bessi A, Damodaran S, Shakarian P, Lerman K, Ferrara E (2017) Early warnings of cyber threats in online discussions. In: Proceedings of the 2017 IEEE International Conference on Data Mining Workshops (ICDMW). Pp. 667–674.

19. Maimon D, Fukuda A, Hinton S, Babko-Malaya O, Cathey R (2017) On the relevance of social media platforms in predicting the volume and patterns of web defacement attacks. In: Proceedings of the 2017 IEEE International Conference on Big Data (Big Data). pp 4668–4673.

References

1. Barabash O.V. (2004) “Construction of functional sources of information systems distribution: monograph.”, NAOU: 224. Print

2. Moore A.P., Ellison R.J., Linger R.C. (2001) “Attack Modeling for Information Security and Survivability.” *Technical Note CMU/SEI-2001-TN-001. Survivable Systems.*

3. Ingols K., Chu M., Lippmann R., Webster S., Boyer S. (2009) “Modeling modern network attacks and countermeasures using attack graphs.” *In Proc of Annual Computer Security Applications Conference (ACSAC ’09), Washington, D.C., USA, IEEE Computer Society*: 117-126. Print

4. Wang L., Islam T., Long T., Singhal A., Jajodia S. (2008) “An attack graph-based probabilistic security metric.” *In Proc. of the 22nd annual IFIP WG 11.3 working conference on Data and Applications Security. Springer-Verlag Berlin*: 283-290. Print

5. Kheir N., Cuppens-Boulahia N., Cuppens F., Debar H. (2010) “A service dependency model for cost-sensitive intrusion response*.” In Proc. of ESORICS 2010, Athens, Greece* : 626-642. Print

6. Samtani Sagar, Ryan Chinn, and Hsinchun Chen. (2015) “Exploring hacker assets in underground forums.”, IEEE (ISI). Print

7. Thonnard Olivier, et al. (2015) “Are you at risk? Profiling organizations and individuals subject to targeted attacks.” *International Conference on Financial Cryptography and Data Security. Springer* .

8. Xu Tingyang, Jiangwen Sun, and Jinbo Bi. (2015) “Longitudinal lasso: Jointly learning features and temporal contingency for outcome prediction.” ACM, KDD.

9. *Social engineering and "secure" protocols: new trends in cyberattacks.* *https://cybercalm.org/novyny/sotsialna-inzheneriya-ta-bezpechni-protokoly-novi-trendy-v-kiberatakah/*

10. Langer T., Pohls H.C., Ghernaouti S. (2016) “Selected Cloud Security Patterns to Improve End User Security and Privacy in Public Clouds. Privacy Technologies and Policy.” APF. *Lecture Notes in Computer Science; Springer: Cham, Switzerland*, Volume 9857. Print

11. Spasic B., Rath A., Thiran P., Boucart N. (2018) “Security Pattern for Cloud SaaS: from system and data security to privacy.” *In Proceedings of the 4th IEEE International Conference on Cloud Computing Technologies and Applications, Brussels, Belgium, 26–28 November 2018.*

12. Subramaniam T.K., Deepa B. (2016) “Security attack issues and mitigation techniques in Cloud computing environments” *Int. J. UbiComp (IJU)*, 7, doi:10.5121/iju.2016.7101.

13. Taherizadeh S., Stankovski V., Grobelnik M. (2018) “A Capillary Computing Architecture for Dynamic Internet of Things: Orchestration of Microservices from Edge Devices to Fog and Cloud Providers. Sensors”, 18: 2938. Print

14. Ondiege B., Clarke M., Mapp G. (2017) “Exploring a new security framework for remote patient monitoring devices” *Computers*, 6: 11. Print

15. Achbarou O., Kiram M.A.E., Bouanani S.E. (2017) “Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems.” *Int. J. Interact. Multimed. Artif. Intell.*, 4: 61–64. Print

16. Sapienza Anna, et al. (2017) "Early warnings of cyber threats in online discussions." *Data Mining Workshops (ICDMW)*.

17. Okutan et al. Cybersecurity (2018) 1:15 https://doi.org/s42400-018-0016-5

18. Sapienza A., Bessi A., Damodaran S., Shakarian P., Lerman K., Ferrara E. (2017) “Early warnings of cyber threats in online discussions.” *In: Proceedings of the 2017 IEEE International Conference on Data Mining Workshops (ICDMW)*: 667–674. Print

19. Maimon D., Fukuda A., Hinton S., Babko-Malaya O., Cathey R. (2017) “On the relevance of social media platforms in predicting the volume and patterns of web defacement attacks.” *In: Proceedings of the 2017 IEEE International Conference on Big Data (Big Data)*: 4668–4673. Print

Автори статті (Authors of the article)

Галахов Євген Миколайович – ст. викладач кафедри вищої математики (Halakhov Yevhen – Assistant of the Department of Mathematics, State University of Telecommunications). Phone: +380 63 592 4517. E-mail: evgen.galakhov@gmail.com.

Собчук Валентин Володимирович – к. ф.-м. наук, доцент, доцент кафедри вищої математики, Державний університет телекомунікацій (Sobchuk Valentyn – candidate of sciences (physics and mathematics), Associate Professor, Associate Professor of the Department of Mathematics, State University of Telecommunications). Phone: +380 50 339 8113. E-mail: v.sobchuk@ugmk.kiev.ua