УДК 004.056:004.491
DOI https://doi.org/10.32838/2663-5941/2021.4/24

Стаценко Д.В.
Київський національний університет технологій та дизайну

Осипенко В.В.
Київський національний університет технологій та дизайну

Злотенко Б.М.
Київський національний університет технологій та дизайну

Кулік Т.І.
Київський національний університет технологій та дизайну

Стаценко В.В.
Київський національний університет технологій та дизайну

СУЧАСНІ ТЕНДЕНЦІЇ КІБЕРЗАГРОЗ У КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

У статті розглянуті тенденції кіберзагроз за 2020 рік та першу половину 2021 року. Наведено приклади змін ландшафту кіберзагроз та їх вплив на комп'ютерні системи і мережі організацій у зв'язку із глобальними подіями 2020 року. Наголошено, що щороку з метою зниження негативних наслідків від кіберзагроз інвестиції у сферу інформаційної безпеки зростають. Проте загальна кількість кіберзагроз не зменшується, а, навпаки, збільшується.

В аналізі останніх публікацій та досліджень наведена інформація про три масштабні кібератаки на міжнародні організації. Зауважено, що за останні три місяці від кібервимагачів постраждали Colonial Pipeline, JBS S.A., Kaseya. Загальна сума збитків може сягати понад 100 млн доларів США.

Розглянуті та проаналізовані різні категорії шкідливого програмного забезпечення, яке використовувалося зловмисниками протягом останніх декількох років. Проведено аналіз витоку даних, викрадених особистих записів та зміни тенденцій у цій категорії кіберзагроз на фоні переходу організацій на дистанційний режим роботи у 2020 році. Наведено статистику розроблених нових версій програм-вимагачів за першу половину 2021 року та 2020 рік. Наголошено, що цей тип шкідливого програмного забезпечення несе велику загрозу комп'ютерним системам та мережам як організацій, так і окремих користувачів. Наведені правила стратегії оборони інформаційних систем організацій, що використовуються для зниження ризиків ураження комп'ютерних систем та мереж. Наведені дані про нові версії шкідливого програмного забезпечення в категоріях Office, Power Shell, Java Script, Coin Miner, Mobile, Malicious Signed Binaries, Mac OS, Exploit Linux, Io Tmai OS. Наведено дані, що більшість успішних кібератак відбулися в результаті людської помилки.

У висновку наведено рекомендації щодо необхідності постійного покращення категорій кібербезпеки.

Ключові слова: *кібербезпека, комп'ютерна система, комп'ютерна мережа, Інтернет, шкідливе програмне забезпечення, витік даних, програма-вимагач.*

Постановка проблеми. Питання, пов'язані з кібербезпекою, з кожним роком стають усе більш розповсюдженими та важливими. Розвиток інформаційних технологій приводить до їх упровадження у важливі сфери людської життєдіяльності. Зростає кількість кіберзагроз, а їх ландшафт постійно змінюється. Наприклад, протягом останнього року відбувся масовий перехід на дистанційну роботу, що призвело до зростання атак на засоби віддаленого доступу, що стали ландшафтом кіберзагроз для організацій, які попередньо з цим не стикалися [1, с. 4–7]. В загальному вигляді до ландшафту кіберзагроз входять уразливості, різноманітне шкідливе програмне забезпечення, різні групи зловмисників та їх методи, що несуть загрозу залежно від конкретної ситуації. На зміну ландшафту загроз можуть впливати такі фактори, як: 1) поява нових або розкриття наявних уразливостей, що у свою чергу дає змогу зловмисникам використовувати нові можливості для

атаки; 2) розроблення нових апаратних платформ, підходів до обробки даних; 3) глобальні події, що призводять до зміни інфраструктури організацій [2, с. 17–30].

Протягом останніх років інвестиції у сферу забезпечення кібербезпеки постійно зростають, і ця тенденція не змінюється. Уразливості кібербезпеки організацій можуть призводити до негативних наслідків, економічних та репутаційних втрат. Проте станом на сьогодні недостатньо інвестувати лише у захист, необхідно також покращувати загальну стратегію безпеки. У загальному вигляді організації мають упроваджувати узагальнену концепцію взаємозв'язку трьох основних етапів стратегії кібербезпеки, таких як визначення, захист та реагування на кіберзагрози.

Аналіз останніх досліджень і публікацій. З кожним роком зростає кількість фахівців та науковців багатьох країн світу, що займаються питаннями, пов'язаними з кібербезпекою [3–5]. Незважаючи на це, кількість кіберзагроз не знижується. Відповідно до офіційних даних світових компаній, пов'язаних із кіберзахистом (Risk Based Security, McAfee Labs, Cybersecurity Education & Training Solutions, Mitre тощо [6–9]), протягом першої половини 2021 року було зафіксовано 2967 випадків витоку даних, до зловмисників потрапило 18,751 млрд особистих записів юридичних та фізичних осіб, серед яких: соціальна мережа Facebook (533 млн записів), один із великих постачальників рецептурних препаратів у США CVSHealth (1,16 млрд записів), міжнародна брокерська компанія FBS Markets Inc. (16 млрд записів). Порівняно з першою половиною 2020 року відбувся спад кількості випадків витоку даних, а саме було зафіксовано 3233 випадки витоку даних, а до кіберзлочинців потрапило 36,132 млрд особистих записів.

Водночас діє інший напрям кіберзлочинів, пов'язаний із вимаганням. Так, 7 травня 2021 року відбулася масштабна атака хакерської групи [10], в результаті чого робота трубопровідної системи Colonial Pipeline була зупинена на 5 днів, за деякими даними, перед зупинкою також було викрадено інформацію обягом 100 Гб [11]. Система була уражена шкідливим програмним забезпеченням (ПЗ): найбільш імовірно, вірус потрапив до мережі за допомогою фішингового листа, який прийшов до адміністративної частини бізнес-сегменту мережі [12], а потім почав заражати критично важливі елементи системи. У результаті цього компанія Colonial Pipeline офіційно підтвердила, що була вимушена заплатити вимагачам 4,5 млн доларів США.

Також за останні три місяці були проведені ще 2 масштабні кібератаки [13]. Перша, на бразильську м'ясопереробну компанію JBSS.A., відбулася 30 травня 2021 року, в результаті чого протягом декількох днів підприємство було вимушене зупинити виробництво у країнах, які входили до мережі компанії, а саме у США, Канаді та Австралії. JBSS.A. була вимушена заплатити 11 млн доларів США викупу. Друга подібна негативна подія мала місце з американською компанією Kaseya, яка працює у сфері постачання корпоративного ПЗ, у результаті чого постраждали також і користувачі цієї організації, які знаходяться в США та європейських країнах. Сума, яку вимагають зловмисники, сягає 70 млн доларів США у біткоїнах. Імовірно, за двома останніми атаками стоїть одна хакерська група [13], за попередніми даними, кіберзлочинці використовували вразливості нульового дня, подібні до тих, що використовувалися під час масового зараження комп'ютерним вірусом WannaCry [14]. Аналогічно до цього робота операційної системи блокується, а всі файли, що знаходяться на уражених технічних засобах, шифруються.

Вищенаведений огляд лише підкреслює актуальність та необхідність аналізу та проведення постійних досліджень у сфері кібербезпеки.

Постановка завдання. Метою роботи є аналіз сучасних напрямів розвитку кіберзагроз, які призводять до негативних наслідків у комп'ютерних системах та мережах організацій і приватних осіб, і надання рекомендацій щодо побудови ефективної стратегії безпеки, яку можна коригувати до зміни ландшафту кіберзагроз.

Виклад основного матеріалу. На рис. 1 та рис. 2 наведені дані за перші 6 місяців останніх 7 років про кількість випадків витоку даних та викрадення записів [6, 7].

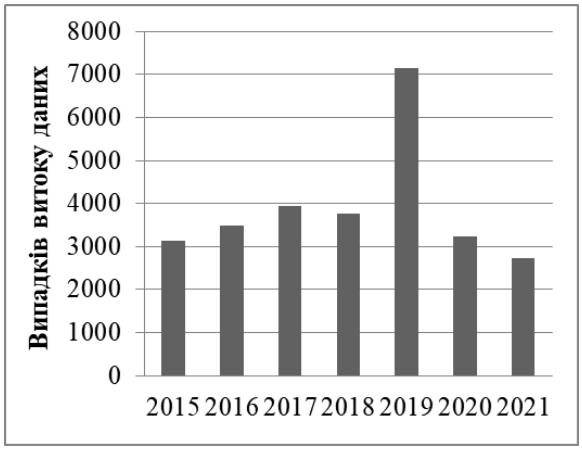

Рис. 1. Кількість випадків витоку даних

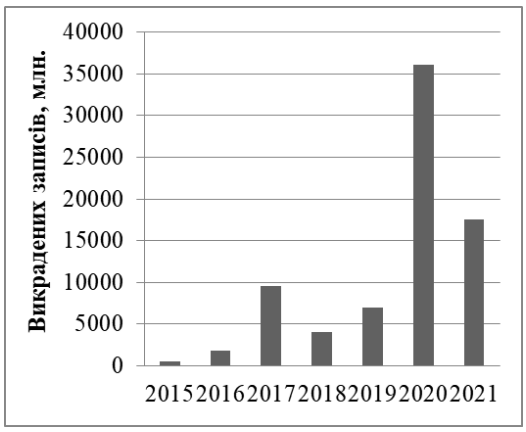

Рис. 2. Кількість випадків викрадення записів

Подібне зменшення кількості випадків витоку даних у першій половині 2021 року порівняно з аналогічним періодом 2020 року може бути пов'язано з адаптацією стратегій кібербезпеки до масового переходу працівників різних організацій на дистанційну роботу у зв'язку з пандемією COVID-19.

Спираючись на результати даних, наведених на рисунках 1 та 2, наданих компанією Risk Based Security, можна зробити висновок, що кількість випадків витоку даних більшою частиною не змінювалося, проте кількість викрадених записів за останні роки зросла.

Варто зазначити, що зібрані дані не є остаточними, до них не входять випадки витоку даних, які не були визначені службами безпеки організацій, або випадки, коли фізичні чи юридичні особи не надавали звітність стосовно компрометації своїх систем.

Крім того, більша частина випадків викрадення записів припадає на декілька великих організацій, які працюють та зберігають мільйони записів. Як уже зазначалося, протягом перших 6 місяців 2021 року відбулося два масштабних витоки даних, що включають у себе більшість викрадених даних, а саме 17693 млн записів, які належать компаніям FBS Markets Inc., CVSHealth та Facebook.

На рис. 3 наведена офіційна статистика визначених унікальних програм-вимагачів, які використовуються для зараження програмного забезпечення, електронних даних та іншої інформації з метою вимагання грошей, за 2020 рік та за перший квартал 2021 року.

Аналіз відомих випадків зараження ПЗ вірусами програм-вимагачів показав, що найбільшу загрозу вони несуть для великих організацій та підприємств. Під час зараження таких компаній відбувається блокування великої кількості робочих місць, автоматичних технічних засобів виробництва, які входять до локальної мережі. Одночасно паралізується робота більшості комп'ютерних систем, у результаті чого компанія несе фінансові та репутаційні втрати і вимушена або платити зловмисникам, або чекати на розблокування програмного забезпечення та дешифрування, відновлення даних службами інформаційної безпеки.

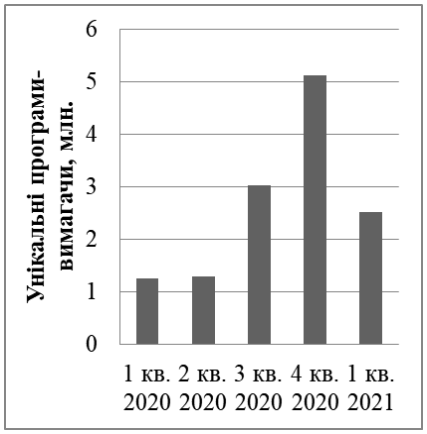

Рис. 3. Кількість унікальних програм-вимагачів за 2020 рік і початок 2021 року

Окрім програм-вимагачів, кількість шкідливого програмного забезпечення з кожним роком збільшується. На діаграмі (рис. 4) показана кількість нових версій комп'ютерних вірусів, створених протягом 2018, 2019, 2020 років та першого кварталу 2021 року, а також загальна кількість наявного шкідливого ПЗ.

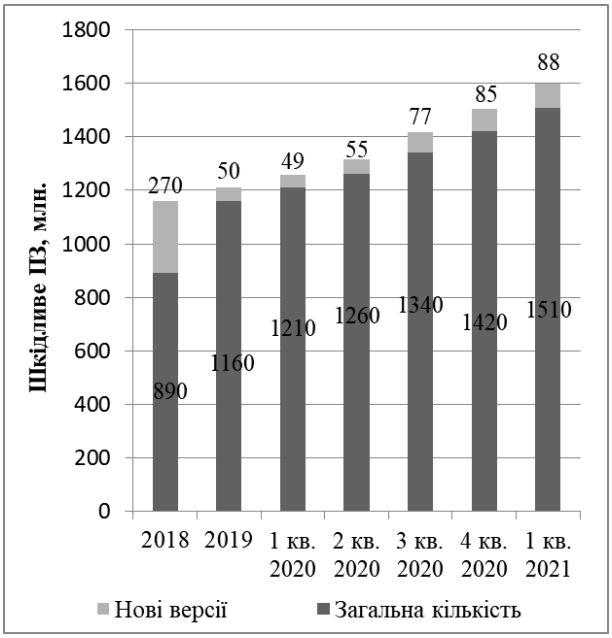

Рис. 4. Загальна кількість шкідливого ПЗ \і нових за 2020 рік та 1 кв. 2021 року

Протягом 2020 року кількість шкідливого програмного забезпечення збільшилося більше

ніж на 200 млн. Аналізуючи результати даних за останні три роки і донині, бачимо, що відбулося збільшення загальної кількості таких об'єктів майже в два рази.

Розглянемо конкретніше шкідливе ПЗ, яке було розроблено протягом 2019 та 2020 років за типами, наведеними на рис. 5.

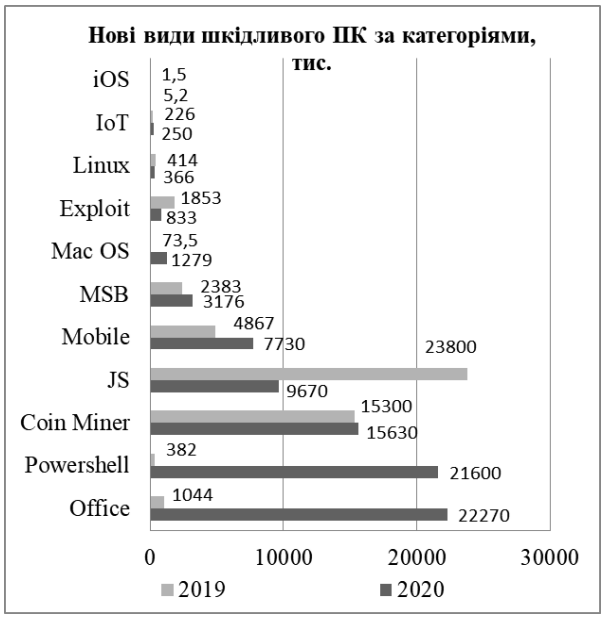

Рис. 5. Кількість нових версій комп'ютерних вірусів за 2019–2020 рр.

Найбільша кількість нових версій вірусів була створена в категоріях Office (шкідливе ПЗ, яке вбудовується в програмні додатки, наприклад Microsoft Office) та Power Shell (віруси, які вносять зміни до командної оболонки). Порівняно з минулим роком їх кількість зросла у 21 раз та у 56 разів відповідно.

Найбільше зменшення серед нових версій, у 2,5 раза, відбулося в категорії JS (віруси, які діють, використовуючи Java Script, розташовані на веб-сайтах та завантажуються до операційної системи за допомогою браузерів).

Шкідливе ПЗ, пов'язане з майнінгом криптовалют (Coin Miner), протягом останніх двох років продовжує збільшуватися, за перший квартал 2021 року кількість нових версій зросла на 6,05 млн [7]. Незважаючи на спад курсу криптовалют, кіберзлочинці, які використовують віруси для збагачення без використання обладнання для майнінгу, продовжують розробляти нові версії ПЗ, що загрожують працездатності персональних комп'ютерів (ПК).

Наступна категорія, Mobile, включає в себе шкідливе програмне забезпечення, яке несе шкоду мобільним приладам. Спираючись на дані, наведені на діаграмі (рис. 5), у 2020 році кількість нових версій збільшилася у 1,5 раза порівняно з попереднім 2019 роком. Наведена категорія вміщує віруси таких видів, як: банківські віруси, мобільні програми-вимагачі, мобільні програми для збору та передачі особистої інформації зловмисникам, MMS- та SMS-віруси. Захист від такого шкідливого ПЗ спирається на такі ж правила, що і для ПК, а саме використання антивірусного ПЗ, перевірки електронних листів на фішинг, використання захищеного Wi-FI-з'єднання.

Також відбувається зростання нових версій у категорії MSB (Malicious Signed Binaries). Віруси цього типу маскуються під виконавчі файли з цифровим підписом, які підтверджені ОС і тому можуть бути не розпізнані програмами захисту.

За 2020 рік збільшилася кількість нового шкідливого ПЗ у категорії MacOS. Кількість нових версій програм типу Exploit за минулий рік зменшилася порівняно з 2019 роком у 2,2 раза, це ПЗ по своєї суті не є вірусами у звичайному розумінні, вони є інструментом, за допомогою якого, використовуючи уразливості системи, шкідливе ПЗ дистанційно потрапляє до комп'ютерних систем.

Кількість нових сигнатур в категоріях Linuxта IoT за останні два роки значно не змінилася. Проте необхідно зазначити, що категорія IoT (Internet of Things) є доволі новою, при цьому захист обладнання, яке підключено до мережі «Розумний будинок», знаходиться не на високому рівні і має велику кількість уразливостей, що може призвести до негативних наслідків для кінцевих користувачів.

Остання розглянута категорія – iOS. До неї входить шкідливе ПЗ, яке розроблюється для мобільних систем, що використовують операційну систему iOS. За видами воно підрозділяється так само, як і в категорії Mobile, яка була розглянута вище. Користувачі пристроїв на базі iOS стикаються з аналогічними проблемами, що і користувачі Androidта Windows Mobile.

Відповідно до звітів MITRE ATT&CK [9], за перший квартал 2021 року кіберзлочинці використовували такі методи, пов'язані з постійними загрозами підвищеної складності APT.

На першому місці серед використаних методів стоїть цільовий фішинг. Як уже було зауважено у аналізі останніх досліджень та публікацій, ураження Colonial Pipeline відбулося за допомогою саме цього методу. На другому місці знаходяться різноманітні інструменти Exploit, що використовують уразливості програм, які доступні не тільки через локальну мережу, а й через Інтернет,

наприклад електроні поштові скриньки, програми типу Moodle та інші. Далі йдуть методи, пов'язані із зараженням та використанням командного рядку (commands hell та/або PowerShell).

Проте необхідно зазначити таке: більше ніж 90% випадків проникнення зловмисників у мережі організацій або приватних осіб відбувається у результаті людського фактору. Тому фішинг та соціальна інженерія є одними з основних методів, за допомогою яких кіберзлочинці обходять системи безпеки та досягають поставленої мети. Останні звіти організацій, що займаються кіберзахистом, підтверджують це твердження. Для зниження ефективності подібних методів необхідно проводити навчальні заняття з підвищення кваліфікації працівників організацій у сфері кібербезпеки.

Для зниження ризиків зараження комп'ютерної техніки, що входить до мережі організацій, використовують такі правила стратегії оборони [2, 4].

По-перше, мережа повинна бути сегментована, фізична частина розділена на різні логічні підмережі, до кожної з них додані інструменти служб керування безпекою підмереж.

Наступний етап передбачає встановлення декількох рівнів захисту та служб керування безпекою, які будуть відповідати за кожний із цих рівнів. Це підвищить безпеку мережі шляхом затримки атак на кожен із рівнів захисту, а датчики, які включені до кожного рівня, будуть повідомляти про незвичайні події.

Вищевказане може бути основою для формування стратегії безпеки з метою нейтралізації уразливостей мережі таким чином:

1) Керування оновленнями, що відповідають за виправлення уразливостей програмного забезпечення.

2) Захист серверного обладнання за допомогою використання політик безпеки.

3) Ізоляція мережі.

4) Встановлення антивірусного програмного забезпечення та брандмауера на комп'ютерні системи, що під'єднані до глобальної мережі.

5) Системи резервного копіювання: як прості, що передбачають наявність запасних копій, що зберігаються на окремих, від'єднаних від мережі організацій технічних засобах, так і складні, що використовують технології створення запасних копій під час роботи системи з визначеним часовим інтервалом.

6) Використання віртуальних приватних мереж (VPN); наприклад, під час дистанційної роботи з базами даних організації виникає необхідність дистанційного підключення до робочого місця, використання стороннього програмного забезпечення не рекомендується, а використання віддаленого робочого столу (RDP) – найбільш уразлива частина, тому що відсутнє будь-яке шифрування. Проте до недоліків VPN можна віднести складність налаштування, додаткові витрати, наявність широкого пропускного Інтернет-каналу. Також у випадку викрадення пристрою з налаштованим автоматичним під'єднанням VPN система буде скомпрометована.

7) Забезпечення неможливості фізичного доступу до комп'ютерних систем мережі зловмисниками. Персона, яка має фізичний доступ до мережі, може, використовуючи програмне забезпечення, отримати адміністративний доступ до мережі.

8) Проведення запланованих освітніх курсів із метою підвищення рівня знань з інформаційної безпеки для працівників організацій.

Якщо в процесі роботи організації виникають потреби додавання нових елементів, наприклад додаються хмарні технології, елементи «Інтернету речей» або інші, тоді необхідно переглянути всю стратегію безпеки мережі спочатку, з метою врахування необхідності додати нові рівні безпеки та пошуку уразливостей, що можуть з'явитися у процесі розширення сегментів мережі.

Висновки. Проведений аналіз останніх тенденцій кіберзагроз у комп'ютерних системах та мережах показав, що, незважаючи на протидію кіберзагрозам, показник кількості постраждалих юридичних та фізичних осіб залишається високим. Окрім цього, фактор людської помилки надає зловмисникам можливість проведення успішної атаки на комп'ютерні пристрої та мережі організацій.

Загальний висновок із виконаного аналізу може свідчити про таке. Якщо не створювати нові, в тому числі інтелектуальні системи кібербезпеки, не виконувати постійного професійного аналізу шкідливого ПЗ, пошуку та усунення уразливостей, не проводити постійного навчання співробітників компаній тощо, то втрати будуть значно вищими.

Список літератури:

1. Global Threat Landscape Report. A Semiannual Report by FortiGuard Labs. URL: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-2h-2020.pdf

2. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны / пер. с анг. Д. А. Беликова. – М.: ДМК Пресс, 2020. – 326 с.

3. Z. Balogh and M. Magdin, The problems of data security in cloudcomputing and its solution using petri nets, Lecture notes in electricalengineering, Springer, vol. 428, 2018, pp. 123–135.
4. Бараненко Р.В. Аналіз методів протидії кібератакам / А.Ю. Задорожна, Р.В. Бараненко/Юридичний-бюлетень. 2018. № 6. С. 148–161.
5. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. Київ : ДУТ, 2015. 288 с.
6. Risk Based Security Reports. URL: https://www.riskbasedsecurity.com/quickviewreports/
7. McAfee Labs Threats Reports. URL: https://www.mcafee.com/enterprise/ru-ru/threat-center/mcafee-labs/reports.html
8. Cybersecurity Education & Training Solutions. 15 Alarming Cyber Security Facts and Stats. URL:https://www.cybintsolutions.com/cyber-security-facts-stats/
9. MITRE ATT&CK. URL: https://attack.mitre.org/
10. Christopher Bing, Stephanie KellyCyber attack shuts down U.S. fuel pipeline. Reuters. URL: https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/
11. Jordan Robertson, William Turton. Colonial Hackers Stole Data Thursday Ahead of Shutdown, Bloomberg News. URL:https://www.bloomberg.com/news/articles/2021-05-09/colonial-hackers-stole-data-thursday-ahead-of-pipeline-shutdown
12. Joe Tidy. Colonial hack: How did cyber-attackers shut off pipeline? BBC. URL: https://www.bbc.com/news/technology-57063636
13. Joe TidyUS companies hit by 'colossal' cyber-attack. BBC. URL: https://www.bbc.com/news/world-us-canada-57703836
14. Pascal Ackerman. Other attack scenarios // Industrial Cybersecurity. Efficiently secure critical infrastructure systems. – Birmingham: Packt Publishing, 2017. P. 174.

Statsenko D.V., Osypenko V.V., Zlotenko B.M., Kulik T.I., Statsenko V.V. CURRENT CYBER THREATS TRENDS ANALYSIS IN COMPUTER SYSTEMS AND NETWORKS

The article considers the cyber threats trends for the 2021 and 2020. Examples of changes in the landscape of cyber threats and their impact on computer systems and networks of organizations in connection with the global events of 2020 are given. It is emphasized that every year, in order to reduce the negative effects of cyber threats, investment in information security is growing. However, the total number of cyber threats is not decreasing, but rather increasing.

An analysis of recent publications and research provides information on three large-scale cyber-attacks on international organizations. It has been noted that in the last three months, Colonial Pipeline, JBS S.A., and "Kaseya" have suffered from cybercriminals. The total damage could reach more than 100 million US dollars.

Various categories of malware used by attackers over the past few years are reviewed and analyzed. An analysis of data breaches, lost records and how trends in this cyber threats category have changed against the background of the organizations transition to remote operation in 2020. Statistics of new versions ransom ware developed during the first half of 2021 and 2020 are presented. It is emphasized that this type of malware poses a great threat to computer systems and networks, both organizations and individual users. The organizations information systems protection strategy rules which are used for defeat risks reduction of computer systems and networks are resulted. Data on new versions of malware in the category of Office, PowerShell, JavaScript, Coin Miner, Mobile, Malicious Signed Binaries, Mac OS, Exploit Linux, IoT and iOS are presented. It is reported that most successful cyber-attacks occurred as a result of human error.

The conclusion provides recommendations on the need for continuous improvement of cyber security categories.

Key words: *cyber security, computer systems, computer network, Internet, malware, data breach, ransom-ware.*