УДК 339.9+330.47

Сазонець О. М., д.е.н, професор (Національний університет водного господарства та природокористування, м. Рівне)

АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНОЇ ЕКОНОМІКИ

В статті представлено найбільш відомі типи загроз інформаційної безпеки корпоративної економіки та суспільно-економічних відносин. Подано аспекти боротьби з уразливістю корпоративних комп'ютерів. Проаналізовано типи уразливостей.
***Ключові слова*: загроза інформаційної безпеки, корпоративна економіка, уразливість, комп'ютер.**

Вступ. Бурхливий розвиток новітніх інформаційних систем у всьому світі спричинив і виникнення проблеми їх безпеки. Поняття кіберзлочинності тісно пов'язане з безпекою. Боротьба з кіберзлочинністю в багатьох країнах зараз стоїть на одному з перших місць. Для розкриття кіберзлочинів необхідно знати мотиви, механізм їх здійснення.

Аналіз останніх досліджень. Напрямком розгляду інформаційної безпеки займалося багато вітчизняних та зарубіжних вчених. Кормич Б. А. розглядав організаційно-правові питання цієї тематики. [1]. Кавун С. В., Пилипенко А. А., Ріпка Д. О. розглянули систему консолідованої інформації з позицій підприємницької діяльності [2]. В цій праці розкрито поняття й основні категорії економічної безпеки. Розглянуто ризики як фактори, що несуть загрози економічній безпеці підприємства, та управління ними. Наведено структуру економічної безпеки підприємства та поняття індикаторів економічної безпеки. Проведено оцінку безпеки економічного простору функціонування підприємства. Висвітлено теоретичні положення з формування системи управління економічною безпекою підприємства. Хансен Ф. та Олешчук В. А. дослідили процес розвитку політики виборчого управління доступом [3]. Щодо розвитку питань праці та захисту даних на корпоративних комп'ютерах представлено роботу Борисова М. А. [4] Розвиток системи економічної інформаційної безпеки розглянуто Щербаковим А. Ю. [5].

Методика дослідження. Для дослідження використано метод групування – для представлення структури системи безпеки корпоративної економіки та метод статистичного аналізу – для виділення найбільших уразливостей в економічних системах.

Постановка завдання. В статті необхідно було надати поняття кіберзлочинця, уразливості, шкідливої програми, хмарних технологій, виявити складові інформаційної безпеки корпоративної економіки і суспільно-економічних відносин, особливу уваги необхідно було звернути на уразливість комп'ютерних систем у сучасному економічному середовищі.

Результати досліджень. Для повної ясності введемо поняття кіберзлочинця. Кіберзлочинець – це висококваліфікований фахівець в галузі інформаційних технологій, який здійснює дію з проникнення в інформаційну систему, що суперечить праву даної країни, з метою порушення її цілісності або використання інформації у корисливих неправомірних цілях.

До кіберзлочинців відносяться хакери. Спочатку хакерами називали програмістів, які виправляли помилки в програмному забезпеченні будь-яким швидким і далеко не завжди витонченим або професійним способом. У сучасному розумінні – це зловмисник, який є експертом щодо певної або кількох комп'ютерних програм, операційних систем, комп'ютерних мереж, який навмисно обходить системи комп'ютерної безпеки і може написати програму, що вживає знайдені незахищеності для злому комп'ютера.

При своїй «діяльності» кіберзлочинець використовує інформацію, вільну для користування в пошукових системах Google, Rambler, Yandex, Yahoo та ін. Зловмисник збирає номери телефонів жертв, адреси електронної пошти, адреси і місця розташування офісів, відомості про ділових партнерів. Потім злочинець розвідує в комп'ютерній мережі адреси і доменні імена комп'ютерів, які в даний момент підключені до Інтернету. З їх допомогою він, зламуючи маршрутизатор, досягає мети. Дамо визначення найпоширеніших загроз безпеки корпоративних систем і суспільно-економічних відносин.

Під уразливістю комп'ютерних систем слід розуміти наявність в них пролому, завдяки якому вони доступні зловмисникові. При цьому він може зробити різні неправомірні дії, а саме, порушити цілісність системи, викликати її неправильну роботу.

Наступним не менше небезпечним засобом досягнення мети зловмисником є шкідливі програми.

Шкідлива програма, або вірус (комп'ютерний хробак), – це програма, націлена на отримання несанкціонованого доступу до електронно-обчислювальних ресурсів комп'ютера або до інформації, що зберігається на ньому, яка здатна відтворювати себе на комп'ютерах з метою несанкціонованого використання ресурсів ЕОМ або нанесення шкоди власнику інформації, комп'ютера і / або інформаційній мережі ЕОМ

шляхом копіювання, спотворення, видалення, блокування, модифікації, копіювання комп'ютерної інформації або її підміни. При цьому користувач не підозрює, що його комп'ютер заражений. Оскільки кожна наступна копія вірусу або комп'ютерного хробака також здатна до самовідтворення, зараження поширюється дуже швидко.

В даний час серед користувачів Інтернет популярним і дуже прогресивним стало використання хмарних технологій.

Хмарні технології – це парадигма, яка передбачає віддалену обробку і зберігання даних. Ця технологія надає користувачам мережі Інтернет-доступ до комп'ютерних ресурсів сервера і використання програмного забезпечення як онлайн-сервісу. Тобто якщо є підключення до Інтернету, то можна виконувати складні обчислення, обробляти дані, використовуючи потужності віддаленого сервера. При використанні хмарних обчислень програмне забезпечення надається користувачеві як Інтернет-сервіс. Користувач має доступ до власних даних, але не може управляти і не повинен піклуватися про інфраструктуру, операційну систему та програмне забезпечення, з яким він працює. «Хмарою» метафорично називають Інтернет, який приховує всі технічні деталі. Однак з їх появою виникли проблеми з проникненням в ці технології і порушенням їх роботи.

Не менш важливим аспектом електронізації діяльності корпорації стала поява мобільних телефонів, якими активно користуються співробітники при веденні бізнесу. На сьогоднішній день за даними фахівців аналітичної компанії IDC по ринку смартфонів за другий квартал 2015 року ринок виріс в порівнянні з тим же періодом 2014 року на 11% – з 302,1 до 337,2 млн штук. Смартфони мають програмне забезпечення, тому, як і інші пристрої, можуть бути схильні до атак.

Останнім часом популярним стало використання соціальних мереж як для особистого листування користувачів, так і для цілей корпорацій. У соціальних мережах компанії розміщують рекламу, повсякденні події, що відбуваються в компанії, інформацію, цінну для компанії. Однак останнім часом треба бути дуже обережним при взаємодії з іншими користувачами через соціальні мережі. Наприклад, «Одноклассники» опублікували «білі списки сайтів», на які переходити небезпечно. За останніми даними ця соцмережа опублікувала також «чорний список» адрес сайтів, на які немає можливості перейти безпосередньо з соцмережі, Таким чином «Одноклассники» запобігають перехід на потенційно небезпечні сайти.

На сьогоднішній день прискорює темп розвиток роботизації. Роботи все більше інтелектуалізуються. І це теж несе в собі загрозу для

людства.

Також необхідно розглянути такий елемент інформатизації корпорацій, як проблема фізичної безпеки пристроїв, які мають кілька аспектів. При цьому необхідно виділити фізичні заходи захисту інформаційних пристроїв – це різного роду механічні, електро- або електронно-механічні пристрої і пристрої, призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів захисту інформації.

У зв'язку з прискореними темпами удосконалень гаджетів підприємства і суспільство в цілому стикаються з новим видом загрози – так званої смартфонозалежністю. Ця загроза особливо поширена у молодих верств населення, оскільки вони більш схильні до впливу нововведень, що з'являються у світі науки і техніки. І це теж є проблемою як на виробництві, так і в суспільному житті людей в цілому.

На сьогоднішній день нестримно поширюється мережа Wi-Fi. У найближчі чотири роки стільникові оператори збережуть у себе всього лише 40% мобільного трафіку, а все інше піде по мережі Wi-Fi. Найактивніше процес буде відбуватися в Європі і Північній Америці: там в 2019 році по Wi-Fi буде передаватися 75% усього мобільного трафіку.

В абсолютних величинах обсяг Wi-Fi-трафіку у світі зросте з нинішніх 30 000 петабайт до 115 000 петабайт. Відносно розвантажені мобільні мережі, проте, теж будуть передавати все більше трафіку щороку, в абсолютних цифрах [6]. З появою можливості спілкуватися з використанням бездротової мережі народилися і нові загрози. Таким чином позитивно налаштованому людству необхідно постійно бути готовим протистояти все більшій і більшій кількості загроз в інформаційному просторі (рис. 1).

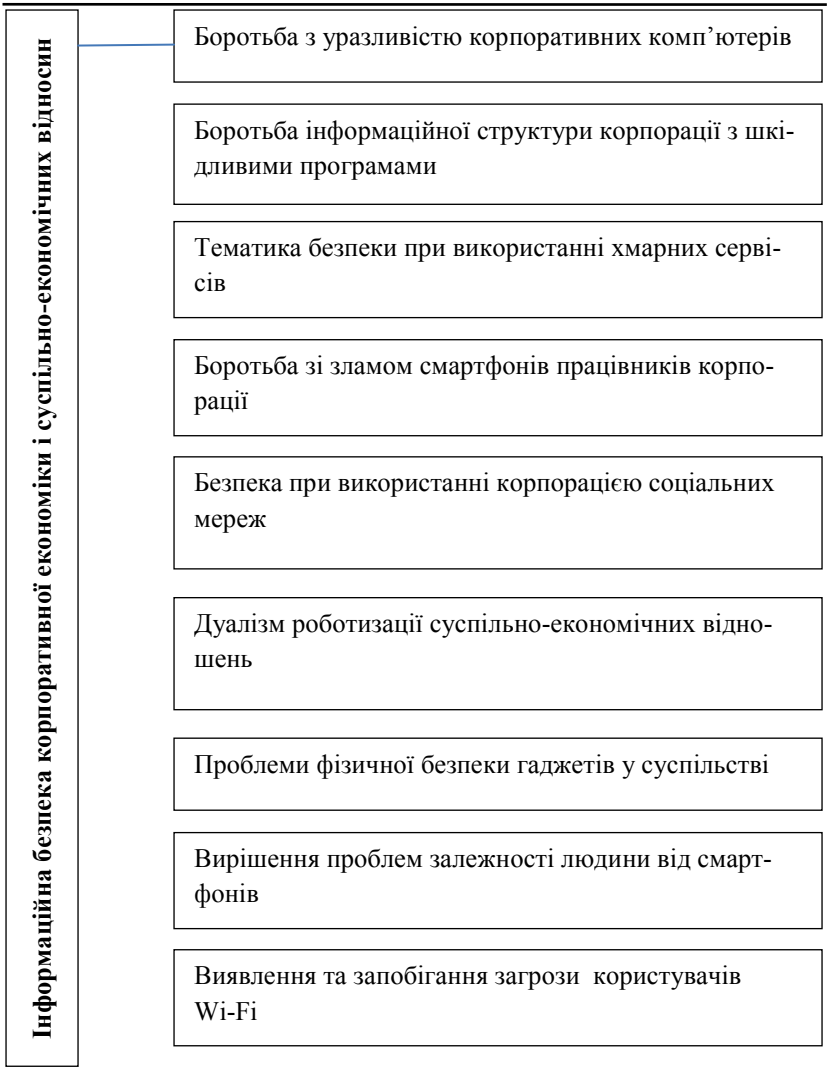

Рис. 1. Схема інформаційної безпеки корпоративної економіки і суспільно-економічних відносин

Представимо процес боротьби з уразливістю корпоративних комп'ютерів. У будь-якій корпорації існує гонитва за новими, досконалими програмами. Реклама штовхає інформаційних працівників

пропонувати нові програмні продукти. Програмісти, поставивши на комп'ютер нову програму, часто навіть не уявляють, наскільки вразливою вона може бути. Наприклад, дослідник з безпеки Тавис Орманді знайшов серйозну уразливість в програмному забезпеченні компанії Symantec. Це програмне забезпечення дозволяло зловмисникові легко отримати віддалений доступ до комп'ютера, на якому воно встановлено. Необхідно відзначити, що серйозну уразливість також мають програми Comodo Firewall або Comodo Internet Security. Помилка була знайдена в програмі GeekBuddy, що використовується для надання платної технічної підтримки користувачам за допомогою з'єднання з бюро технічної підтримки. Як виявилося, це з'єднання не було захищено паролем. Пізніше творці ПЗ усунули помилку завдяки Тавісу Орманді [7].

Популярна ОС Linux також не позбавлена цих недоліків. Кіберексперти з компанії Perception Point виявили уразливість, яка присутня у версіях ядра ОС Linux, починаючи з версії 3.8. Ця вразливість дозволяла користувачам і програмам в обхід заборон отримати повний доступ до ОС в якості адміністратора. В результаті в небезпеці опинилися десятки мільйонів комп'ютерів. Так як багато мобільних телефонів використовують ОС Android, засновану на ядрі Linux, вони теж виявилися в зоні ризику [8].

У дорогої комп'ютерної техніки компанії Apple Mac також були виявлені вразливі місця. Їх виявили працівники компанії LegbaCore. Не дивлячись на труднощі, пощастило усунути неполадки до оголошення цього інциденту широкому загалу. Через два місяці компанія Apple купила LegbaCore. Завдяки цій угоді багато користувачів тепер можуть безболісно використовувати комп'ютери Mac.

Зустрічаються уразливості, які «сидять» в комп'ютерах довгий час і залишаються невиявленими. Так, в програмному забезпеченні процесора Intel виявлена існуюча 18 років вразливість, що дозволяє хакерам встановлювати на комп'ютери «вічні» віруси, а також порушувати роботу ПК. Компанія після виявлення проблеми виправила її для останнього покоління комп'ютера і випустила патч (патчем називається автоматизоване програмний засіб, що окремо поставляється і використовується для усунення проблем в програмному забезпеченні або для зміни його функціональності) для чіпів попередніх поколінь. Однак його застосування не завжди призводить до «вилікування» комп'ютерів.

Уразливості відрізняються за типом (рис. 2).

Ми бачимо, що найбільш поширена загроза – відмова в обслуговуванні для мережевого обладнання, не на багато менше – виконання до-

вільного коду. Найнижчий показник мають помилки при роботі з пам'яттю.

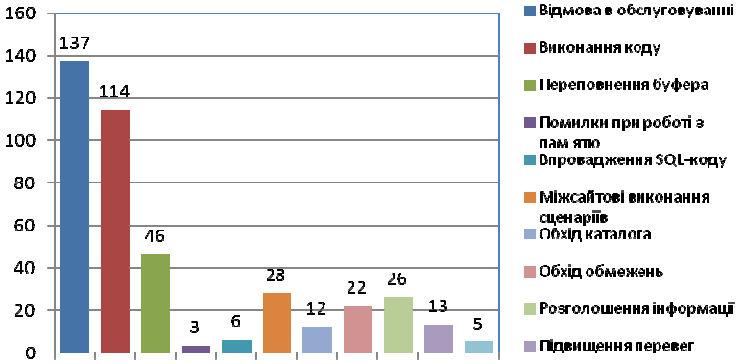

Рис. 2. Розподіл кількості уразливостей за типом [9]

Висновки. У даному дослідженні виявлено найбільш поширені види загроз: уразливість комп'ютерів, атака з боку шкідливих програм, загрози при використанні хмарних технологій, злам смартфонів, небезпека у соціальних мережах, небезпека роботизації виробництва і суспільного життя, фізична небезпека гаджетів, зростаюча залежність людини від мобільних телефонів, небезпека в мережі Wi-Fi. Вони впливають як на корпоративну діяльність людини, так і на стан суспільно-економічних відносин. Проведено аналіз складових уразливості комп'ютера. Встановлено таку найбільш поширену загрозу, як відмова в обслуговуванні для мережевого обладнання. Показано, що друге місце займає виконання довільного коду, а найнижчий показник мають помилки при роботі з пам'яттю.

1. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України: Автореф. дис. д-ра юрид. наук: 12.00.07. / Б. А. Кормич. – Х. : НХУ України, 2004. **2.** Кавун С. В. Економічна та інформаційна безпека підприємств у системі консолідованої інформації : навч. посіб. / С. В. Кавун, А. А. Пилипенко, Д. О. Ріпка; Харк. нац. екон. ун-т. – Х. : ХНЕУ, 2013. – 362 с. –С. 337–352. **3.** Hansen F. and Oleshchuk V. A. Conformance Checking of RBAC Policy and its Implementation, The First Information Security Practice and Experience Confe-?ence, ISPEC 2005, Singapore, LNCS. – Volume 3439. – Pp. 144–155, 2005. **4.** Борисов М. А. Особенности защиты персональных данных в трудовых отношениях. (Гриф УМО по дополнительному профессиональному образованию) / М. А. Борисов. – М. : Книжный дом «ЛИБРОКОМ», 2013. – 224 с. **5.** Щербаков А. Ю. Современная компьютерная безопасность. Теоретические

основы. Практические аспекты / А. Ю. Щербаков. – М. : Книжный мир, 2009. – 352 с. **6.** Світова статистика використання WIFI: частотний ресурс закінчується. – Https://xakep.ru/2015/06/26/wifi-stat/ **7.** Уязвимость в Comodo позволяла удаленно захватить компьютер [Електронний ресурс]. – Режим доступу: http://prostotech.com/internet/95-uyazvimost-v-comodo-pozvolyala-udalenno-zahvatit-kompyuter.html **8.** Уязвимость в Linux поставила под удар десятки миллионов компьютеров [Електронний ресурс]. – Режим доступу: https: //lenta.ru/news/2016/01/20/linuxfail/ **9.** Популярное сетевое оборудование и статистика уязвимостей – SecurityLab.ru. – [Електронний ресурс]. – Режим доступу: http: //www.securitylab.ru/analytics/423523.php.

Рецензент: д.е.н., професор Левицька С. О. (НУВГП)

Sazonets O. M., Doctor of Economics, Professor (National University of Water Management and Nature Resources Use, Rivne)

ASPECTS OF INFORMATION SECURITY OF CORPORATE ECONOMY

The paper presents the most famous types of threats to information security of corporate economics and socio-economic relations. Posted aspects of combating vulnerability corporate computers. Analyzed the types of vulnerabilities.
***Keywords*: threats to information security, corporate economics, vulnerability, computer.**

Сазонец О. Н., д.э.н., профессор (Национальный университет водного хозяйства и природопользования, г. Ровно)

АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ ЭКОНОМИКИ

В статье представлены наиболее известные типы угроз информационной безопасности корпоративной экономики и общественно-экономических отношений. Подано аспекты борьбы с уязвимостью корпоративных компьютеров. Проанализированы типы уязвимостей.
***Ключевые слова*: угроза информационной безопасности, корпоративная экономика, уязвимость, компьютер.**
